Ismét elesett a kekesteto.com

2009.01.01. 10:27 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: deface kekesteto törökök

Nem kellett sok idő ahhoz, hogy **támadók ismét lecseréljék** a turisztikai weboldal címlapját.

Mint arról az Index beszámolt, 2008. december 26-án ismeretlen török elkövetők **defacelték az oldalt**. Most a weboldalra a "HaCKeD Cyber_Melankolia" felirat mellett Izrael ellenes szöveg került.

A Kekesteto.com oldalnak normál esetben valahogy így kellene kinéznie, és a **Fuck Izrael helyett hójelentések, időjárás, fényképek, nyitvatartások szerepelnének rajta**.

Ha a Googleban rákeresünk a korábbi eset "HACKED ßy" stringjére, több találatot is kapunk. Ami azonosnak látszik például az imrejozsef.blog.extra.hu oldal és a kekesteto.com esetében, az az **Apache 2.2.3 és a PHP 5.2.x**.

Valószínű, hogy a támadóknak totál **lényegtelen volt a weboldal tartalma** (nem a Kékestetőt akarták kiemelten bántani), hanem sérülékenységkeresés közben ezekbe a helyekbe botlottak. Az imrejozsef... oldal esetén az az elszomorító, hogy valakinek van egy saját weboldala, és **július óta nem veszi észre a dúlást rajta**.

A kekesteto.com oldalnál pedig elképzelhető, hogy az első támadás után csak a tartalom mentésből való visszaállítása történt meg, **a szükséges logelemzés, nyomozgatás, szoftverfrissítés esetleg nem**.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/851225

Kommentek:

Nincsenek hozzászólások.

Túlzott jogok a brit rendőrségnél

2009.01.05. 18:37 | Csizmazia István [Rambo] | 1 komment

Címkék: internet brit adatbázis ellenőrzés kémprogram

Nem meglepő, hogy emberjogi szervezetekkel az élen többen is tiltakoznak az ellen, hogy **bírósági felhatalmazás nélkül is információkat lehessen majd gyűjteni az angol állampolgárok számítógépeiből**.

Az adatgyűjtés kiterjed minden telefonhívásra, e-mailre és a meglátogatott weboldalak adataira is. Ez a módszer szinte azt jelenti, hogy **minden állampolgárnak el kell tűrnie, hogy a számítógépébe hivatalosan betörjenek**. **A jogvédők tiltakoznak**, pert fontolgatnak.

A cikkben nem ismertetnek közelebbi technikai részleteket, de izgalmas kérdések így is vannak. A rendőr szabadon nézegetheti majd például Joanne Kathleen Rowling adatforgalmát és elsőnek olvashatja a Harry Potter 100-at? **Ki és milyen körülmények között tekinthet bele majd ebbe a gigászi adatbázisba?** Mi védi meg a privátszférát a túlbuzgó állami ellenőrzéstől? Megannyi homályos részlet.

És persze az is egy érdekes esemény lehet, ha valaki éppen ebbe az adatgyűjtőközpontba tör majd be...

Félreértés ne essék, senki nem akarja a pedofilokat és a terroristákat védeni, **itt a kulcsmomentum a "bírósági végzés nélkül is" kategória** az, ami elég durvoid beavatkozásnak tűnik az átlagfelhasználók ellenében - **ha valóban megszavazzák ebben a formában**. Mindenesetre kíváncsian várjuk a további fejleményeket.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/859296

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.01.11. 18:00:35

A magánélet minden ember joga :-)
www.penzcentrum.hu/cikk/1015362/1/egy_evig_kell_majd_tarolni_az_e-maileket

Kártevő-e a rendőrségi kémprogram?

2009.01.07. 14:01 | Csizmazia István [Rambo] | 2 komment

Címkék: brit spyware kémprogram detektálás

Komoly indulatokat kavart a múltkori posztban említett **brit törvénytervezet**, ahol ráadásul magáncégek bevonásában is gondolkodnak a totális ellenőrzésnél.

A külön **ügyészi vagy bírósági engedély nélküli behatolás a számítógépekbe annyira abszurd**, ráadásul pont egy ilyen régi demokráciában végrehajtva valóban furcsa és meglepő. Nyilván senkinek a szeme sem rebbene, ha mindez Kubában vagy Kínában történne, és ezen a **terrorveszélyre való hivatkozás** sem enyhít eleget.

Mindenesetre érkeznek az első reakciók is, amelyben a biztonsági cégek is erős kritikával illetik az ilyen típusú felügyeletet. Ezúttal Graham Cluely, a Sophos szakértője nyilatkozott, és **megerősítette, nem tesznek kivételt a kártevők között. Ha a brit rendőrség kémprogramját észlelik, detektálni fogják azt**.

Kérdés persze, mi fog történni majd a valóságban a különböző szoftverek esetében, ha ugyanis **mégis igyekeznek az adott ország törvényeit betartani**, az szülhet konfliktusokat. A CheckPointtól egy hasonló kérdésfelvetésre olyan választ olvashattunk, ami nem zárkózik el a kérésre történő fehérlistára vételtől. ("We do have a policy whereby legal, legitimate software programs from any third-party vendor can be 'whitelisted' from detection upon request. We would afford law enforcement the same courtesy.")

Nem most lenne persze az első eset, mikor a cégek titokban beadják a derekukat és ebből később botrány kerekedik. Jó példa erre a Microsoft védett tárolóinak franciaországi titkosítása, de akár a kínai Google működése is megérdemelne egy misét. Érdeklődőknek **jó olvasmány lehet egy korábbi felmérés**, még évekkel korábbról, ahol a résztvevők zöme "No", "Oh, not at all", "Absolutely not" vagy "Hmm" válaszokat adott, ahogy egy jó titkos ügynöknek is azt kell válaszolnia a "Titkos ügynök ön?" kérdésre, hogy "Természetesen n de ha az lennék, sem mondhatnék mást."

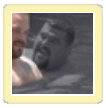
Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/863131

Kommentek:



GayBears · http://gaybears.blog.hu/ 2009.01.07. 18:27:35

egy reklámblogban a nod32 véleménye miért nincs feltüntetve?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.07. 21:05:19

Csákó!

A kérdés filozófiailag is érdekes, görög drámákat idéző lehet akár egy Ancsel Éva könyvben. Mondjuk te vagy Eugene Kaspersky és behivat Putin elnök egy kis elbeszélgetésre, ahol egy "apró baráti szívességet" kér, pl. ne észlelj egy adott kémprogramot. Egyik kezében X csillió dollár, a másikban a gyereked fotója, ahogy kilép az óvodából, az asztalon pedig Szibéria hegy és vízrajzi térképe ;-)

A viccet félretéve a 2007-es körképben ahogy láttad, nem szerepelt az ESET, ahogy látom, jobbára a jelentősebb állami megrendelések beszállítóit faggatták. A poszt nem a NOD-ot akarta dícsérni, és közben a többieket fikázni, hanem pusztán erre a furcsa felemás helyzetre akarta felhívni a figyelmet.

Személy szerint nem ismerem az ESET hivatalos állásfoglalását, de megpróbálom megkérdezni, és ha lesz info, akkor beírom majd kommentbe.

BUÉK.

Az online játékosok jelszavait lopják a kártevők

2009.01.08. 11:12 | Csizmazia István [Rambo] | 1 komment

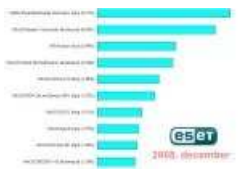
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET **több százezer hazai felhasználó adatain alapuló vírusstatisztikája** szerint itthon is elterjedtek azok a károkozók, melyek **az online játékok belépési adatait lopják el a számítógépekről**. A megszerzett felhasználóneveket és **jelszavakat a bűnözők az interneten értékesítik**.

Eddig jobbára csak az Egyesült Államokban és Nyugat-Európában terjedtek azok a kártevők, melyek az internetes játékok belépési adatait lopják el a felhasználók számítógépeiről. A hazai játékosok számának szaporodásával együtt azonban **a magyar vírustoplista 6. helyén is megjelent a külföldi listákon már veteránnak számító Win32/PSW.OnLineGames kártevőcsalád**. A hazai fertőzések körülbelül 2 százalékáért felelős károkozó olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekeznek gépünkre telepíteni. A vírus gyakran olyan úgynevezett rootkit komponenssel is rendelkezik, amelynek segítségével megpróbálja leplezni, eltüntetni állományait, illetve működését a fertőzött számítógépen. A kártevőcsalád tevékenysége **jellemzően az online játékok jelszavainak begyűjtésére, és a jelszó adatok titokban történő továbbküldésére koncentrálódik**. A vírusok készítői ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz jutnak hozzá, melyeket aztán **illegális csatornákon továbbértékesítenek**.

Decemberben a magyar vírustoplista első helyein is történt változás. A régóta vezető, Virtumonde névre keresztelt károkozó átengedte az első pozíciót a WMA/TrojanDownloader.GetCodec trójainak, így most csak az ezüstérmes helyet foglalja el. A két kártevő működése hasonló: **mindkettő ingyenes és hasznosnak tűnő alkalmazásokat vagy tartalmat kínál letöltésre** a felhasználóknak. Mellékhatásként azonban kéretlen reklámokat jelenítenek meg a számítógépeken, és úgynevezett hátsó ajtót nyitnak, melynek segítségével a bűnözők akár a gép irányítását is átvehetik. A két vezető kártevő nagymértékű elterjedtsége mutatja, hogy **a rendszeres figyelmeztetések ellenére a magyar felhasználók továbbra is maguk telepítik a hasznos szoftvereknek álcázott kártevőket**.

Szintén a felhasználók gondatlanságát igazolja, hogy a januári toplistára – méghozzá az 5. helyre – felkerült a Win32/Conficker.A nevű károkozó, **mely a Windows egy már hónapok óta ismert biztonsági hibáját használja ki. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőség javítására a Microsoft már tavaly októberben kiadott egy frissítést, melyet sokan mindmáig nem töltöttek le**. A tanulság, hogy a vírusok elleni védekezésben nem csupán a frissített vírusirtó szoftver, de a gondos felhasználói magatartás is fontos szerepet játszik.



Végül következzen a **2008. decemberi magyarországi toplista**. Az ESET statisztikai rendszere szerint az elmúlt egy hónapban az alábbi 10 károkozó terjedt a legnagyobb számban, melyek együttesen az összes fertőzés 36,2%-ért voltak felelősek:

1. WMA/TrojanDownloader.GetCodec.Gen trójai
Elterjedtsége a decemberi fertőzések között: 9.31%
Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry

bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

2. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a decemberi fertőzések között: 8.86%
Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

3. INF/Autorun vírus
Elterjedtsége a decemberi fertőzések között: 5.48%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

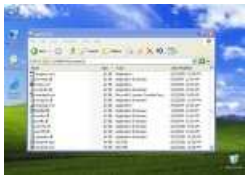
4. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a decemberi fertőzések között: 2.69%

Működés: Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

5. Win32/Conficker.A féreg
Elterjedtsége a decemberi fertőzések között: 2.49%

Működés: A Win32/Conficker.A egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy onnan további kártékony kódokat töltsön le.



A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/conficker-a

6. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a decemberi fertőzések között: 1.62%

Működés: Ez a kártevő család olyan trójai programokból áll, amely billentyűleütés-naplózót (keylogger) igyekszik gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével megpróbálja állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására és a jelszó adatok titokban való továbbküldésére koncentrálódik. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyet aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

7. Win32/VB.EL féreg
Elterjedtsége a decemberi fertőzések között: 1.61%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.

A számítógépre kerülés módja: fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.
Bővebb információ: http://www.eset.hu/virus/vb-el

8. Win32/Agent trójai
Elterjedtsége a decemberi fertőzések között: 1.57%

Működés: Ezzel a gyűjtőnévvel azokat rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

9. Win32/Patched BU trójai
Elterjedtsége a decemberi fertőzések között: 1.46%

Működés: A Win32/Patched.BU trójai a Windows XP operációs rendszerben, a C:\windows\system32-ben lévő dmserver.dll állományt módosítja oly módon, hogy a fájl eredeti mérete nem változik. A fájl a Logikai Lemezkezelő Szolgáltatáshoz tartozik.

A számítógépre kerülés módja: más kertevő telepíti.
Bővebb információ: http://www.eset.hu/virus/patched-bu

10. Win32/CMDOW.143 alkalmazás
Elterjedtsége a decemberi fertőzések között: 1.36%

Működés: A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. A Cmdow egy olyan parancssori segédprogram, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhetjük, átnevezhetjük, elrejthetjük vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk illetve inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cmdow alkalmazás egy 31 KB-os végrehajtható fájl, amely nem ír a rendszerleíró-adatbázisba, nem igényel külön telepítést, elég lefuttatni. Eltávolításához elegendő ezt az állományt törölni.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/cmdow-143

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/864995

Kommentek:

keeroy · http://music.blog.hu 2009.01.08. 22:55:58

Köszönjük szépen az összefoglalót.

A 25 legveszélyesebb programozói hiba

2009.01.12. 18:02 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hiba biztonság programozás sans mitre

A CWE/SANS közzétette a **huszonöt legveszélyesebb programozói hiba** listáját.

A PDF fromátumú összefoglalóban nem csak XSS, SQL injection, stb. hibaleírások szerepelnek, de **javaslatok, megoldások és tanácsok is, hogy lehet csökkenteni a veszélyt, illetve elkerülni**, hogy e sebezhetőséget a támadók kihasználják. A programozóknak szánt útmutatót az NSA támogatásával, illetve finanszírozásával sikerült összeállítani.

1940 novemberében az amerikai Tacoma-híd a szél által keltett rezgéshullámok miatt összeomlott. Olyasmi történt, AMIRE A TERVEZÉSKOR NEM SZÁMÍTOTTAK.

A dokumentációt MITRE és SANS Institute kezdeményezésére **különféle cégek biztonsági szakemberei készítették**, például a Symantec, Microsoft, a DHS's National Cyber Security Division, az NSA's Information Assurance Division, de szerepelnek még a japán IPA, illetve kaliforniai egyetemek munkatársai is. Minden (webre) programozónak **kötelező olvasmány** lehet(ne). Letölthető innen.

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/872825

Trackbackek, pingbackek:

Trackback: BuheraBlog 2009.01.17. 13:13:47

SlágerlistákA héten megjelent egy, a SANS, az NSA, a Symantec és még egy sor neves szervezet közreműködésével készült, a 25 legveszélyesebb programozói hibát tartalmazó toplista. A gyűjteménynek jó nagy médiavisszhangja lett, jó eséllyel a Common Weakness…

Kommentek:

Nincsenek hozzászólások.

Fertőzött volt Paris Hilton weboldala

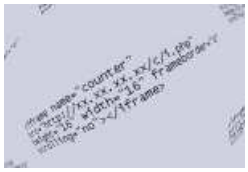
2009.01.13. 18:25 | Csizmazia István [Rambo] | 11 komment

Címkék: weboldal paris fertőzés hilton iframe exploit

Az dolog ahhoz a korábbi esethez hasonlított, mikor az amerikai baseball és hoki liga weboldalát fertőző bannerhirdetésekkel támadták meg. Ennek hatására **a gyanútlan látogatók gépeit kártevők árasztották el**.

Paris Hilton weboldala, a www.parishilton.com január 9-én szenvedett támadást. Mint azt **a ScanSafe kutatói észlelték**, a weboldal kódjába ismeretlenek olyan IFRAME taget ágyaztak be, amely a you69tube.com pornó oldalon elhelyezett kártevőre mutatott. Ez letöltött egy olyan **preparált PDF állományt**, ami aztán egy exploit kihasználásával igyekezett megfertőzni a számítógépeket.

A kártevő **igyekszik további kártékony komponenseket is letölteni** egy felbukkanó popup ablakon keresztül, f**üggetlenül attól, hogy az OK vagy a CANCEL gombra** kattintunk-e. Tapasztalatok szerint ilyenkor csak a CTRL + ALT + DEL billentyű kombináció segíthet, ki kell lőni a feladatkezelőben a böngészőt. A szakértők még nem azonosították be, hogy **pontosan mely sebezhetőség kihasználásával operál**, állítólag ez egy már novemberben befoltozott hiba, de ezt a hírt nem erősítették meg. Mary Landesman, vezető biztonsági kutató szerint 38 antivírusprogramból egyelőre mindössze csak 7 észleli.



Beigazolódni látszik az a jóslat, amely **a böngészés során terjedő fertőzések jelentős emelkedését prognosztizálta**. Valószínű, hogy a híresség weboldala rajongók és a fiatalok körében nagy népszerűségnek örvend, ezért **jelentős számú látogatót vonzó célpontnak gondolták a támadók**.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/875249

Kommentek:

keeroy · http://music.blog.hu 2009.01.13. 20:12:17

Szép munka. Természetesen sokszoros idézőjelbe téve. A továbbiakban én is nagyon is el tudom képzelni, hogy az "ovis", klasszikus deface-ek helyett inkább észrevehetetlenül ilyesmit ágyaznak be az oldal kódjába. Lesz ebből még fejfájás bőségesen.

gothmog 2009.01.13. 20:33:19

NoScript továbbra is a barátunk.

mnmnbkhj 2009.01.13. 20:35:56

Pornó meg a kate perry? nem áll mesze egymástól :)

mnmnbkhj 2009.01.13. 20:41:02

izé paris bocsi :)

agyvihar · http://agyvihar.blog.hu/ 2009.01.13. 21:15:14

Operával biztonságban érzem magam. 1% alatti böngészők támadásával csak nem bajlódnak. :D

Bambano 2009.01.13. 22:22:56

Számítógépeket??? Milyen számítógépeket?

WUT (törölt) 2009.01.13. 22:56:13

hol van kate perry-s pornó??

:DD

on.

tisztelt Csizmazia Úr!

olyan miért történhet, hogy a gépem (Win XP oprendszer van rajta) hirtelen azt jelzi , mintha egy pendrive-ot csatlakoztattam volna usb-n, új hardver stb de közben nem?! és rövidesen eltűnik az egér kurzora! nem tudom használni az egeret!

eddig kétszer fordult elő az elmúlt 1 hétben, először Ctrl + Alt + Del-lel, feladatkezelővel elkezdtem kikapcsolgatni a futó programokat, és sikerült valahogy visszahozni az egeret, de második alkalommal már manuálisan (a Power gomb 5 mp-ig lenyomva tartásával) ki kellett kapcsolnom a gépet, mert nem tudtam mást csinálni! A feladatkezelő is használhatatlan volt.

Ez most szombaton volt, azóta folyamatosan használom a gépet, és semmi gond nincsen.

hozzá kell tennem, használok NoScriptet, legutóbbi Spybot-keresés 2 hónap után nem talált semmilyen kártevőt (ez még az eset előtt volt, azóta nem scanneltem), használok vírusirtót, Gmailen levelezek, semmilyen spam-gyanús dolgot nem nyitok meg, pornóoldalakra nem megyek stb., nem értek az internet-biztonsághoz, de valamennyire "felvilágosultnak" tartom magam, és legalább próbálom a biztonságos utat járni.. de ilyennel még soha nem találkoztam. Ez lehet kártevő?

Hozzá kell tennem, hogy amikor ez történt, egyszerre ment a zene, a torrent kliens, az excel, a firefox legalább 10 ablakkal, köztük a honlapom admin-felületével és egy online deviza-kereskedő szoftver felületével, + Word + Adobe Reader is megvoltak nyitva.

Előre is köszönöm, ha valaki tud adni tanácsot ebben.

Hun.Spb · http://www.hunspb.blog.hu/ 2009.01.14. 15:24:53

USB-s egér?

r@ek (törölt) 2009.01.14. 16:41:52

Ismet egy roppant izgalmas post..
Ennel mar csak a kekestetoi deface volt erdektelenebb. Azert egy szint ala csak nem kene mar lemenni..

Skiddie vadasz! :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.14. 21:17:50

@Fiveeeee:
Sajnálom, ha nem tecc.

@WUT:
Szerintem is jó ötlet Hun.Spb felvetése, ha valóban USB-s egeret használsz. Egy egér driver ellenőrzés mellett ha a teljes, full opciós vírusellenőrzés nem talál semmit és nem történik semmi további furcsaság, akkor lehet, hogy nem is fertőzés. Lehet még további progikkal is próbálkozni, nekem volt hogy a Spyware Terminator megtalált olyat, amit a S&D nem. Aztán ott vannak még online scannerek is (az ESET-nek is van ilyenje: www.eset.hu/viruslabor/onlineellenorzes), ezeket is rá lehet kergetni a gépre, ha biztosra akarsz menni.

WUT (törölt) 2009.01.16. 13:30:37

köszönöm a választ!

az egér egyébként nem usb-s, csak amikor ez a dolog történt, az egér megszűnt működni! a feladatkezelő nyomogatásán kívül tehetetlen voltam. de remélem, nem fordul elő többet, nekiállok vadul scannelni :)

tetszik a blog, a NoScript nevű progit is az egyik cikk alapján kezdtem használni, azóta nagyságrendekkel csökkent a kártevők száma :)

Szépen muzsikál a NOD32 a Win7 bétán

2009.01.14. 11:11 | Csizmazia István [Rambo] | Szólj hozzá!

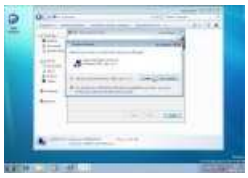
Címkék: béta teszt security smart eset windows7

Egy rövid teszt erejéig kipróbáltuk a számos újdonságot felvonultató ESET Smart Security 4 béta verzióját a Windows 7 béta változatán. Az ESET fejlesztői szerint tökéletesen működik integrált biztonsági programjuk a vadonatúj operációs rendszeren, és ez tapasztalataink szerint így is van.

Mindenek előtt **a programok letöltési lehetőségeiről ejtünk szót**. A Windows 7 béta mindenki számára letölthető, eltörölték a korábban megszabott 2.5 milliós korlátot. Sőt, nem csak 30 napos, de egészen augusztus 1-ig érvényes termékkulcsot is igényelhetünk egészen január 24-ig. A Windows7 a Microsoft weboldaláról tölthető le. A Smart Security 4 béta pedig az ESET weboldalán található, a letöltési szekcióban.

Indulhat a telepítés a Win7 alatt

A Vistához hasonlóan itt is engedélyezni kell az UAC (User Account Control) alatt



A szükséges ESET driver telepítése következik a varázslóban

Kész is a telepítés, ideje használatba venni.

Keletkezett a menüben egy ESET Smart Security gyorsindító ikon

A Maximum protections status jó jelnek tűnik

Indítsunk egy kézi keresést a teljes merevlemezre!

Az About screenen nem csak az látszik, hogy ez a 4.0.68.0 build, hanem az is, hogy bár csak 512 MB RAM van a gépben, mégis minden problémamentesen működik.

Az EICAR teszt rendben jelez, és a jelzett eltávolítási gond sem valódi, hiszen egy CD ROM lemezről van szó, ahol ugye a törlés, mentesítés ezúttal nem lehetséges

Az ingyenesen letölthető béta változatok után **a végleges 4.0-ás verziók várhatóan 2009. februárban lesznek elérhetőek** először angol nyelven, majd pedig magyarul egy-két hónappal később kaphatjuk kézhez.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Utaljunk pénzt a S.O.C.A.-nak
- 25-ször több a mobilos kártevő
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/875483

Kommentek:

Nincsenek hozzászólások.

Osama Bin-Laden Viagrával

2009.01.15. 18:44 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam hoax osama viagra

Két érdekes email is érkezett a mai postával. Egy **ordas nagy hoax**, meg egy rakat Windows Live profilszerűség, linkhivatkozással ellátva. Ami közös bennük, hogy mindkettő átverés.

Az első levélnél nem mehetünk el szó nélkül amellett, **hány luzer "há' azér' továbbküldöm, ki tudja..." mentalitással, mentalista érzet nélkül;-) csak azért is továbbítja**. A forwardozók egy része talán túl buta, egy részük talán túl lusta, a maradék meg a kettő együtt :-), mindenesetre sajnos jellemző ez a hozzáállás főleg a vállalati levelezésben.

Íme a levél szövege:

"Téma: Figyelem!Olvasd el,fontos!!!!!!

Az elkövetkezendő napokban E-mail útján képeket küldhetnek, melyen
Osama Bin-Laden vagy felakasztva látható, vagy elfogása látható. .
Ha ilyen E-mailt kap(sz), ezt a mellékletet nem szabad megnyitni,
mert a merevlemezt azonnal, menthetetlenül tönkreteszi, leégeti.
Kérem, küldje tovább ezt az üzenetet mindenkinek, aki az E-mail
listá(do)n van! Inkább kapjuk meg ezt a veszélyt jelző üzenetet
100xszor, mintsem tönkremenjenek a legfontosabb adataink a számítógéppel
együtt.
Ha olyan üzenetet kap(sz) amelynek címe: ?Invitation" ? függetlenül
attól, hogy ki küldte, azonnal ki kell törölni, mindenhonnan,
lomtárból is, és a számítógépet le kell állítani!
Ez a vírus, mely világszerte kering, eddig minden más vírusnál
kártékonyabb. Ennek veszélyét a CNN tett közzé.

--
Puszi xxxxxxx

email cím: xxxxxxxxx@yyyy.zz"

Mint láthatjuk, **ide vezet, ha a butaság szorgalommal párosul**. Bár ki tudja, az utóbbi napok **kemény hidegje után sokan még hálásak is lennének**, ha lángragyújtaná a winchestert, és az adna egy kis meleget ;-) A magyar nyelvű levélnél talán hatásosabb lehetne, ha a CNN helyett a Megasztár zsürijére hivatkoznának, na majd a V:2.0-ban lehet korrigálni.

Másik levelünk már inkább social engineering fronton mutathat újat, ahol azzal áltatnak minket, hogy **azért kapjuk a levelet, mert az MSN-ben feliratkoztunk rá**, na persze. A levélhez mellékelt linken aztán **vagy egy Windows Live profilt kapunk** meg, ami egy link hivatkozással mi mást is reklámozhatna, mint egy "kanadai" gyógyszer oldalt, Viagrával, Cialisszal és társaikkal, **vagy pedig semmi cicó, közvetlenül a gyógyszertári oldalakra mutat egy link**.

Ebből a típusból csak ma vagy tíz felett érkezett, jól láthatóan ez is egy vonal a spammereknél. A resume dettó, magára vessen, aki ilyenekre kattint, ritkán irkálnak nekünk Redmondból direktben. Szerencsére most ezekben nem találtunk semmilyen kártevőletöltésre utaló jelet, de majd hamarosan jöhet a Conflickerrel ellátott változat is.

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/879892

Kommentek:

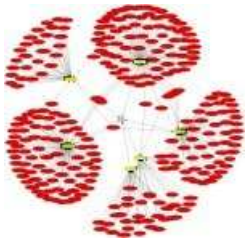
Nincsenek hozzászólások.

Új trükk a férgek elleni védekezésnél

2009.01.16. 12:25 | Csizmazia István [Rambo] | 5 komment

Címkék: hálózat felismerés támadás féreg ids

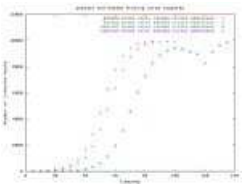
Meglepő ötlettel álltak elő a kaliforniai Davis egyetem és az Intel munkatársai. Olyan programrendszert terveztek, amely **valós időben értékelné az egyes gépeken, mi kerül többe:** a számítógépen éppen végzett feladat stratégiai értéke, vagy a fertőzés elhárítása érdekében annak hálózatról történő lekapcsolása.



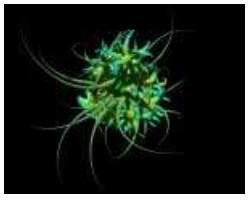
Az már most is megvalósul, hogy a gépek érzékeljék (IDS), ha egy **másik gép megpróbál ellenük támadást intézni**, de ez nem okvetlenül őrzi meg a korábbi támadások információit. Ha egy **vállalati környezetben gyanús, szokatlan hálózati tevékenységet észlelünk**, felvetődhet, hogy ez egyaránt **lehet ritka, de valós** és legális tevékenység, illetve **akár támadást is jelezhet**. A hálózati adminisztrátornak **ott a dilemma**: ha nem kapcsolja le idejében, akkor a fertőzés veszélyeztet; ha pedig lekapcsolja a hálózatról, akkor esetleg kárt okozhat a folyamatos munkákban a hamis riasztás miatti pár órás kieséssel.

Sok fejfájást okozott a maga idejében a Blaster (MSBlast)

A szellemes ötlet lényege, hogy **a gépek a rendellenes tevékenységekkel kapcsolatban információkat osszanak meg egymással**. A PC-k a hálózati adatforgalomból folyamatosan értékelik annak valószínűségét, fennáll-e egy lehetséges, most induló féregtámadás esélye. Egyetlen gyanús aktivitás még nem mond túl sokat, de **ha például száz gép közül 5-10 helyen is tapasztaljuk ugyanazt a szokatlan tevékenységet**, akkor már joggal gyanakodhatunk.



A **stratégia második része pedig egy olyan algoritmust használ**, amely összehasonlítja, hogy az egyes gépeken pillanatnyilag mi kerül többe, a számítógépen éppen végzett feladat stratégiai értéke, vagy a fertőzés elhárítása érdekében annak hálózatról történő lekapcsolása. **Ez az érték folyamatosan változik annak függvényében**, hogy mekkora a támadás kiszámított valószínűsége, és attól is, hogy az adott számítógép éppen milyen jellegű munkákban vesz részt. Ha például egy online sales munkatárs gépét csak akkor kapcsolják le, ha egy támadás már teljességgel bizonyos, akkor **ez valószínűleg több hasznot jelenthet, mint a kieső munka** egy esetleges hamis riasztás miatt. (Bár ha a féreg a vállalati vevőadatbázist lopja el éppen, akkor statisztika ide vagy oda, elkésett a a beavatkozás.) Ennek éppen az ellenkezője, ha valakinek a munkájához (szövegszerkesztés, helyi számítási vagy programozási feladatok, stb.) nem okvetlenül szükséges az online jelenlét, **őt akkor is megéri leválasztani a hálózatról, ha igen nagy a vakriasztás esélye**, hiszen ezzel a vállalatnál várhatóan nem keletkezik komoly bevétel kiesés.



Alex Dragulescu: MyDoom című festménye

A tanulmány a tavalyi év végén jelent meg *"Recent Advances in Intrusion Detection"* címmel, és **majd a jövő dönti el**, megvalósul-e és be tudja-e majd váltani a hozzáfűzött reményeket. Elképzelhető, hogy a jövő adminisztrátorai egy hatékony eszközzel lesznek gazdagabbak.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/881235

Kommentek:

Maestro 2009.01.16. 13:14:19

ötletes,

Salvia Divinorum (törölt) 2009.01.16. 14:14:50

Vállalati környezetben egyszerűbb lenne felrakni egy linux disztribúciót, akkor nem kell ilyenekkel szarozni

mnmnbkhj 2009.01.16. 14:25:08

Majd meglátjuk. Persze ez amerika, mire ideér az még...

mindentől függetlenül 2009.01.16. 14:50:48

miezasokerőspaprikaaképen?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.16. 15:10:53

Szia Mindentől függetlenül!

Paprika januárban? ;-) Ha ráböksz, akkor ki tudod nagyítani a képet. Az ábra egyébként a Nachi féreg egy honeypot elleni támadásának elemzésekor készült, annak logbeli adatainak grafikus megjelenítése.

Adatvesztés - ezúttal vírus nélkül

2009.01.19. 15:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: barracuda seagate merevlemez firmware adatvesztés

Az adatvesztés réme nem csak a klasszikus biztonsággal összefüggően jelentkezhet, ide tartozik a véletlen törlés, illetve formatálás is. A kártevők is folyamatosan veszélyeztetik az állományainkat: letörlik, ellopják, elkódolják, illetékteleneknek továbbítják, stb. Mostani esetünkben azonban nincs szó kártevőről, **egy bizonyos Seagate merevlemez széria firmware hibája** okozott komoly fejfájást számos felhasználónak.

A hírek szerint több típus is érintve lehet, köztük **az 1 TB kapacitású Barracuda winchester** is, illetve még további más, 2008 decemberében gyártott modell, például DiamondMax 22, Barracuda ES.2 SATA illetve SV35. A felhasználók lassulásra, lefagyásra, egyes esetekben pedig adatvesztésre panaszkodtak. Ez **a használt operációs rendszertől függetlenül jelentkező** probléma volt, Vistások éppúgy voltak az áldozatok között, mint a Linux illetve OS X juzerek. **Bár a felhasználói panaszok számos esetben sérült, elveszett, elérhetetlen adatokat jelentettek, a gyártó szerint nem léphetett fel adatvesztés a firmware hiba folytán.**

Mindenesetre a Seagate egy telefonszámot bocsátott a bajbajutottak megsegítésére, valamint emailen is várja a pontos típusszám, gyáriszám és firmware verzió megjelölésével a hibajelentéseket. **Igéretük szerint az adatvesztéses esetekben segítséget fognak nyújtani az ügyfeleknek** (ezek szerint elismerik, hogy mégis van?!), a továbbiakban pedig az azonnali firmware frissítést tanácsolják, ami megoldja a jövőbeni problémákat.

Nem lehet elégszer hangsúlyozni az adatmentés fontosságát, azonban egy dolog itt is felvetődik *(mint ahogy a hóekevezetők hogyan jutnak el reggel a munkahelyükre; vagy ha a repülőgép feketedoboza mindent kibír, miért nem készítik az egész gépet ebből az anyagból; illetve ha a macska mindig talpra esik, és ha a vajas kenyér mindig a vajas felére esik, akkor egy macska a hátára kötött vajaskenyérrel melyik oldalán landol majd a földön? gondolatmenetek nyomán)* **mi van, ha valaki a mentését éppen pont egy Seagate Barracuda 1 TB merevlemezre végezte?**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/888593

Kommentek:

Nincsenek hozzászólások.

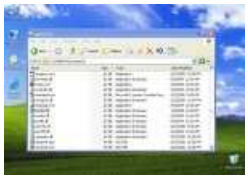
Itt az idő erős jelszót választani

2009.01.20. 15:01 | Csizmazia István [Rambo] | 5 komment

Címkék: frissítés jelszó erős conficker

Sokszor és sokat vétkezünk a biztonság terén, többek közt **a megfelelő minőségű jelszó kiválasztása okoz gondot sokaknak**, és akkor a kívánatos legalább negyedéves cserélgetésről még nem is ejtettünk szót. Pedig a Win32/Conficker féreg megadja az apropót hozzá: **nem csak a befoltozatlan** MS08-067-es biztonsági közleményben ismertetett Windows sebezhetőség a lehetséges gyenge pont, de **a rendszerszintű megosztásokhoz használt túl egyszerű, és így a féreg által szótárral könnyen kitalalálható jelszavak** is.

Egyes jelentések szerint már ausztriai közhivatalokban, kórházakban, bútorboltokban is felbukkant, és tömeges elterjedésétől tartanak az F-Secure webblogja szerint is, bár valószínűleg **a 9 millió darab megfertőzött számítógép csak egy saccolt adat**. Voltak incidensek ausztriai magánbankban, sőt Bulgáriában minisztériumi valamint rendőrségi gépeknél is okozott kalamajkát. A **frissítési hajlandóság tehát csak az egyik** fontos probléma, amit nem is szabadna halogatnia senkinek. Mindenesetre vállalati környezetben rendkívül bosszantó lehet, ha a **sűrű jelszópróbálgatás miatt valódi, legitim juzereket zár ki a hálózat** a sikertelen kísérletek miatt - itt külön utánajárás, beállítgatás szükséges, hogy az illető ismét munkába tudjon állni. Persze ennél már csak egy rosszabb, ha a gyenge jelszó miatt mégis sikerül a kártevőnek belépnie a nevünkben.



A Conficker - aminek immár saját Wikipédia szócikke is van - rendületlenül tör előre és **működéséhez Metasploit egyik modulját is felhasználták** a McAfee kutatói szerint.

Vagyis a javítófoltok letöltése és futtatása, valamint a megfelelően beállított és frissített antivírus mellett azért érdemes egy kis időt szánni a szofisztikált jelszóválasztásra is, ingyen van, és nagyon úgy tűnik, rendbetételét, **beállítását már csak ezért sem érdemes sokáig halogatni a történtek láttán**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/890558

Kommentek:

cworm (törölt) 2009.01.21. 11:32:48

Az ilyen szótárazós férgek általában csak angol szavakat tartalmaznak, nem? Vagy ha kifogytak belőlük, elkezdik őket variálni?
Tehát ha valaki pl nemlétező szavakat, esetleg mondatokat használ jelszónak, az jóval védettebbnek érezheti magát, vagy nem?:) Főleg ha mondjuk magyar vagy más, nem angol szavakat használ.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.21. 11:59:13

Hali!
Ez így van, az esélyeink jobbak a nyelvi elszigeteltségünk miatt. Azért a legtutibb, ha mindenből: kisbetű, nagybetű, szám, és egyéb írásjel is fel van használva hozzá jó hosszan, és jól összerázva, nem keverve ;-). Az egyediség, a különcség, a túlfejlett paranoia itt kimondott haszon.

A feltörés első lépése szokott a szótáralapú lenni, ha ennyi is elég a sikerhez, addig nem is lépnek tovább a sokáig tartó egyéb módszerek felé, pl. bruto force, stb.

És elvileg akármilyes királycsászár jelszavad van, időnként negyedév, félév, de legalább évente érdemes cserélni, pl. felnyomják a hivatalt, vagy a szolgáltatót, nem fog sietni beismerni az incidenst, a te "sdkjh(=76ugkLéLLp+!%553" jelszavad pedig akármennyire furmányos, ott lehet az SQL adatbázissal együtt a támadó ölében.

r@ek (törölt) 2009.01.21. 15:18:46

"a te "sdkjh(=76ugkLéLLp+!%553" jelszavad pedig akármennyire furmányos, ott lehet az SQL adatbázissal együtt a támadó ölében. "

...amitol persze nem esek ketsegbe, mert azert egy 23 karakteres salted hash feltoresere korulbelul semmi esely nincsen :-DDD

lacyc3 2009.01.24. 16:32:18

Viszont van md5 hash adatbázis, ahova csak becsurran az md5 és kicsurran a jelszó..

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.27. 11:20:46

Esetleg ideje jelszó helyett megfelelő iPhone rázási módszert választani:
www.hirado.hu/Hirek/2009/04/27/10/Nem_mindenki_orult_.aspx

Eljött a hamis rendszerüzenetek kora

2009.01.21. 15:35 | Csizmazia István [Rambo] | 1 komment

Címkék: usb eset autorun egyedi mentesítő conficker

A tegnapi postban sok mindenről szó esett már **a Conficker féreg kapcsán, kivéve talán egyet, hogy az Autorun folyamat manipulálásával** külső USB eszközök révén is tud fertőzni. A kártevő készítői nem spóroltak az ötletekkel, és egy olyan **lehetfinom social engineering trükköt is bevetettek**, ami csak keveseknek fog feltűnni.

A mai kártevők készítőit senki nem nevezheti kontároknak, szó sincs fércmunkákról, tudatos és **tervszerű fejlesztés, programozás zajlik**, sokszor még a csalinak szánt alkalmazások vonzó, esztétikus külsőt is kapnak - ezt már sokan megtapasztalhatták a hamis antivírus programok esetében. Üveghatású gombok, gyárinak ható menüstruktúra, igazinak tűnő weboldal. Igen jelentős erőfeszítéseket tesznek továbbá, hogy minél nehezebb legyen mentesíteni a megfertőzött gépeket.

Mai történetünk még ennél is kicsit továbbmegy, a Conficker féreg a fertőzött USB egység behelyezése után Windows Vista gépen próbálva **egy az eredeti rendszerüzenethez hasonló, de hamis ablakot jelenít meg**. Az extra sor pedig nem mást tesz, mint **lefuttatja a kártevőt az adott gépen, és ebben a felhasználó maga segít neki**.

Úgy tűnik, nem csak az erős jelszavak választásának és a gátlástalan, operációs rendszer által használatosra megszólalásig hasonlító **megtévesztő rendszerüzenetablakok kora jött el** (elismerem, nem egy egyszerű mondat ez;-), de az összes külsős eszköz autoplay, autorun futtatási lehetőségeinek azonnali korlátozásának és megszüntetésének időszaka is.

Ehhez tippeket az alábbi postban és kommentjeiben is lehet találni. **A jelentős mennyiségű fertőzés miatt** pedig az ESET egy külön mentesítő segédprogramot is a kibocsátott a nagyközönség számára, amelynek segítségével **a Conficker által megtámadott Windowsos gépeket lehet megtisztítani.**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/893240

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.22. 10:14:56

További háttérinfo Conflickerről, németül tudóknak:
www.eset.at/blog/1576

Emelkedik a fertőző weboldalak száma

2009.01.22. 14:00 | Csizmazia István [Rambo] | 3 komment

Címkék: spam statisztika weboldal letöltés kártevő fertőző websense

A WebSense felmérése szerint a népszerű, és nagylátogatottságú weboldalak mintegy 70 százaléka volt már érintve kártevő terjesztésben. A statisztika alapján azt is láthatjuk, évről évre romlik a helyzet.

A "biztonságunk érdekében csak megbízható weboldalakat látogassunk" szlogen úgy tűnik, értelmét vesztve végleg kiment a divatból. Az Alexa.com szerinti Top100 weboldalak **fertőzöttsége az előző féléves időszakhoz képest 16, míg az egy évvel ezelőtti értékhez képest 46 százalékkal növekedett**. Legitim webhelyek ellen sokféle módszerrel tudnak támadást intézni, és kártevőket terjeszteni a bűnözők. A repertoár a fertőzött bannerhirdetéseken át az ellopott bejelentkezési adatok birtokában feltöltött rosszindulatú kódokon át egészen az SQL kódbefecskendezéssel végrehajtott IFRAME-es akciókig vezet, és **még ennél is szélesebb palettán** mozoghat.

Sajnos **továbbra sem javul a kéretlen levelek aránya a valódiak számához képest, itt 85 százalékos** értékét mérték, ami gyakorlatilag azt jelenti, minden 100 levélből ennyi a szemét, ami roppant magas. Természetesen a kéretlen levélszemét jelentős része (mintegy 90%-a) igyekezett **URL link segítségével valamilyen kétes, csaló vagy kártevőletöltést végző oldalra irányítani** a linkre kattintókat. Az elektronikus levelek mindössze 6 százaléka volt adathalász célú támadáshoz köthető - ez ugyan 33%-os csökkenés a 2008-as esztendő második félévéhez képest -, de azért összességében ez sem kis szám, és ugya tudjuk, hogy elég, ha csak minden századik-ezredik ember dől be a csalásnak, a bűnözőknek még úgyis búsásan megéri.

Ugyanezen időszak alatt a pornográf témájú spam üzenetek aránya nem emelkedett látványosan, "mindössze" 9 százalék volt. Az adatok szerint a rosszfiúk ehelyett **kiemelt erőfeszítéseket tettek az adatlopó trójaiak terjesztése és a DNS mérgezéses támadások irányába**.

A jövőben is érdemes tehát vigyázni, és addig is csak megbízható weboldalakat látogassunk ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/895276

Kommentek:

cworm (törölt) 2009.01.22. 17:56:01

Várom már mikor jelennek meg az olyan blogok, amik ilyen antivirus blognak álcázzák majd magukat, de közben az internetbűnözők állnak mögötte és hamis infókat szórnak szét, hogy később a user még az addig megbízhatónak hitt cégek mondanivalójában is elkezdjen kételkedni, és végleg magára maradjon a weben... vagy hülyeséget vizionálok?:)

Vidi Rita · http://www.hosnok.hu 2009.01.30. 15:56:08

Igen... :)
Mivel kissé nagy munka ilyen blogot üzemeltetni, ez nem éri meg a bűnözőknek...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.23. 11:45:45

2008-ban jelentős szerepet játszottak az SQL injectionnal megfertőzött weboldalak a kártevőterjesztésben:
jeremiahgrossman.blogspot.com/2009/02/sql-injection-eye-of-storm.html

Kell-e nekünk Autorun?

2009.01.23. 16:15 | Csizmazia István [Rambo] | 30 komment

Címkék: windows usb idiótaság autorun conficker

Már napok óta csak ~~a mamára~~ a Confickerre gondolok mindig, meg-megállva. Már a korábbi évek Sony rootkites botrányainál is látszott, hogy ez **az Autorun akkor jó, ha már jól ki van kapcsolva, mondhatni "a halott Autorun a jó Autorun".**

Nem igazán volt jellemző az utóbbi években, hogy a Sircam, LoveLetter, Blaster és hasonló világszerte nagymértékben elterjedt kártevő **ennyire magára magára irányítsa a figyelmet**, úgy tűnik, ez most mégis sikerül a Confickernek. Az utóbbi napok postjai nálunk is erről a témáról szóltak, és az események miatt az ESET is megjelent egy egyedi mentesítő segédprogrammal, **amit ajánlunk jó szívvel.**

Sokan az események értékelésekor úgy gondolják, **nahát ez a csúnya Microsoft MS08-067 sebezhetőség, ez az oka mindennek**. Pedig a valóság inkább közelebb van ahhoz, hogy az Autorun "feature" sokkal jobban rákfenéje a kialakult helyzetnek, mint az előbb emlegetett sérülékenység. Ha pedig komplexen vizsgáljuk a problémát, akkor **több dolog is párhuzamosan okozója** a mostani káosznak. A bekapcsolt Autorun mellett a frissítési hajlandóság és gyorsaság alacsony szintje, a fájlmegosztások elégtelen biztonsága, de persze a gyenge admin jelszavak is említhetők, és **lehetne még hosszan sorolni**. A nem megfelelően elvégzett vagy egyszerűen kihagyott IT jellegű feladatok aztán idővel szépen visszaütnek.

Kezeket a paplan fölé, éljenek a csajok, no meg a "védd az erdőt, egyél hódot" jegyében mindenki inkább kapcsolja ki az automatikus futtatást az USB-e eszközeinél - olvashatjuk a jótanácsokban. **Aztán a végrehajtáskor derül csak ki, ez a leírás nem kapcsolja ki teljesen**, mégsem tökéletes megoldás, további kézi berhelések kellenek a nyugalomhoz. **Éppen emiatt adott ki a CERT egy a kártevő elleni védelemre kihegyezett összefoglalót,** hogy a kialakult helyzetben ezzel is segítsen a felhasználóknak.

Nyilván belejátszik ebbe a tömeges fertőzésbe valamennyire az is, hogy **míg egy autótulajdonosnak kell valamennyire érteni az autójához (nincs jogsi kötelezően fejbetöltött és levizsgázott ismeretek nélkül)**, ezért mondjuk nem rak kockacukrot vagy vizet a saját benzintankjába, **ám egy számítógép felhasználó a legnagyobb nyugalommal ül oda a minimálisnál is kevesebb körültekintéssel, tudással, odafigyeléssel**, pedig pár egyszerű alapszabályt muszáj lenne nekik is betartaniuk. Noha **eleinte úgy tűnik, ez csak és kizárólag az ő érdeke lenne**, azért messzebbről nézve összességében mégis mindannyiunké.

Továbbá reménykedjünk, hogy **a következő Windows operációs rendszer esetleg már alapértelmezetten KIKAPCSOLT Autorunnal fog érkezni**. Reménykedni szabad, azt a törvény nem bünteti ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/897812

Kommentek:

Sákif za morro? 2009.01.23. 19:59:27

Ezt én sohase értettem, hogy a kibaszott vindóz miért akarja kitalálni hogy én mit akarok csinálni?! Miért nem dönthetem én el? Ill. miért kell először kikapcsolni azt amit ő szeretne, és utána az enyémet megcsinálni? Miért? Miért? Miért? :-S

Charlie Brown 2009.01.23. 20:22:21

Egy ideje én is tűzzel-vassal kapcsolom ki az autorunt, ahol érem.
Így viszont bizonyos másolásvédett dvd filmek nem hajlandók lejátszódni, lévén a titkosításukat az autorunnal a lemezről lefutó cucc kezeli le. Az meg valami rejtett cifraság, kézzel nem futtatható. Mindegy, aprócska áldozat a biztonság oltárán.

amondó (törölt) 2009.01.23. 20:24:49

Én jót derülök mindig, amikor autorun.inf-et találok egy usb-s meghajtón, ami az ugyanazon a meghajtón található E:\Recycle.bin\akármiservice.exe nevű rejtett rendszerfájlra mutat. Aztán szépen törlöm a fenébe, linuxszal persze.

Amikor egyszer az összes családi wines gépről kellett leirtani egy ilyet, akkor nem derültem annyira.

És ez nem a felhasználók hibája. Miért kéne a felhasználónak egy rejtett feature-ről tudnia, amire ráadásul nincs is szüksége? Ha a felhasználó elindítja a levélben kapott nudebritney.jpg.pif.exét, akkor ő a hibás, na de itt, honnan a retkesből tudja, hogy a fényképelőhívásnál a sd-kártyájára rákerült egy rejtett, törölhetetlen fájl, ami automatikusan terjed, amint berakja a gépébe, mert a windows olyan jófej, hogy lefuttatja kérés nélkül?

amondó (törölt) 2009.01.23. 20:26:24

@Charlie Brown:

És ha a filmet a boltba visszaviszed, és megmondod, hogy nem szabványos dvd, mert nem játszódik le a sima dvd-lejátszó programmal, te meg nem vagy hajlandó ismeretlen szoftvert telepíteni a gépedre?

Royaljerry · http://be.net/royaljerry 2009.01.23. 20:48:04

@Charlie Brown: parancssort (Command Line) elindítod a DVD-meghajtón, és beírod ugyanazt a sort, ami az autorun.inf

filban található, kapcsolókkal együtt.

dark future · http://www.andocsek.hu 2009.01.23. 20:56:26

Egyetértek a posttal, az autorunt KI KELL KAPCSOLNI.

Pl. így: www.webdiag.hu/autorun_off.zip
(a csomagban egy registry-javító bejegyzés van, szimplán csak kattintani kell rá, garantáltan vírusmentes)

dark future · http://www.andocsek.hu 2009.01.23. 21:04:58

A pendrive-okat, SD-kártyákat meg tessék csekkolni (legegyszerűbb Total Commanderrel, ha be van kapcsolva a rejtett fájlok megjelenítése funkció). Ha találtok autorun.inf-et, az gáz, végig kell nézni az összes olyan gépet, amiben járt a kütyü.

Ha egyszer már felkerült a gépre a cucc, és akkor nem fogta meg a víruskereső, akkor már mindegy, leszedni általában úgysem tudja. Meg sajnos a user sem, kár is próbálkozni. A rendszervisszaállítás néha szokott segíteni, de csak ritkán, mert bootolás után a legtöbb vírus azonnal bekerül a memóriába, és nem nagyon hagyja magát kiirtani. Ha valaki vírustémadásra gyanakszik, legjobb, ha hozzáértő segítségét kéri. Általános receptek sajnos nincsenek, csak céleszközök (pl. CD-lemezes XP), meg sok-sok tapasztalat.

cuebler 2009.01.23. 21:08:42

nekem most valami resycled mappa jelent meg az összes meghajtómon... mondjuk tudom az okát, szántszándékkal mentem fel egy cracker honlapra...

aqswdefr 2009.01.23. 21:26:00

"(a csomagban egy registry-javító bejegyzés van, szimplán csak kattintani kell rá, garantáltan vírusmentes)"
Hahaha, becsszó? :)

-=Z=- 2009.01.23. 21:33:42

Namost én eztet úgy csináltam meg, hogy minden pendriveomon készítettem a gyökérben egy "autorun.inf" nevű könyvtárat, amit írásvédetté tettem. Most gyakorolhatnak a vírusok. Ha eltűnne a könyvtár csak észrevenném, akármilyen is a gép beállítása.
:-)

MP 2009.01.23. 21:34:39

Szerintem a helyzet nem ennyire egyértelmű. Egy átlag felhasználónak az autorun nagy segítség. Az más kérdés hogy ha egy gépszerelő elmegy hozzá s feltesz vírusirtót tűzfalat egyebet akkor azt nem kell letiltania vagy felülbírálnia. De egy ilyen helyzetben a felhasználót hibáztatni nem tisztességes. Az autós példánál maradva a vizsga után mindent el szoktak felejteni. Az átlag autós max azt tudja hogy milyen folyadékot hová kell tölteni.

Sákif za morro? 2009.01.23. 21:50:47

@Moneymaker: Kurvaanyád!

Charlie Brown 2009.01.23. 21:52:08

amondó:

Akkor az eladó készségesen megmutatná a doboz hátulján a figyelmeztetést, hogy a lemez másolásvédett. Ha még mindig erősködnék, akkor visszavenné, nekem meg nem lenne filmem, az pedig nem jó, mert én csak olyan filmet veszek meg ami

nélkül rosszul alszom. :)

Royaljerry:

Bizisten nem emlékszem, mert régen volt és hamar túlléptem a kérdésen, de a megoldás nem volt ilyen triviális. Ha jól emlékszem, a lemezt a gépbe rakva nem látszott semmilyen autorun.inf, sem a futtatandó kód. Nyilván ennek érdekében volt ott minden, második session, korrupt tartalomjegyzék, satöbbi. A dolog természete onnan volt látható, hogy az automatikus futtatás ki-be kapcsolásával ment illetve nem ment a lejátszás.
Ha eszembe jut, melyik film volt az, meg fogom nézni közelebbről.

Sákif za morro? 2009.01.23. 21:52:16

@-=Z=-: Az autorun.inf nem fájl véletlenül? Amúgy az ötlet nem rossz. :-) Én a munkahelyi számítógépes buziságok ellen csináltam ilyet. Egyedül az én gépemről lehet pronó oldalakat látogatni. :-)

dark future · http://www.andocsek.hu 2009.01.23. 21:55:21

@aqswdefr:
Nem :-) Sikerült 262 bájtban vírust írnom :-)

Gyulimali 2009.01.23. 22:10:13

@dark future: Biztos az csak a bootloader, és a 'zinternetről tölti le a vírustrójaiadvárét! :-)

amondó (törölt) 2009.01.23. 22:18:47

Az autorun egy elavult, nehézkes fájlrendszer terméke szerintem: az, hogy a felcsatolt meghajtó egy tetszőleges betűjelet kap, azt eredményezi, hogy az egyszerű felhasználó nem fog rájönni, hogyan kell a lemez tartalmához hozzáférni. Win 3.11 alatt még kézzel kellett beírni, hogy D:\install.exe (és nem is biztos, hogy D, lehet E, F... is!), win 95-től meg a sajátgépben kellett turkálni.

Erre, ahelyett, hogy valami tiszta, szép új megoldást találnának ki, belehekkelték a windowsba, hogy nosza indítsa el azt, amit az autorun.inf-ben talál. Az eredmény nyilvánvaló.

A normális megoldás az lett volna, ha a betett lemez/floppy/pendrive ikonja, neve feltűnően megjelenik berakáskor (pl az asztalon), és a felhasználó azt észrevéve, maga indítja el a rajta lévő fájlt. Így a kicsit is odafigyelő felhasználó láthatná, hogy EXÉ-t indít vagy JPG-et nyit meg.

Az OSX alatt már ősidők óta az asztalon jelenik meg a meghajtó ikonja, az újabb linuxokon is.

Ezek után mindenféle utólagos megoldás (autorun kikapcsolása, vírusellenőrzés) csak félmegoldás lehet. És utálom, hogy 1-2 nap szükséges ahhoz, hogy egy windows rendszert hülyebiztossá tudjak tenni.

Androsz 2009.01.23. 22:25:12

Bocs, hogy elemi dologról kérdezek, de csak most jöttem rá, hogy én itt valamivel nem vagyok tisztában. Azért nem foglalkoztam sokat az autorunnal, mert egyrészt valamennyire ki van kapcsolva a gépemen, másrészt én baromira utálom, ha a rabszolgám izgágáskodik, ezért oda szoktam figyelni a gép manővereire. De mégis felmerült bennem a kérdés, hogy ha van is a lemezen autorun.inf, de a lemez behelyezésekor az az ablak jön elő, hogy mondjam meg szépen, mi a tervem a lemezzel a következők közül, akkor az autorun.inf még nem futott le, igaz? Annál is inkább hiszem ezt, mert én szépen megnézem, melyik exe van a fájlban indításra előjegyezve, és ha az tetszik nekem, akkor kézzel elindítom. Szóval, a jelek alapján, akkor most nálam ki van kapcsolva vagy nincs ez a hülyeség?

Charlie Brown 2009.01.23. 23:52:07

Androsz:

És hogy nézed meg az autorun.inf tartalmát? Ahhoz előbb meg kell nyitnod a meghajtót. Márpedig az autorun fő veszélye nem az, hogy bedugáskor rögtön lefut valami (alapértelmezés szerint az usb eszközökön hiába van ott, nem fut le automatikusan az

autorun.inf tartalma, ellentétben az optikai lemezekkel!), hanem hogy az autorun.inf fájlban át lehet definiálni az történéseket (vagyis azokat a parancsokat, amik a jobbgombos context-menüben is olvashatók), valamint hogy mi legyen az alapértelmezett (a context menüben vastag betűvel szedett) parancs, ami duplakattintásra végrehajtódik. Tehát pl meg lehet adni, hogy a "Megnyitás" parancsra az történjen, hogy lefut egy rejtett exe, és csak azután nyissa meg a meghajtót az intézőben. Ilyenkor elég, ha a Sajátgépben duplakattintással próbálsz megnyitni egy usb meghajtót, vagy a csatlakoztatáskor felkínált menüből kiválasztod a "megnyitást", és már meg is vagy fertőzve. Nem fut le semmi automatikusan, te magad futtatod az exét, csak épp nem tudsz róla!

Ha a viszont a meghajtót a Sajátgép címsorának legördülő menüjével nyitod meg, akkor nem fut le az autorun.inf-ben definiált "megnyitás" szekvencia, tehát ha nincs írmagostul kiirtva az autorun a gépen, akkor javasolt ezt használni duplakattintás helyett. Másik lehetőség hogy minden usb meghajtót pl. Total Commanderben nyitsz meg, az sem futtatja az autorun tartalmát, ráadásul figyelmen kívül hagyja a Windows rejtett fájljait, akkor is mutatva azokat, ha az intézőben nem látni őket -sokszor épp mert a féreg letiltotta a láthatóságukat. A fertőzés egyik legbiztosabb jele, hogy az intézőben nem lehet látni a rejtett fájlokat, és hiába is próbálod bekapcsolni a láthatóságukat.

The Great Destroyer 2009.01.23. 23:56:46

Az a legnagyobb gáz, hogy az autorunt nem lehet kikapcsolni...
Az autorun ugyanis az automount része.
Amikor berakunk egy cd-t, vagy bedugunk egy pendriveot, akkor a felcsatolással együtt(amikor megjelenik a sajátgépben a meghajtó, vagy a lemez) lefut az autorun, nem lehet őket szétválasztani, amikor letiltod az autorun "szolgáltatást", akkor csak azt tiltod meg, hogy az autorun.inf fileban megadott opciók szerint csináljon valamit a meghajtón lévő fileokkal.
Ha tényleg ki akarod kapcsolni, akkor azt csak a biztonsági házirend módosításával tudod megtenni, de akkor viszont muszáj lesz a helyi lemezkezelésből le/fel csatolgatni a meghajtókat(pendrive, cd, stb...).
Ebben az egészben az a mókás, hogy kb egy éve néhány ismerősömmel (hardcore kockák) azon röhögtünk, hogy a windows összes biztonsági résének 99%-a az úgymond kényelmi szolgáltatásokat érinti, mostanra kiderült, hogy tényleg így van.

Charlie Brown 2009.01.24. 00:11:05

atka:

"amikor letiltod az autorun szolgáltatást, akkor csak azt tiltod meg, hogy az autorun.inf fileban megadott opciók szerint csináljon valamit a meghajtón lévő fileokkal"

Pont ez a cél, nem? Hogy ne hajtsa végre az autorun.inf tartalmát, sem csatoláskor automatikusan, se máshogy. Így viszont nem értem, mit értesz "lefutó autorun" alatt, ha nem az inf-ben definiált dolgok futtatását?
Nálam kis lett kapcsolva az autorun a policiy editorban, ott vigyoroghat a görénység az usb meghajtón, nem fut le, és mégsem kell kézzel föl-le csatolnom a meghajtókat. Akkor most hogy is van ez?

The Great Destroyer 2009.01.24. 00:27:37

Ok, akkor érthetőbben.
Az autorun tulajdonképpen egy alkalmazás, ami minden esetben lefut, ha a windóz magától felcsatol egy eszközt a filerendszerbe, az autorun.inf tartalma minden esetben értelmezésre kerül, ezután a benne hivatkozott programok a megadott paraméterekkel elő lesznek készítve az indításra.
Hiába nem indul el egy adott alkalmazás, attól még bekerül minden hozzátartozó szutyokkal együtt a virtuális memóriába.
Mivel a M$ nem vitte túlzásba a biztonság kérdését '94ben(főleg, mivel még csak nem is sejthették a pendrájv korszakot, amikor mindenki mindenféle vackot beledugdos mindenféle lyukba), amikor fejlesztették az NT kernelt(ez van moszt a zikszpé és a viszta alatt is, csak picit felpiszkálva) és azóta sem sikerült elfogadható szintre csökkenteni a kockázatot.
Az autorun csak az automounttal együtt irtható le teljesen, mivel egy és ugyanaz a rendszerszolgáltatás mind a kettő, attól, hogy egy elb...ott cuccnak letiltod egy ficsörjét, attól még ugyanolyan elb...ott cucc marad ugyanolyan biztonsági résekkel.

VaZso 2009.01.24. 00:31:19

Soha nem értettem, hogy miért hiányzik az összes újabb pendriveról az "írásvédő kapcsoló".

Többek között éppen a vírusok miatt, ugyanis többször van szükségem turkálni egyes gépek rendszerén, ahol így nagyon sokminden megtörténhet... :(

Ugyan van a driveon live Linux, de azért mégsem ugyanarra találták ki mint egy nyamvadt írásvédő kapcsolót.

Az egyik leglényegesebb és biztonsági megfontolásból legfontosabb dolgot hagyják ki... és senkinek fel sem tűnik.

□.A.Lacky 2009.01.24. 00:59:17

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveAutoRun

illetve a

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoDriveTypeAutoRun

értékek legyenek mind 255 (FF).

Ha nincsenek ilyenek, akkor létre kell hozni (duplaszó, azaz DWORD). Ezzel minden autorun le lesz tiltva. Persze én kötelezném a Microsoftot, hogy ezekkel az értékekkel szállítsa a rendszert, és én majd visszaállítom, ha akarom.

Itt egyébként az érték minden bitje egy meghajtót jelent sorrendben, és amelyik 0, ott lehet Autorun-t végrehajtani. Mert bár az autorun.inf írásvédett könyvtár létrehozása is teljesen hatékony, de azt minden esetleges új meghajtóra fel kéne tenni.

Miután ezeket az értékeket beállítottam, simán töröltem az összes autorun file-t. Addig hiába próbáltam, mindig visszajött.

verghaust (törölt) 2009.01.24. 01:20:25

conficker b+

Charlie Brown 2009.01.24. 03:14:33

atka:

Hol lehet az automount és az autorun elválaszthatatlan egységéről bővebben olvasni? Kicsit túrtam már a Guglit meg a Technetet, de eddig nem találtam erről semmi releváns infót sehol.

espadazo - Játékbolt: · http://aruhaz.nettfilm.hu 2009.01.24. 09:11:06

Én feltettem egy víruskeresőt, ami minden ilyen lehetőségnél megkérdi, hogy engedem-é, avagy sem. Én meg nem engedem.

Androsz 2009.01.24. 15:58:41

@Charlie Brown: Azt valóban kihagytam, hogy én gyakorlatilag kivétel nélkül mindig Total Commanderben kezelem a háttértárakat, ami ezek szerint kisebb kockázatot jelent. Viszont a sajátgépes tanácsot köszönöm, még nagyon hasznos lehet.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.02. 13:46:54

Hogy kikapcsolt Autorunnal jön-e, azt nem tudjuk, de hogy szabadon kikapcsolható UAC-cal, az tuti :-)
www.hwsw.hu/hirek/37984/microsoft_windows_7_biztonsag_user_account_control_jogosultsag.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.30. 15:32:05

Észbekapás esetének fennforgása van - végre-valahára:
index.hu/tech/szoftver/2009/04/30/korlatozza_az_automatikus_futtatast_a_windows_7/

A PC ügyvédje

2009.01.26. 16:31 | Csizmazia István [Rambo] | 17 komment

Címkék: szerződés analízis gyanús eula eulalyzer

Ha feltennénk a kérdést, **vajon mindenki alaposan elolvassa-e a szoftverekhez mellékelt felhasználói szerződést, nem kellene felnyújtott karerdőtől tartani**. Mindenesetre kipróbáltunk egy érdekes megoldást, ahol **némileg automatizálva hamar kiderülhetnek** a szerződésben szereplő nagyobb disznóságok.

Az EULAlyzer a SpywareBlaster készítőinek munkája, és nyilván ők is megtapasztálták, vannak esetek, amikor a kilométer hosszú felhasználói szerződés (End User Licence Agreement) **apróbetűs részeibe kétes dolgokat bírnak elrejteni a fejlesztők**. Aztán ha kiderül, hogy nem túl etikus vagy nem egészen tisztességes dolgokat művel az adott szoftver, akkor **széttárják a karjukat: Hja kérem, a felhasználó elfogadta, a felhasználó kattintott**, mi nem tehetünk semmiről.

Mint a nevéből is kikövetkeztethető, az EULA-t (End User Licence Agreement / végfelhasználói licenc szerződés) képes átfutni, s abból a gyanús szavakat, mondatokat kiemeli. Így nem kell fáradni a sokszor többszáz soros szövegek átolvasásával, amit a legtöbben soha nem is tesznek meg.

Ez most tiszta, de sose felejtsük el, egy telepítőben - különösen ismeretlen programnál, vagy ismert program kétes helyről való letöltésével kockáztatjuk, hogy az már esetleg kártevőt is tartalmazhat

Vicces módon ez az EULA sem kerülhetne be a Guiness rekordok évkönyvébe, mint a legrövidebb licenc szerződés

Ennek persze több oka is lehet, mint például **a nyelvtudás teljes hiánya, de azért közepes angol tudás birtokában is beleütközhetünk néhány olyan kacifántosan megfogalmazott kitételbe**, ami az értelmezést egyáltalán nem segíti. És persze **ott van még a jó öreg lustaság is**, rákönyöklünk a Next gombra, és minden mindegy alapon települ fel az illető program.

Akár egy víruskeresőhöz, rendszeres adatbázis frissítések jelennek meg

A program képes kimásolni a szerződés szövegét a telepítőből, de **természetesen kézzel is beilleszthető a szöveg a vágólapon keresztül**, ez utóbbi akkor lehet hasznos, ha például az EULA részletei csak a weben, online érhetőek el.

Most épp egy Macromedia szerződés van a munkapadon

Csak két közepes fokú figyelmeztetést kapunk, rendbenlévőnek látszanak a dolgok

Az **analízis eredménye a készítőknek is elküldhető a programból**, ami egyrészt egy folyamatos visszajelzés a számukra, ami hasznos a fejlesztéshez, illetve akkor is profitálhatunk belőle, ha valamilyen problémás szöveggel találkozunk, ami feladja az értelmezési leckét, vagy nagyon gyanúsnak tűnik.

Próbaképp betöltöttük a MyWebSearch licencét is, és jól láthatóan nagyságrendekkel több és mélyebb warning keletkezett

Bár a program használatának **vannak gyenge pontjai**: csak angol nyelvű szerződéseket elemez, nem pótolja a profi szakértelemmel rendelkező szoftverjogászokat, továbbá a hazug szoftverlicencek elemzésével csak a telepítés után döbbenünk rá a valóságra, azért **sok esetben valóban hasznos lehet az átlagfelhasználók számára, és ráadásul folyamatos frissítések is érkeznek a programhoz, működése pedig villámgyors**. Mi a program **ingyenes változatát nézgettük**, de fontos megemlíteni, hogy létezik egy fizetős PRO verzió is, amihez már folyamatos technikai supportot is biztosít a gyártó.

A szerződések beküldésével magunk is segíthetjük a fejlesztést

Egy összesített statisztikai nézetet is lekérhetünk az eddigi elemzéseinkről

Ide kívánkozik egy story a múltból, H. Kovács történetei következnek ;-) Egyik korábbi munkahelyemen komoly szövegszkennélési munkák néztek ki, sokezer oldalas mérnöki tanulmányok beolvastatása és karakterfelismerése volt a cél. Engem küldtek a szoftvert előzetesen megnézni, ahol nemes egyszerűséggel **azt kértem a bemutatón, csapjuk fel a karakterfelismerő szoftverhez mellékelt gépkönyvet valahol, és azt olvastassuk be**. Várakozásom ellenére nem lett se 100%, se 99%, valahol csak a kilencven százalék körül volt. Belegondoltam, hogy egy átlag titkárnőnek begépelni egy adott, akár számoszlopokat és képleteket is tartalmazó oldalt mennyi idő lenne, és egy beszkennelt oldalon milyen munka lenne az ellenőrzés, hogy hibamentes legyen. Ennek függvényében úgy döntöttem, nem javaslom főnökeimnek, hogy vásároljuk meg az akkor igen borsos áru programot.

Ezzel rímel egy picit "amikor a hóhért akasztják" címmel - a fentiek fényében - a kellően rosszindulatú ;-) **blogíró nem bírja ki, hogy magának az EULAlyzernek a licencét is meg ne vizsgáltassuk** a programmal, íme az eredmény ;-)

Végezetül ezúton **köszönjük Mrszitya nevű olvasónknak**, hogy figyelmünkbe ajánlotta ezt a programot. Ha az olvasók közül valakinek van mélyebb tapasztalata ezzel a szoftverrel, vagy hasonlót ismer, amit érdemesnek tart a többiek figyelmére, az bátran kommenteljen!

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/903556

Kommentek:

Krisoft · http://krisoft.blog.hu 2009.01.26. 17:33:56

Ez tök jó lenne, ha nem kéne installálni. Szerintem az egészet meglehetne oldani webes felületen, szebben, jobban.

lacalaca · http://cydonia.blog.hu 2009.01.26. 19:14:37

Hát igen, Linux alatt már az is hatalmas felháborodást okozott, hogy Firefox 3-hoz mellékelni merészeltek EULA-t. Aztán gyorsan átalakították about:rights lappá vagy mivé.

Mindenesetre hasznos lehet olyanoknak, akik egyáltalán felfogják, mit jelent az "I accept" gombocska, az installer lassításán kívül.

Laciii 2009.01.26. 19:17:33

A legszebb amikor az EULA a dobozban van, és persze a doboz felnyitásával elfogadod a benne leírtakat, ki van ez találva kérem.

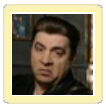
dArKhAlF 2009.01.26. 20:56:33

ez bejön

nyalógép 2009.01.26. 21:11:02

Ez mind semmi, az én esetemhez képest!
Több évvel ezelőtt rábeszélésre naívan regisztráltam egy német webáruházhoz, mint utólag kiderült úgy szólt a szerződés, hogy ha nem vásárolunk évente valamit akkor 99Euro tagdíjat vagyunk kötelesek fizetni. .[sternesammer.de] volt.
Azóta ezt mint szót is kitörölték a google-ról.

baliquez 2009.01.26. 22:06:57



Szvsz hótfelesleges. Na és akko' mi van, ha kacifántos megfogányzások vannak benne, nem installálod fel dacból? Vagy visszaviszed a boltba azzal hogy jogi aggályaid vannak? Ugyanmár.

Perillustris 2009.01.26. 23:10:50

@baliquez: te amit leveszel a polcról az élelmiszerboltban, azt mindenképpen megveszed és megeszed, akármit is olvasol a cimkéjén?

misc · http://misc.blog.hu 2009.01.26. 23:23:36

az EULÁ-ba be lehetne írni, hogy az "I accept" gombbal eladod anyádat-apádat, a családodat és a saját lelkedet a szoftver készítőinek 1 dolláros vételárért, a felhasználók 99% rákattintana.. egyébként meg nem hinném, hogy a mezei, nem üzleti célú felhasználókat bármilyen mértékben érintené az, ami egy átlagos licenszszerződésben benne van.

Hivatásos beszólóművész 2009.01.26. 23:44:16

Szerintem pont tök mind1 mi van odaírva.
Az átlag programoknál mind1 mit vésnek bele, úgysem pakolnak olyat hogy pl. Amennyiben telepíted minden nap román vendégmunkás megerőszakol, miközben egyet orálisan elégítessz ki miközben azt kell mondanod, hogy "Ó míly csodás teazsúr!"

Az olyanoknál, mint webshop, stb a felhasználási feltételeket egyszer illik átnyálazni és aki neten vásárol ezt 99%ban meg is teszi.

És különben is, olvasol vmit amit ez a gyík program kiemel, és ezért nem fogsz dvd nézni, vagy word-t használni? Esetleg vindózt telepíteni?
Kétlem...!
Fölösleges ez a program, annak jó csak, aki a közértben is ráköt az alkalmazott fejű csókára, hogy figyeljé ez a kenyér csak 95 dkg há hüjének nézel engem vagy mi van, mi, sz*rt akarsz eladni?!

Hivatásos beszólóművész 2009.01.26. 23:47:08

@Perillustris: Te agy! :D Becsülöm az ilyen tudatos váésárlókat! :D Feltehetőleg te a közértben 2-3 órát is eltöltessz, pontos összetétel, min. megőrzi: nap.hó.év tanulmányozással, és tökéletes gr/fillér összehasonlítással, elemzéssel! Mind a 200 terméknél.
Majd elégedetten távozol azzal a tudattal, hogy 3 tejen, 1 kenyeren és 20 dkg párizsin spóroltál majdnem 80ft.-t. :D

Kérdés megérte-e az a 2-3 óra!

Androsz 2009.01.26. 23:50:00

@Perillustris: Némi túlzással: igen. Én ugyanis nem vagyok sem élelmiszervegyész, sem patológus, sem minőségvizsgáló intézmény veteránja, sem más efféle beavatott. Kénytelen vagyok megvenni, amit árulnak a boltban, egyrészt mert, figyeld meg, jóformán semmiből sem árulnak annyi félét, hogy akkora gondot jelenthetne a válogatás; másrészt pedig minden élelmiszer tartalmazhat ártalmas dolgokat, amelyeket én még akkor sem fogok felismerni, ha nagybetűkkel a csomagolás elejére pingálják. Tudod, a liposzómák és a többi bűvös szó korában eltompul az ember ösztönös idegenkedése minden fennhéjázó és rejtélyes szövegeléstől.

Egyébként rendes országban nekem nem is kellene azzal foglalkoznom, hogy a termékre írva van-e valami riasztó. Azt ugyanis, ha a kereskedőben nem bízunk meg, már elbírálta volna az importőr, a behozatalhoz szükséges engedély megszerzésekor az illetékes ellenőrzés, a szúrópróbaszerűen dolgozó minőségvizsgálók, tisztiorvosi szolgálatok és fogyasztóvédők is. Nekem nem kell mindenhez értenem, arra lenne ott az állam.

Az EULA pedig egy kalap szar, miért is kellene sokáig olvasgatni? Jogászok szülték, és mérget vehetsz rá, hogy az alapján bármit rádbizonyíthatnak, valamint az elenkezőjét is, akár egyszerre. És ha nem tetszik, akkor mihez kezdj? Kell a program, nem? Már az is művészet, hogy egy tényleg működő programot találj a feladatra, még a jogi maszlagot is számításba kellene venni? Lehet, hogy eladom benne a házamat, de már eleve arra a reményre építünk, hogy a szerződést kiötlők és veled aláíratók talán sosem fognak tudomást szerezni arról a botlásodtól, hogy használatba vetted a programjukat. Tudjátok talán, hogy milyen szabályok vonatkoznak azokra, akik a biciklijüket az üzlet elé láncolva hagyják, amíg bemennek egy doboz cigiért? Vagy azokra, akik a parkoló kocsitól távolabbi automatához mennek jegyet venni? Vagy ha a villamoson akkor sem ülsz le, ha van üres hely? Nem? És mégis megteszed bármelyiket, igaz-e?

Bambano 2009.01.27. 00:07:00

Én el szoktam olvasni az eulákat, utána meg hülyének néznek, ha egyes szoftvereket nemhogy a saját, de még idegenek gépére se rakok fel...

fireman4 2009.01.27. 08:03:34

Az EULA csak azokra az esetekre vonatkozik, amikor a felhasználó megveszi a programot.

Perillustris 2009.01.28. 00:23:11

@Hivatásos beszólóművész: OFF. Őszintén, mikor vásároltál egyszerre 200 féle terméket? Én amúgy márkahű vagyok. Ami egyszer bevált, ahhoz ragaszkodom addig, amíg valamilyen objektív tény nem sarkall változtatásra. Így egy nagybevásárlás alkalmával sem kell mindent megnéznem. Mióta az árcédulán feltüntetik a kg vagy a liter árat is, ezen sem kell agyalni. Szóval igen, tudatos vásárló vagyok, szerencsére nem a beteges fajta - bár ki tudja, hol lehet határt húzni.

Perillustris 2009.01.28. 00:26:17

@Androsz: Ismétlem, nem beteges mértékben kell gondolkozni. Mikroszkópot én sem viszek a boltba.

Különben a hasonlat arra volt reakció, hogy 'baliquez' mindenképp telepíti a programot.

dis 2009.01.30. 11:39:23

@Hivatásos beszólóművész, @Androsz
én is olvasok cimkéket! [EULA-t kevésbé:)]
jó példa a mustár: többnyire van olyan ami vízből, mustármagból, ecetből és fűszerekből áll és többen amiben már van tartósító ésvagy ízfokozó ésvagy mesterséges színezék stb.
egyszer kiolvasom, utána már csak azt veszem.

@fireman4
egy csomó freeware-nek van EULA-ja. pl.: spybot sd

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.23. 10:27:36

Egy kis adalék a témához, benne olyan érdekességgel, hogy hiába olvasod el A napon az apróbetűst is, ha később B napon értesítés nélkül egyoldalúan megváltoztatja a szolgáltató. Tényleg, ilyenkor ez miért érvényes szerződés. hiszen nem írta alá mindkét fél az új feltételeket?
index.hu/tech/net/2009/02/23/1251687/

Támadási lehetőség az Apple OS X ellen

2009.01.28. 15:11 | Csizmazia István [Rambo] | 1 komment

Címkék: mac black hat injection exploit elmélet gyakorlat macintosh apple

A következő Black Hat konferencián, február 18-19-én mutatja be az olasz Vincenzo Iozzo azt a módszert, mellyel illetéktelenül kódot lehet bejuttani az Apple MacIntosh számítógépek memóriájába.

Az eljárás segítségével úgy lehet jogosulatlan szoftvereket "injektálni" a Mac-ekbe, hogy **semmilyen látványosan érzékelhető jele sem marad** az ilymódon végrehajtott támadásnak a számítógépen. (Persze egy alapos memória vizsgálat, vagy egy jó IDS kiszúrhatja.) Az már korábban is ismert volt, hogy ez operációs rendszertől függetlenül **elvileg megvalósítható**, de az OS X ellen **eddig nem létezett olyan jól működő és könnyen reprodukálható kód**, amelynek rossz kezekbe való kerüléséért aggódni kellettt volna. **Most majd kiderül, eljött-e ez az idő**.

Ha és amennyiben igen, akkor az **eredetileg törvényszéki nyomozók által használt technika** jó eséllyel pályázhat majd arra a sorsra, hogy segítségével a jövőben támadók kártevőket injektáljanak a Mac-es gépekbe.

Úgy tűnik, **lassan annyira népszerűek és elterjedtek lesznek ezek a gépek**, hogy Richard Burton Világok harca című film elején elmondott híres szavait idézhetjük: ("And slowly, and surely drew their plans against us"). És egyfelől a biztonsági programok fejlesztőinek tenni kell ez ellen, másrészt a juzereknek is el kell fogadniuk, hogy **pusztán a MacIntosh gépek használata hosszútávon nem tesz majd senkit támadhatatlanná**.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/908168

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.19. 10:04:17

Eredmények az idei Pwn20wn versenyről:
buhera.blog.hu/2009/03/19/pwn2own_mindenki_elhasalt

Törött ablakokról filozofálunk

2009.01.29. 16:56 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: microsoft windows frissítés patch ablak törött hibajavítás conficker

Terjed a Conficker, és már **sokadszorra esik szó az elmaradt Windows biztonsági frissítésekről**, amikről ugyebár a számítógép felhasználóknak kellene gondoskodni.

A Win32/Conflicker.A hálózati féreg a Microsoft Windows egyik biztonsági hibáját kihasználó exploit kóddal terjed, és azt az RPC (Remote Procedure Call) vagyis a távoli eljáráshívással kapcsolatos sebezhetőséget használja ki, **amelyet a 2008 októberben kiadott MS08-67 jelű Microsoft biztonsági javítócsomag már vígan elhárítana**, de sokan mégsem töltik és futtatják le. Egyes becslések szerint **a Windows alapú számítógépek egyharmada egyáltalán nincs frissítve**, ezért nagyon magas a veszélyben lévő számítógépek száma. Hiába vannak segítő és könnyen használható automatikus eszközök is, **hiába áradnak a figyelmeztetések, falrahányt borsó az egész**.

A minap olvastam **egy nagyon klassz cikket**, amelyben a "Törött Ablakok Elmélete" szerepelt. Mindenkinek jó szívvel ajánlom, olvassátok végig. Hadd idézzek egy picit belőle:

A városok leromlását tanulmányozó kutatók meg akarták érteni, hogy miért kerüli el a belváros bizonyos részeit szlömösödés, és hogy a közvetlen szomszédság – ugyanolyan demográfiai és ökonómiai adottságokkal – miért válik pokollá, ahová a rendőrök is félnek bemenni. Tudni akarták mi a különbség.

A kutatók csináltak egy tesztet. Vettek egy szép autót, mint pl. egy Jaguár és leparkoltatták New York Dél-Bronx-i részén. Egy rejtekhelyre vonultak vissza és onnan figyelték mi történik. Ott hagyták az autót vagy négy napig és semmi sem történt. Hozzá sem nyúltak. Ekkor odamentek, betörték egy kis oldalsó ablakát és újra elrejtőztek. Nem telt bele négy óra és az autót felfordították, felgyújtották, lecsupaszították – teljesen.

Tovább tanulmányozták a témát és kidolgozták a Törött Ablak Elméletet. Egy ablak betörik egy bérházban, de senki nem javítja meg. Úgy hagyják. Aztán valami más is eltörik. Lehet véletlen baleset, vagy nem, de szintén nem javítják meg. Falfirka jelenik meg. Egyre több sérülés halmozódik fel. Nagyon gyorsan exponenciálissá válik ez a folyamat. A teljes épület leromlik. A bérlők elköltöznek, a bűnözés beköltözik. A játszma elveszett. Mindennek vége.

Ami miatt szóba hoztam, az kétségkívül az, hogy ha elegendő mennyiségű elhanyagolt (kitört ablakú) Windows fellelhető, biztonmegérkeznek a törni-zúzni vágyók.

Bégány Attila találó mondása ugrott be erről, nem igazán szorul magyarázatra: **"Aki nem védelmezi az értékeit, az provokálja a másikat"**. Nem kellene hagyni, ne éljünk együtt törött ablakkal!

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit

- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/910557

Kommentek:

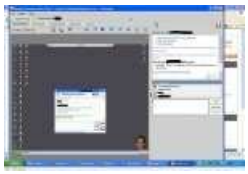
Nincsenek hozzászólások.

Obama féreg. Igazi vagy csak diákcsíny?

2009.01.30. 12:10 | Csizmazia István [Rambo] | 1 komment

Címkék: médiahack vagy obama diákcsíny féreg

Egy cikkben arról olvashatunk, hogy **egy illionisi iskolában körülbelül száz számítógépen tűnt fel egy olyan féreg**, amely a képernyő jobb oldalán Barack Obama fotóját jelenítette meg.



A cikk Roger Thompson blogjára hivatkozva képernyő fotót is közöl, és valóban látszik az ominózus Windows XP screenshot, rajta az elnök fejével. Első látásra olyan, mintha valaki visszarepített volna minket az időben, vagy szándékosan egy retro kártevőt próbált volna készíteni. **Lelassítja a rendszereket, USB eszközökön terjed, a megfertőzött gépen megjeleníti a fotót** és állítólag nem ismeri fel egyetlen antivírus program sem. Reméljük a hazai változatokban nem magyar politikus ábrázatokkal fogja majd riogatni a gyanútlan felhasználókat ;-)

De vajon igazi-e ez a kártevő? Egyrészt **elég gyanús, hogy ez csak egy helyben megtörtént** esemény, ami vagy egy új, Mitnick örökébe lépő ifjú tehetséget jelenthet, aki diánycsinyként kereste a feltűnést, **vagy egy olyan unatkozó rendszergazdát, akinek túl sok a szabadideje**, és túl kevés a munkafeladata. És sajnos ilyenkor indulnak meg aztán az olyan e-mailes álhírek (hoaxok), amik egy új veszélyes vírusra figyelmeztetnek és azzal a mondattal zárulnak "és küldd tovább minden ismerősödnek!".

Van azonban egy harmadik lehetőség is, hiszen az eddigi információk alapján **nem lehetünk benne biztosak, hogy ez egy valódi, vadon élő kártevő. Sőt** a Google-ben rákeresve azt láthatjuk, minden hivatkozás egyes egyedül ugyanerre az egyetlen blogbejegyzésre hivatkozik, azt cizellálja, azt tupírozza fel, annak a képernyőképét közli. Még az sem kizárt, hogy médiahack az egész, és a készítők a háttérből már a térdüket csapkodják a nevetéstől, vagy már egyenesen a leleplezésről szóló dokumentumfilmjüket tervezgetik legott.

A "magyarabok" isszák a barackpálinkát a lecsó után

Ennek ellenére **ha valaki mégis találkozik ezzel az Obama fejes féreggel, és merő véletlenségből nem pont az inkriminált Illionis állambeli iskola tanulója, szóljon, egy VirusTotalos ellenőrzésre befizetünk :-P**

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/911970

Kommentek:

Kösz jól vagyok! Ne tessék aggódni! • http://tudtad.blog.hu 2009.01.30. 13:07:12

első

Védtelenül hagyja a bootoló PC-t a 2009-es Norton

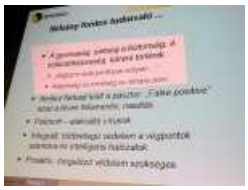
2009.01.30. 18:21 | Csizmazia István [Rambo] | 9 komment

Címkék: biztonság veszély norton védelem szemfényvesztés sebesség kikapcsolt

"A **Norton AntiVirus és az Internet Security 2009-es változata** jópofa trükköt alkalmaz a bootolás felgyorsítására, azonban ennek ára van: a számítógép a rendszerindítás ideje alatt teljesen védtelen."

Ezzel a bevezetővel jelent meg **a HWSW portálon egy cikk, amely arra hívja fel a figyelmet,** hogy a sebességhajszolás bűvöletében a védelem csorbult.

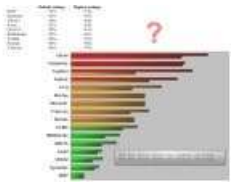
A **gyors indulás miatt kikapcsolt védelem a bekapcsolt számítógépnél olyan sokára** töltődött be a kísérletezés közben, hogy a tesztelésre szánt **eicar.com állományból addigra nem kevesebb, mint 46 másolatot tudott** a cikkíró készíteni. **Ez pedig az jelenti, hogy ez alatt az idő alatt egy vírus is** bátran tehet bármit.



Voltak már előbb is intő jelek, mint arról már mi is beszámoltunk, a Norton korábbi változatainak lassúsága miatt azt kommunikálta, csak lassan szépen, a sebesség olyan hátrány, ami a minőség rovására megy. Mégis a Norton Internet Security új változatánál már azzal dicsekedtek, **kiküszöbölték a zavaró lassulást**.

Aztán új 2009-es szoftverüknek megjelenésekor egy olyan trükkhöz folyamodtak, amely kikapcsolta a rendszer visszaállítás lehetőségét, **ezzel kisebbnek tüntetve fel a telepítési csomagját**. Ezzel még nem is lett volna semmi baj, azonban a rendszer visszaállítás kikapcsolásáról **egyáltalán nem tájékoztatták a felhasználókat**, ami nem túl tisztességes eljárás, és a dologról is csak véletlenül szerezhettünk tudomást: szakértők elkezdtek kísérletezni, onnan derült ki az egész.

Az AV-Comparatives 2008. novemberi tesztjén, a 10. oldalon látható **a „Boot Time test" – ha az Early Load opciót bekapcsoljuk, a Symantec már nem a második leggyorsabb lesz a listában**, hanem alaposan hátrakerül ebben a sorrendben.



Szerencsére **az ESET NOD32 Antivirus és az ESET Smart Security is úgy biztosít gyors bootolási időt a felhasználóknak, hogy eközben még a gépet is védi** :-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/912209

Kommentek:

Ötvös Tomi 2009.01.30. 19:40:57

Szia Rambo!

Én sajnos bedőltem a reklámnak, megvettem a NIS 2009-et, de ezek után visszaküldöm a terméket. Előfizettem most egy újságra, -gondolom a nevét nem írhatom le, mert reklám lenne,-és abból fogom használni az ESET Smart Security-t.
Volt néhány gyanús fájlom, amit több cégnek elküldetem, így a Symantecnek is. A mai napig nem ismeri fel a Norton ezt a kártevőt, a többiek reagáltak rá. Megjegyzem, az ESET rögtön riasztott rá. (Variant of Kryptik trójai). Azt hiszem, hogy az 5-15 percenkénti adatbázis frissítés nem egyenlő a gyorsabb reagálással. Sajnos, egy csomó embert megvezet a Symantec így.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.30. 19:55:05

Szia Tomi!

Üdv a blogon :-) Ha gyanús fájljaid vannak, azokat elég jól le lehet ellenőrizni a www.virustotal.com oldalon.

És még egy apróság: éppen délután láttam egy műsort az ATV-n, amelyben Szilágyi János említett, hogy abnormális módon az emberek annyira meg vannak félemlítve, hogy nem is mernek cégneveket, áruházakat egy betelefonálós műsorban megnevezni. Pedig ez abszurd helyzet, az a helyes, ha mindenki nevén nevezheti a dologokat, és a néző, hallgató, betelefonáló és természetesen a kommentelő is bátran leírhat konkrét neveket, hiszen ettől lesz konkrét információ tartalma, emiatt gondolkoznak el majd rajta a többiek.

Ötvös Tomi 2009.01.30. 21:11:11

Szia Rambo!

Igen, én is a virustotal.com-ot használom, éppen innen derült ki, hogy szegényke (NIS 2009)még mindig nem ismeri fel a kártevőt.
A másik dologra visszatérve akkor nevezzük nevén a dolgokat: Nos a PC World jóvoltából használom ezentúl a Smart Security-t. Igaz, még nem jött meg az újság, de addig fut a 30 napos változat. Egyből felgyorsult a gépem.

HoratiusW (törölt) 2009.01.31. 13:39:03

Ezt nevezik reklámnak :)

Ötvös Tomi 2009.01.31. 14:28:03

Szia Rambo!

Nem az előbbi témához tartozik, de most, hogy elkezdtem használni az ESS-t, felmerült bennem a kérdés, hogy az alapbeállításokon felül is kell még beállítani valamit?
Mivel új vagyok itt, nem tudom, hogy privát üzenet formájában megtudhatnék-e valamit, vagy mi a módja neki?

Köszi előre is!

Ötvös Tomi 2009.01.31. 14:30:11

Még valami eszembe jutott ezzel kapcsolatosan. Használsz még valamit ezen felül? Valahol már biztos leírtad, de sok végigolvasni az összes kommentet.

Köszi még egyszer!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.31. 20:41:54

Hi!

Igazából én Linuxozom, csak azért van egy Wines gépem is, hogy legyen min futnia vírusoknak ;-)

Az ESS mellett nekem egy Spyware Terminator fut, jól megférnek együtt, én paranoid módon szeretem azt a feelinget, amit például a NoScript ad a Firefoxhoz. Itt is minden Registry módosításnál kérdez, hogy "Mehet?" "Nem mehet?" És biztos van akit ez zavar, én meg szeretem látni, hogy mikor, mi és miért történik. Van még plusz a routerben is egy tűzfal, és persze a Firefoxban egy rakat plugin, ami nélkül már csupasznak érezném a böngészőt :-D

Az ESS beállításoknál én be szoktam jelölni a "Veszélyes alkalmazások keresése" és a "Kéretlen alkalmazások keresése" opciót is, sőt a "Kiterjesztett heurisztikát" is, hadd dolgozzon.

Szerintem érdemes átlapozgatni ezt is, sok okosság van benne:
www.eset.hu/files/kezikonyv/ESET_Smart_Security_telepitesi_utmutato.pdf

Ötvös Tomi 2009.01.31. 21:06:41

Szia Rambo!

Nagyon köszönöm a részletes válaszokat, megfogadom! Ez a Spyware terminator tényleg jópofa kis program, szépen megférnek együtt. A NoScript-el már kicsit nehezebben barátkozom.

Kodomo 2009.02.01. 19:22:05

A Chip-ben és a PC Word-ben is van 1 hónapos kód többféle vírusirtóhoz (Nod32, Kaspersky), tűzfalhoz. AVG, Avast kód nélküli otthonra.

Mostanában -eléggé ell nem ítélhető módon- tört Nod-dal is megkínáltak (frissít kód nélkül).

Veszélyes lehet a Google videó kereső

2009.02.02. 17:59 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google flash video adobe update kártevő

A Google Video Search keresőoldal **találatait mérgezik rosszindulatú kódokkal**, ezért nem árt résen lenni a szolgáltatást gyakran használóknak.

A TheRegister figyelmeztet, hogy szándékosan erre a célra létrehozott kártékony weboldalak segítségével zajlik egyfajta célzott támadás, amikor a keresett video film helyett egy **kártevő igyekszik letöltődni a gépünkre Adobe Flash frissítés gyanánt**. A codec letöltési vagy flash frissítési trükk maga nem új, erről már a blogon is írtunk, de hogy a találatok tömegesen épüljenek be a keresési eredmények közé, az már valóban újdonság.

A Trend Micro kutatói szerint **több kulcsszó sokezer találatába sikerült beférkőzniük** a fertőzött linkekkel, ezért mindenképpen indokolt az óvatosság. **Az eset teljesen független attól a szombati malőrtől**, amikor a Google kereső minden találati oldalt veszélyesként jelölt meg, ez utóbbi egy emberi mulasztás miatt (PEBKAC) történt.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Utaljunk pénzt a S.O.C.A.-nak
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/918261

Kommentek:

Nincsenek hozzászólások.

Járvány vagy hisztéria?

2009.02.03. 13:20 | Csizmazia István [Rambo] | 3 komment

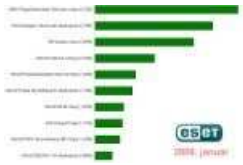
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET **több százezer hazai felhasználó adatai alapján készült statisztikái** szerint a magyar toplistán is előrelépett a **világszerte erősödő Conficker féreg**. Az előzetes jóslatokkal szemben egyelőre nem okozott tömegjárványt, annak ellenére, hogy évek óta nem volt példa ilyen erős víruskitörésre.

A rendkívül **összetett és gyorsan terjedő Win32/Conficker.A** az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos **sebezhetőségére épít**, így a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. **A Microsoft már októberben kiadta az MS08-67 biztonsági javítócsomagot**, amely megszünteti a rendszer sebezhetőségét, a vírus terjedése ugyanakkor jelzi, hogy a felhasználók jelentős része nem frissíti az operációs rendszerét. **„A felhasználók gyakran figyelmen kívül hagyják a szoftverfejlesztők figyelmeztetéseit, amelyek a biztonsági frissítések fontosságára vonatkoznak. Egyes becslések szerint a számítógépek egyharmada egyáltalán nincs frissítve, sok vírusíró éppen erre épít" – mondta Csiszér Béla**, az ESET kizárólagos hazai képviseletét ellátó Sicontact Kft. ügyvezetője.

A sebezhetőség kihasználása mellett **a Conficker az automatikus futtatási lehetőség segítségével is terjed**. A kártevők készítői felismerték a hordozható eszközök – például MP3 lejátszók – fokozódó népszerűségében rejlő lehetőségeket, és olyan károkozókat készítenek, melyek az eszköz csatlakoztatásakor automatikusan elindítják magukat. A Conficker is képes magát ezekre az eszközökre másolni, az autorun.inf fájl felhasználásával pedig különböző kártékony kódokat futtat le.

A féreg emellett egy hálózatra kerülve **szótár alapú támadást indíthat a gyenge admin jelszavak ellen**, feltörve az olyan gyakran használt szókombinációkat, mint a „123", az „admin" vagy a „pass". Így a fertőzés következményeinek kivédésében nagy szerep jut az erős jelszavak használatának. (Itt ellenőrizheti jelszava erősségét: http://www.netacademia.net/jelszoellenor/.)



Mindent összevetve a Conficker nem okozott itthon tömegjárványt, bár igaz, hogy évek óta nem volt példa ilyen erőteljes víruskitörésre. Ennek oka, hogy a kártevő gyorsan mutálódik, így előfordulhat, hogy egyes új variánsait az antivírus programok nem ismerik fel. **Az ESET szoftverei az elsők között voltak képesek a kártevő detektálására, a cég víruslaboratóriumának szakemberei pedig olyan ingyenes eltávolító eszközt készítettek**, mely az esetlegesen bekövetkező fertőzés után is képes maradéktalanul megtisztítani a számítógépeket. Ez a Sicontact Kft. honlapjáról (www.eset.hu) letölthető.

Ugyan az ESET Magyarországra vonatkozó statisztikái szerint a vírustoplista első három helyén nem volt változás, a sereghajtók közt a Conficker erősödése mellett más átrendeződés is történt. **Az 5. helyet egy korábban már sok fejtörést okozó trójai, a Swizzor foglalta el, mely többnyire reklámprogramokat** jelenít meg a fertőzött számítógépeken.

Végül következzen a magyarországi toplista. Az ESET statisztikai rendszere szerint 2009 januárjában az alábbi 10 károkozó terjedt a legnagyobb számban, melyek együttesen az összes fertőzés 34,17%-áért voltak felelősek:

1. WMA/TrojanDownloader.GetCodec.Gen trójai
Elterjedtsége a januári fertőzések között: 8,22%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

2. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a januári fertőzések között: 6,76%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

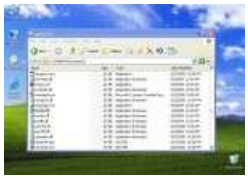
3. INF/Autorun vírus
Elterjedtsége a januári fertőzések között: 5,66%

Működés: INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

4. Win32/Conficker.A féreg
Elterjedtsége a januári fertőzések között: 3,42%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy onnan további kártékony kódokat töltsön le.



A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/conficker-a

5. Win32/TrojanDownloader.Swizzor trójai
Elterjedtsége a januári fertőzések között: 2,34%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat töltöget le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a „csomagban". Ha a Documents and Settings\User\Application mappán belül találunk egy „DVDAUDIO" könyvtárat, az is árulkodó jel lehet.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-d

6. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a januári fertőzések között: 2,15%

Működés: Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

7. Win32/VB.EL féreg
Elterjedtsége a januári fertőzések között: 1,65%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.

A számítógépre kerülés módja: fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.
Bővebb információ: http://www.eset.hu/virus/vb-el

8. Win32/Agent trójai
Elterjedtsége a januári fertőzések között: 1,57%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

9. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a januári fertőzések között: 1,42%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amely billentyűleütés-naplózót (keylogger) igyekszik gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására és a jelszó adatok titokban való továbbküldésére fókuszál. A távoli támadó ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthat hozzá, amelyet aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

10. Win32/CMDOW.143 alkalmazás
Elterjedtsége a januári fertőzések között: 0,98%

Működés: A cmdow.exe állományra sok antivírus program nem jelez, hiszen nem vírusról, hanem egy hacker eszközről van szó. A Cmdow egy olyan parancssori segédprogram, melynek segítségével Windows NT4/2K/XP/2003 rendszereken kilistázhatjuk, átmozgathatjuk, átméretezhetjük, átnevezhetjük, elrejthetjük vagy ismét láthatóvá tehetjük, minimalizálhatjuk vagy kinagyíthatjuk, helyreállíthatjuk, aktiválhatjuk, illetve inaktiválhatjuk, továbbá bezárhatjuk, leállíthatjuk az ablakokat. Az eredeti cmdow alkalmazás egy 31 KB-os végrehajtható fájl, amely nem ír a rendszerleíró-adatbázisba, nem igényel külön telepítést, elég lefuttatni. Eltávolításához elegendő ezt az állományt törölni.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/cmdow-143

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/920078

Kommentek:

Kösz jól vagyok! Ne tessék aggódni! • http://tudtad.blog.hu 2009.02.03. 18:16:40

ez bazi hosszú

LongJohnHolmes 2009.02.03. 18:39:04

Azt hittem az influenzáról lesz szó :(

CApa (törölt) 2009.02.03. 19:09:50

Mindig jó érzéssel tölt el, ha ilyen helyre kis virnyákokról olvasok - nehéz időkben is biztosítva van így a megélhetésem... :-))

Ja, otthon Apple fut - legszebb öröm a káröröm...

Ha nem lenne mindenki admin...

2009.02.06. 11:58 | Csizmazia István [Rambo] | 21 komment

Címkék: admin internet jog root kártevők jogosultság

Egy friss tanulmány szerint a 2008-as esztendőben történt Microsoftos sebezhetőségek döntő hányada megelőzhető, vagy hatása csökkenthető lett volna, **ha a felhasználók többsége nem állandóan adminisztrátori jososultságokkal** használná a Windowsos számítógépét.

A BeyondTrust elemzése arra hívja fel a figyelmet, hogy a **kritikus sebezhetőségek kihasználása miatti biztonsági incidensek körülbelül 92 százaléka lenne megelőzhető**, ha a felhasználók nem root joggal használnák állandóan a gépüket. A **böngészés közben begyűjtött kártékony kódok az ilyen gépeken admin joggal** tudnak garázdálkodni, és ezzel jelentős biztonsági kockázatot okoznak. Egy Linux vagy OS X rendszeren **nincs ilyen jellegű "véletlen" kódfuttatás, kéretlen telepítés**, hiszen ott üzemszerűen sosem rootként használjuk a gépet, hanem csak bizonyos, kulcsfontosságú műveletek alkalmával - például telepítés - hajtunk végre parancsokat adminisztrátorként.

Sajnos az **XP alatt csak kevesen élnek ezzel a lehetőséggel**, vagy használják az olyan ötletes megoldásokat, mint például a DropMyRigths, amely egy adott alkalmazás elindítása után eldobja a különleges admin jogot, és a továbbiakban jóval veszélytelenebbül, felhasználói szinten futtathatjuk a programot. A **támadások jelentős része alapoz arra**, hogy a hozzáférnek a megtámadott géphez, a Windows rendszerfájljaihoz. Emiatt tehát **minden, internet eléréssel rendelkező alkalmazásunknál** (levelező, böngésző, chat, Voip, stb.) érdemes lenne használni valamilyen jellegű jogosultságbeli korlátozást. **Nyilvánvalóan ennek elemzésnek az is az egyik célja**, hogy jobban felhívja a figyelmet a tanulmányt készítő cég saját, jogosultságkezelést végző, Privilage Manager szoftverére.

Persze elviekben mindez szép és jó, de a dolognak két oldala van. A probléma megfelelő megoldásához **az is szükséges lenne, hogy a Windows programozók ne olyan programokat írjanak, ami csak és kizárólag adminisztrátori jogosultságokkal futtatható**.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/925964

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.06. 13:42:04

Ez már csak hab a tortán:
ipon.hu/hir/ms_nem_hiba_a_hiba/5336

Droli · http://nivo.blog.hu 2009.02.06. 13:46:01

Az utolsó mondatot nagyon aláhúznám. A szolgáltatóm által adott betárcsázós programot pl. nem lehet userként használni, így kénytelen vagyok admin módban netezni, s reménykedni, hogy semmit nem szedek össze. Eddig szerencsére nem volt gond.

Kreta 2009.02.06. 13:54:19

Az én HP!!! scanerem sem hajlandó halandóként scanelni.

Rob67 2009.02.06. 14:02:46

Én sem vagyok hajlandó Userként dolgozni :)

Yeto 2009.02.06. 14:06:09

És akkor nem is említettük, hogy az America's Army se feltelepülni, se futni nem hajlandó ha nem adminisztrátorként futtatja az embör...

Hurrá Torpedó · http://www.youtube.com/watch?v=br-D7UneS0E 2009.02.06. 14:44:39

admin módban használom a wint otthon. utálnám ha ezért azért át kellene lépnem óránként admin userre. sosem fosok hogy bekapok vírust, vagy spyt. van egy jó routerem, megfelelően van konfigurálva, emellett a gépeim is rendelkeznek tűzfallal, és vírusírtóval is. no para.

a melóhelyen szigorúan userként futok. itt az adatok miatt sokkal nagyobb a fegyelem ilyen tekintetben. utálom is a sok szar programot hogy úgy kell szarozni hogy fussanak userként. millió egy ilyen van a könyvelő, banki progi, de még a szaros szkenner is kiakad ha nem admin vagy alapból. ilyen szempontból csillagos 5-ös a nero burn rights. nyilván a többi program is megoldottuk a futást userként, csak nem mindegyiknél egyszerű.

Hurrá Torpedó · http://www.youtube.com/watch?v=br-D7UneS0E 2009.02.06. 14:48:53

mivel látom HP szkenner nem hajlandó működni leírom a teljesség kedvéért, hogy itt nálonk a CANON nem ment alapból. legalábbis a gyors funkciógombok a szkenneren de megoldottuk, és a legnagyobb analfabéták is 1 perc alatt tudnak szkennelni.

debilgyik (törölt) 2009.02.06. 14:56:35

a franc, tiszta linux ez a windows :-) ha "normálisan" akarod használni, akkor ügyeskedni kell :-)

nálam vista sp1 van, canon multifunkciós simán megy - igaz, vista telepítés után mindig első dolgom az UAC kikapcsolása :-p

WonderCsabo 2009.02.06. 14:59:51

Azért a cikkben hozzátehetted volna, hogy a Vistában és a 7-ben sem adminisztrátori joggal garázdálkodik az ember...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.06. 15:15:40

@WonderCSabo:
Igen, ez igaz és a Windows Server 2008-ban is így van.

artifex · http://www.amywinehouse.co.uk/ 2009.02.06. 15:40:35

Kedves Microsoft, a DropMyRights helyett talán inkább telepítéskor nem egy Admin jogosultságú embert kellene létrehoznia a rendszernek, hanem egy Admin-t és egy Felhasználót, utána a Felhasználóval használni. Mert az emberek 99.9%-a nem fog létrehozni magának egy Felhasználót, hogy a szar programok miatt (cikkben utolsó mondat ugye) folyamatosan váltogasson usert. Lehet a Vista már máshogy működik, nem használom, de az emberek döntő része még XP-t használ.

viks 2009.02.06. 15:41:52

Érdekes, hogy a hőn utált Vista sohasem került a pozitiv példák közé - ez kicsit olyan mint a számitástechnika HirTVje,D

Az ördög oprendszere az a Vista(UAC) - az ördögé uraim - és monnyon le!

PTibor (törölt) 2009.02.06. 15:43:43

Nem, nem kellene minden alkalommal kilépni, belépni, erre van a "run as administrator". Mondjuk a Vista már megpróbálta behozni ezt, csak ők átestek a ló túloldalára, mert kb a monitor felbontását sem tudtad megváltoztatni. otthon osx-en teljesen jó, hogy komolyabb rendszerbuzergálás előtt elkéri a jelszavamat. szóval nem is root (vagy hogy hívják osx alatt) userrel kell belépni, hanem a saját neveddel sudo-zol

zsoci 2009.02.06. 16:00:47

@artifex: Az lehet hogy az emberek többsége xp-t használ, de meg is érdemlik. Lassú ,insatbil, elavult. Nekem a Vista hibátlanul fut már kb1,5-2 éve. Csak csinálják a cirkuszt mindenfele egy csomó ember meg fosik a Vistától, ok nélkül.

Bambano 2009.02.06. 16:14:00

@Droli: mi akadályoz meg téged abban, hogy a betárcsázás után másik userként futtasd az explorert?

Egyébként az én felméréseim szerint az ms hibák 100%-a megelőzhető lenne, ha nem használna senki ms szoftvert...

mnmnbkhj 2009.02.06. 16:17:39

Ugye, a suliban nincs ilyen baj, mert ott semmit nem lehet futattani :D

sid2008 2009.02.06. 16:26:10

@zsoci: Akkor biztos a microsoftnál is hülyék dolgoznak mert ők sincsenek elájulva töle,nem beszélve azoktról a független szakértökröl akik lehúzzák az értékeléseken és a baráti társaásgombrol akik szintén szidják.Nem baj te értesz hozzá az a lényeg

Füstkarikagyáros 2009.02.06. 16:58:32

@zsoci: az én xp-m nem lassú, nem instabil, nem csicsás, egyik gépen sem. Akkor én is megérdemlem?

zsoci 2009.02.06. 21:44:22

@Füstkarikagyáros: Meg. Nekm se volt insatbil, csak épp minden sp után lasult egy kicsit és furcsa dolgokat csinálni. Az sp2 után már borzalom lett.
@sid2008: Az hogy ez is mondja az is mondja én is olvasom, csak azt nem írja senki sehol, hogy pontosan mi is a gond vele.

r@ek (törölt) 2009.02.08. 09:58:49

@zsoci: Van egy mondas:

"A szamitogep nem kivansagaink, hanem parancsaink szerint mukodik"

Optimalizalni kell es nem fog se fagyni, se furcsa dolgokat csinalni.

4 eve fut csont nelkul az xp-m, pedig ezen aztan minden szar volt mar :-D

artifex · http://www.amywinehouse.co.uk/ 2009.02.13. 13:10:07

@zsoci: 2004-ben telepítettem az XP-met, előtte 98SE volt a gépem, azóta már nem egy program fordult meg rajta, változott is pár hardver alatta és stabil, semmi baja. Ennyit az instabilitásról.

Ha feltenném a Vistát, akkor tehetnék bele több memóriát, jobb videókártyát, hogy elérjem ugyanazt a sebességet, amit most tud. Ez tényleg nagy előnye. Már ha hardver kereskedésed van persze. Ezt átnéztem és nem láttam semmi olyan kiugró különbséget, amitől egyből Vistára váltanék:

www.tomshardware.com/reviews/xp-vs-vista,1531.html

Ennyit a sebességről.

Miért elavult? Mert a programok 99.9% megy rajta? DX10-re szarok, azt nálam ne hozd fel mellette, nem csak játékra használjál az emberek a gépet. Ennyit az elavultságról.

Leírásod alapján gondolom te vagy az a felhasználó, aki az átlátszó (lehetőleg állíthatóan!) ablakokra élvez és az összes programján valami csicsás skin van, mert attól döglik a paraszt. Ha így van, valóban a rendszered csak Vista lehet.

Nem hiszem, hogy az emberek fosnak a Vistától, egyszerűen semmi olyan mértékű előnyt nem ad, amiért érdemes átállni rá. Számomra jelenleg biztos nem. Ha majd minden jó cucc Vista alatt fut kizárólag, akkor biztos átállok rá. De ez még messze van, úgy érzem.

A social engineering 1000 arca

2009.02.09. 14:38 | Csizmazia István [Rambo] | 3 komment

Címkék: social csalás megtévesztés engineering

Semmi sem állandó, csak a változás maga - szól a Herakleitosz idézet nagyon is találóan, rámutatva arra, hogy a kártevők elleni védekezés semmiképpen nem egy kőbevésett statikus szabályrendszer, hanem egy naponta változó milliónyi trükköt, emberi gyengeséget kihasználó megtévesztés, sok leleménnyel, és **mindig új megnyilvánulási formákkal**.

A Halál ezer arca című film szerint az élet addig tart, ameddig a szívünk dobog **(vagy ameddig ki nem fogy a medveetetésnél a zacskóból a chips)**. Ezzel analóg módon úgy is fogalmazhatunk, hogy a számítógépes biztonságunk pedig addig tart, ameddig az agyunk forog.

Az egyik friss hír szerint veszélybe kerülhetnek az XBox tulajdonosok, ha bedőlnek a Microsoft pontgyűjtési csalásnak. Akár hitelkártya adataikat, összegyűjtött játékospontjaikat és megvásárolt játékaikat is elveszthetik azok az Xbox felhasználók, akik ingyenes Microsoft pontok reményében illetéktelen kezekbe adják felhasználónevüket és jelszavukat. **A pénzért megvásárolható Microsoft pontok fizetőeszközként szolgálnak az Xbox játékkonzolhoz különböző kiegészítő tartalmakat árusító Xbox Live felületen**. Az internetes bűnözők megszerzik a játékosok belépési adatait, így hozzáférhetnek azok személyes és hitelkártya adataihoz, elkölthetik a Microsoft pontjaikat, de akár elvehetik az elsősorban presztízsértékű játékospontjaikat (gamerscore) is.

VIGYÁZAT, a videó vírusos fájlt tartalmazó linkre mutat!!!

Az elkövetők legtöbbször ingyenes pontokat ígérnek a gyanútlan felhasználóknak. Az adathalász weboldalakra irányító üzenetek sokszor játék közben, maguktól a játéktársaktól érkeznek, de a YouTube-on is számos hamis útmutatót találhatunk.

A másik érdekesség a parkolással kapcsolatos, **itt az autók szélvédőjére kapnak egy csali értesítő levelet az áldozatok** azzal az ürüggyel, hogy lefotózták és megbüntették autónkat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetjük az inkriminált képet. A büntetőcédulák persze hamisak voltak, a weboldal pedig kártékony szoftvereket próbált telepíteni az áldozatok számítógépére. Azért itt valóban **nagy a kísértés, hogy valaki gondolkodás nélkül ellátogasson** a megadott oldalra.

Mai harmadik példánk pedig a társkereséshez kapcsolódik. Ahogy a szegény országokban önálló foglalkozás lett a gazdag túristák autói elé ugrani, aztán pénzeli kártérítést követelni, miközben persze egy egész falu tanuskodik, hogy "mindent látott", úgy tűnik, **az iparszerű házasság szédelgők is sportot űznek a gyanútlan ügyfelek megkopasztásából**. A trükk lényege, hogy az ismerkedés kezdeti szakaszában, amikor már túl vannak az első levélváltásokon, de még a valódi találkozás előtt állnak, **a csaló előáll egy kifogással, hogy valamelyik családtagja váratlanul súlyosan megbetegedett, és pénzzavarában segítséget kérne**. Aki bedől az ilyen mesének, vélhetősen sosem fogja megtalálni a hercegét fehér lovon. Sokkal valószínűbb, hogy a pénz küldése után bottal ütheti a nyomát a herceg és az összegnek egyaránt. A történet külföldön már annyira gyakori, hogy az áldozatok egy külön honlapon osztják meg egymással információikat.

Minden nap, minden perc azért van, hogy utód legyen - énekelte anno a P.Mobil a "Főnix éjszakája" című nótában, és a párhuzam jogos, elpusztíthatatlanul, megannyi formában támad, támad fel, és pesszimistán szólva **a kísérleteknek soha nem is lesz vége**. Tehát nekünk kell tartani a lépést, felkészülni, vigyázni. **A social engineering ellen nem véd semmilyen program**, a technikai fenyegetéseket - például jelszólopó programokat és trójaiakat - azonban a rendszeresen frissített vírusirtó nagy biztonsággal megállítja. Az internetezés alapvető szabályairól - így például arról, hogy **ne adjuk ki felhasználónevünket, bankkártyaadatainkat és jelszavunkat ismeretlen oldalakon - még egy jó biztonsági program birtokában sem szabad megfeledkeznünk**. Kételkedem, tehát vagyok - ez kellene leginkább a fejlett biztonságtudatosságunkhoz.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/932217

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.04.02. 11:32:37

Férfi az internetes csalások száma ;-)
index.hu/tech/biztonsag/2009/04/02/no_az_internetes_csalasok_szama/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.06. 10:49:13

Ez is egy elég érdekes történet, ami nem szűkölködik tanulságokban:
homar.blog.hu/2009/05/05/miert_esznek_a_bankok_kulfoldi_kartyakat

Az én szemüvegemen keresztül Somogg hozzászólása látszik a legtalálóbb kommentnek, látszik, hogy nem hazudott Mitnick :-)

"Ha jol latom a levelbol, elutotted a pin kododat ezert nyelte el az atm. Az is eloforulhatott volna, hogy egy tolvaj teszi ezt, es faxot kuldve visszakapja az ellopott kartyadat. Tudom, hogy kartyat nem igy lopnak (csak a magnescsikon levo info a fontos) es atmhez is ritkan mennek vele, de attol ez meg biztonsagi kockazat. Gratulalok, felfedeztel egy biztonsagi rest. Ha a bank a jovoben valtoztat a kartya visszadasi szokasain, akkor hasznos volt a poszt."

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.13. 09:40:06

Épp most olvasom az interjút Randy Abrams-szel a Chip magazinban, és hogy a social engineering milyen változatos lehet, meg hogy milyen nehéz ellene a védekezés. Akkor egy kis hazai adalék álrendőrökkel:
index.hu/bulvar/2009/07/13/alrendor/

Nyertem a lottón...

2009.02.10. 14:41 | Csizmazia István [Rambo] | 28 komment

Címkék: spam lottó csalás e mailcím

Sajnos nem az ötösön vagy a hatoson, hanem **kihúzták az emailcímemet a londoni City Lottón**. Erről levelet kaptam, rögtön kettőt is és **a nyeremény nem kevesebb, mint 500,000.- angol font, azaz 166 millió forint**. Azt hiszem, elrollerezek Kalkuttába, és útközben mindenhol azt hirdetem, hogy a nyerskoszt csodákat művel :-D

Kihúzták az email címemet, és **nyolc ilyen szerencsés fickó is volt**. Hurrá, vár a verőfényes Kalifornia! A 7916/06 sorozatszámon én is egy lehetek ezek közül, és ezt ugye el is hiszem.

Az esélyek állítólag nagyon kiélezettek voltak, hiszen **kilencszázezer címből történt a választás**, és Kanadából, Ausztráliából, Amerikából, Ázsiából, Európából, a Közel-Keletről valamint Afrikából illetve Óceániából is voltak résztvevők **az idei nagy nemzetközi sorsoláson**. Itt már **az sem világos, hogy miért nem a sorsolási elnök unokaöccse nyerte meg a pénzt**, de lehet, hogy ez csak magyarországi pályázatokon, tendereken eddzett hazai elme bohókás pavlovi reflexe ;-)

Sajnos, ha jobban megnézem, bár a leveket állítólag Londonból, az AFRO-ASIAN Zonal Coordinator írta, a City Lotto International cégtől, **mégis egy semmitmondó, sorszámos hongkongi Yahoo címre kellene válaszolni?!** Nyilván a részletes személyes adataimat, PIN kódjaimat és jelszavaimat kellene elküldenem hozzá;-) Válságos időkben sajnos úgy tűnik, újra megszaporodnak az efféle adatgyűjtő átverések. Phh, úgy látszik, nem lesz ebből a pénzből se semmi, ágyő milliomos lét...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog

- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/934506

Kommentek:

m. kisasszony · http://kisasszony.blog.com 2009.02.10. 15:15:37

Igen, ez ismerős, én is szinte minden nap meggazdagodnék, ha elküldeném nekik az összes személyes adatomat. :]

movhu 2009.02.10. 15:48:41

Volt egyszer verseny a neten, hogy kinek mennyije van abban a hónapban a nigériai levelekből. Most éppen lottóból lehetne ilyet nyitni.
(Amúgy volt már magyar áldozata a nigériai leveleknek és a holland lottónak is, szóval van felvevőpiac)

Ventura Blvd 2009.02.10. 16:06:02

@movhu:
Ja a másik bejegyzés írója egymillió eurót nyert: mertmegerdemled.blog.hu/2008/12/10/ev_vegere_milliomos_leszek05
üdvözlet a milliomosok klubjában

Vámpír\\\'08 2009.02.10. 16:17:06

Attól félek hogy van olyan barom, akinél ez be is válik... :)

AndOr01 2009.02.10. 16:25:41

Ha mindenki visszaküldene nekik egy választ hamis adatokkal, akkor legalább megdolgoznának a semmiért! :)

Juzo 2009.02.10. 16:34:22

Tiszta Rém Rendes Család:D
Ott a föld összes emberének a nevét tették egy kalapba, és azt is az angolok csinálták:D

-putyin- 2009.02.10. 16:56:56

vagy egy FBI email cím, ahol várják ezeket, oda kell forwardolni és joccakát.

hadrianus 2009.02.10. 16:57:15

Én a helyedben elküldenék mindenféle fals számot, had görcsöljön a patkány.(:

Roy 2009.02.10. 17:02:20

@hadrianus: Ez nem rossz ötlet.

Roope_Renegade 2009.02.10. 17:08:02

egy csomó ilyen kamu céget már le is kapcsoltak.. cikk: www.hackthat.net/df/ddos/60722/index.hack

Lucius Flavius Arrianus 2009.02.10. 17:08:58

"útközben mindenhol azt hirdetem, hogy a nyerskoszt csodákat művel"
Minden tiszteletem a T. Szerzőnek, ámde - némileg offtopik jelleggel - idéznem kell Winston S. Churchillt, aki szerint:
"Rengeteg egészségmániákust ismertem a magevőkig bezárólag, és mind fiatalon halt meg egy hosszabb, szenilitásban eltöltött időszak után."
Elnézést még egyszer :-)

köpőcsésze 2009.02.10. 17:10:20

eddzett?

és miért csak nyilván kellene elküldeni? Nem ezt kérték?

Méhenkívüli 2009.02.10. 17:16:18

Abba gondoljatok bele, hogy vannak olyan - nem teljesen egészséges elméjű - embertársaink, akik például a képes beszédet, iróniát kevésbé képesek dekódolni. Akik inkább szó szerintiségben élnek.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.10. 17:21:12

Szia Lucius Flavius Arrianus!

Az idézet a Piszkos Fred közbelép Fülig Jimmy őszinte sajnálatára című veretes munkából való eredetileg.

Köszi azért a jótanácsokat, igyekszem megzabolázni az egészségmániámat :-) Csak azok a fránya hangok is békénhagynának már a fejemben ;-)

polarc 2009.02.10. 17:25:33

egyszer egy ismerősöm nagy izgalomban volt, mert ő volt a 999.999-ik látogató egy amerikai honlapon, és csak a számlaszámát kellett elküldenie, cserébe pár napon belül utalnak ennyi-meg annyi pénzt.
Mi egy halk sóhajtás közben csak annyit kérdeztünk, hogy már elküldte-e a levelet...

kartunboj · http://kartundoboz.blogspot.com 2009.02.10. 17:37:41

Mázlista. Az ilyen tíipusu spam-ek évek óta dőlnek ki a virtuális postaládákból :)

mnmnbkhj 2009.02.10. 17:40:24

soha senkinek, semmit se adjunk ki :D

bnőm is könyörög a jelszavamér de nem kapja meg :D

debilgyik (törölt) 2009.02.10. 17:42:56

a franc, hogy sose kapok ilyet :-)

igaz, én "normál" embert is spamlistára teszek minden gátlás nélkül, ha az első figyelmeztetés után is további méretes pps-fájlokkal próbálja meg megtömni a postafiókomat.

Lucius Flavius Arrianus 2009.02.10. 17:53:58

@Csizmazia István [Rambo]:
a hangoknak vissza kell kiabálni. Az ember ezzel a metódussal Ámerikában felette sikeres televíziós hittérítő is lehet, valag ájuldozó rajongóval, nehézsúlyú bankszámlával és könnyűvérű, ámde a phishingnél és a trojanoknál picit veszedelmesebb szőkékkel, a vírusoknál pedig sokkal veszedelmesebb adóhatósággal :-))
A blog remek, mindig szívesen olvasom.

kpityu2 2009.02.10. 18:22:35

Nem tudom, én szinte sohasem kapok spamet. Pedig négy címet is használok. A szinte azt jelenti, hogy nem emlékszem olyan esetre, hogy ismeretlen forrásból kaptam volna emailt, vagy ismerőstől viagra vagy egyéb reklámot. Lehet hogy mázlista vagyok ? :-)

kyanzes (törölt) 2009.02.10. 19:07:55

Egy nő 400 ezer dollárt bukott a nigériai trükkön, szóval van veréb. Ellőtte a család minden megtakarított pénzét, odaadta a férje nyugdíjmegtakarítását, jelzálogot tetetett a házra, eldurrantotta azt a lóvét is, végül még a kocsira is kapott valami pénzt. Vannak még szerencsétlenek bőven.

Volkov 2009.02.10. 19:14:08

A vicc az, hogy ha nem vagy elég gyors, akkor visszapattan a válasz, hogy ismeretlen cím.
Nekem erre van jó kis template-levél gyártva. A rövidebbik változat a "f*ck off scammers!", a hosszabbik pedig plusszban egy 2 megás bmp képet is tartalmaz, ami ... hmmm... nem tul szalonképes. Aztán magyarázkodhattam, amikor a spamszürő kifogta a külföldi partner levelét is, és ő is kapott egyet.

A legutóbb amit olvastam, hogy a magyar célközönséget román és ukrán fizetett(!) spammerek bombázzák.
Egyszer viccből válaszoltam rá, mint aki tényleg elhitte. És válaszoltak! Nem formalevél, hanem pocsék angolsággal megirt válasz. A kedves levelezés akkor szakadt meg, amikor belátták. hogy olyan hülye vagyok, hogy minden baromságot kérdezgetek, de csak nem akarom az utlevelem szkebelt változatát mellékelni.

Azt beszélik elvileg nálunk is létezik olyan nyomozó csoport akik ezek figyelésével fogalakoznak, de elérhetőséget nem találtam.

@Kpityu2:
Egy két szolgáltatónál a beépített spamszürő megfogja őket.

Volkov 2009.02.10. 19:15:35

Ja: a googleban a Fraud411-re keresve friss infókat is lehet olvasni ezekről.

Hakkar 2009.02.10. 19:15:59

Én kimondottan gyüjtöm az efféléket. Sokszor végignézem a bejövő spamet, ha másért nem, hogy lássam manapság mivel szopatják az embereket. Nos jobb napokon 8-10 millio euro/dollar/frak/font is bejönne, ha igaz lenne.
A kedvenceim egyike az alevél (már vagy 5x megkaptam) amiben egy microsoftos emberke értesít, hogy az MS kisorsolta az e-mail címem, és nyertem valami 500.000 USD-t. És sügősen válaszoljak az xy@GMAIL.COM címre. nagyon szeretném látni kik lehetnek azok, akiknek még ez sem tűnik fel.
Már tervezem hogy csinálok egy blogot kimondottan ezeknek, és teszek rá egy számlálót, hogy mennyi az eddigi össznyeremények.

Aki nem kap ilyet, annak valoszinuleg szerver oldalon van igen kellemes spamszűrője, így gyakorlatilag a szemét nagyja el sem jut hozzá. Én a magam részéről jobban szeretek kliens oldalon szűrni, miel már túl sokszor került olyan cég blacklistre akiktől kimondottan fontos levelet vártam.

Walhalla 2009.02.10. 19:26:05

Hahaha, en hulyesegeket irtam nekik vissza es "felnyomtam" oket az igazi Holland Lottonal. Meg szantam ra egy kis idot es az osszes kamuzot emailben scam buntett miatt jelentettem az adott email szolgaltatoknal. Le is tiltottak oket, persze ez nem egy nagy dolog, biztos nyitottak egy masikat, de azert remelem tortem egy kis borsot az oruk ala amikor rajottek ,hogy a 100 szamra kikuldott emailekben szereplo "adataik" mar nem jok...FENE BELEJUK!!!! Csucs az volt amikor magyar (??!!) email cimrol jott ue a general hulyeseg. Lehet, hogy mar ezeknek is van MLM halozatuk es tobb honfitarsunk ontja a hasonlo leveleket, jajjjjjjj.....

kpityu2 2009.02.10. 19:42:18

Lehet, hogy alaposan előszűrnek nekem a szolgáltatónál. Mondjuk egy partnercégtől elvárom, hogy a leveleiket ne spékeljék meg spamgyanús tartalommal.(Még jó,hogy a telefon és kábeltévé számlákat nem emailben kapom, mert tuti a kukában végeznék.:-)

debilgyik (törölt) 2009.02.10. 19:42:42

nem t'om, van chellós, freemailes, céges, gmail-es címem, első három átirányítva a gmail-re, chellós spamszűrő kikapcsolva, freemail-es minimumumra állítva (azon a xaron ugye nem lehet kikapcsolni), a cégesen kikapcsolva, és mégse sikerül napi 2-3 spamnél többet begyüjtenem, az is a gmail spam mappájában köt ki.

mázlista vagyok, csak a lottón nem nyerek :-)

dimitrij 2009.02.10. 20:29:58

és mi a gond? küldj el nekik valami tetszőleges számsort, meg szám és betűhalmazt, agyaljanak csak, hogy mi mire jó, meg mivel mit kell kezdeni.

Valentin napi kártevők

2009.02.11. 11:17 | Csizmazia István [Rambo] | 1 komment

Címkék: nap szerelem email valentin képeslap bálint féreg kártevő ecard elektronkus

A vírusok készítői minden alkalmat megragadnak, hogy az elkészített kártevőket eljuttassák a gyanútlan áldozatok gépeire. A Bálint nap újabb lehetőséget jelent nekik, számunkra pedig azt, hogy jobb, ha óvatosan nyitjuk meg **az aranyos kiskutyás üdvözlőlapokat**.

Néhány nappal Bálint nap előtt már **megjelent a Win32/Waledac féreg egy újabb variánsa**, mely az elektronikus üdvözlőlapok növekvő népszerűségét használja ki. Ha arról kapunk e-mailt, hogy valaki **elektronikus üdvözlőlapot küldött számunkra, és a levél törzsében egy link szerepel**, melyre rákattintva megtekinthetjük a képeslapot, érdemes gyanakodnunk. A vírusok készítői most ugyanis éppen **így próbálják megfertőzni számítógépeinket**.

Akár a képeslapra mutató link, akár az ajánlott ingyenes Valentin napi üdvözlőkártya-készítő linkje mutathat olyan fertőzött állományra (például: mylove.exe), melynek letöltése, lefuttatása vírust juttat komputerünkre. **Még akkor is érdemes gyanakodnunk, ha az eredeti e-mailt valóban ismerőstől kaptuk, hiszen az ő számítógépe is fertőzött lehet**. Ha pedig ezeket a kiskutyákat látjuk, szinte biztosan a vírussal van dolgunk.

A most terjedő Win32/Waledac féreg nem ismeretlen a vírusvédelemmel foglalkozó cégek számára, hiszen korábbi változatai is rendre hasonló technikával igyekeztek terjedni. Ha a vírus sikeresen megfertőzi a számítógépet, akkor egy rendszerbejegyzés segítségével arról is gondoskodik, hogy minden Windows indítás után lefusson a kódja, majd **különféle weboldalakról további kártékony komponenseket próbál letölteni**.

"A bűnözők anyagi lehetőségeit és kreativitását mutatja, hogy már hetekkel ezelőtt tucatjával foglalták le a Bálint naphoz kötődő domainneveket, melyeket feltehetően mindössze néhány napig akarnak használni" - emelte ki Csiszér Béla, a NOD32 vírusirtót forgalmazó Sicontact Kft. ügyvezetője.

A megfelelő védekezéshez elengedhetetlen a frissített vírusirtó használata, de a szakember arra is felhívja a figyelmet, hogy a következő egy hétben mindenképpen **érdemes gyanakvóbbnak lennünk az elektronikus képeslapokkal kapcsolatban**. Aki igazán szeret, az majd átölel minket, vagy ha esetleg távol van tőlünk, akkor felhív bennünket telefonon vagy küld egy hagyományos emailt ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/936418

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.22. 09:34:43

Mr. Waledac újabb trükkjei ;-)
www.mxlogic.com/securitynews/viruses-worms/waledac-variant-uses-sms-spy-social-engineering-theme092.cfm

A Conficker féreg további trükkjei

2009.02.12. 14:50 | Csizmazia István [Rambo] | 2 komment

Címkék: debug gép trükk registry virtuális conficker visszafejtés

A Conficker úgy tűnik, még rengeteg bosszúságot fog számunkra okozni. Egy elemző Ollydebugos visszafejtés közben két újabb érdekességre is felhívja a figyelmet.

Már a hamis antivírusokkal vivott küzdelemben megtapasztalhattuk, egyre nehezebb a mentesítése a fertőzött gépeknek, trükkök tucatjai (megtévesztő szerviz nevek, Registry kulcsok, stb.) nehezítik a tisztítást. Az utóbbi időben a Conficker nevű kártevő **tette tiszteletét sok milliónyi példányban**, és sajnos úgy tűnik, a készítői elég alapos munkát végeztek.

Az első érdekesség, amire a SANS-nál felfigyeltek, hogy a kártevő egy RegSetKeySecurity() ADVAPI32.dll függvényhívással **kitörli saját szervizénél a SYSTEM kivételével az összes hozzáférést**. Ez persze nem egy vadonatúj dolog, erről szó sincs, de **jól demonstrálja, hogy az egyszeri vagy egyszerű felhasználó életét igyekeznek alaposan megnehezíteni**: ne legyen olyan játci könnyű kitörölni az adott folyamatot. Mondhatjuk persze erre azt is, hogy az eredeti Windows Feladatkezelő / Task Manager helyett mindenki használjon Process Explorert és Process Monitort ;-)

Kapnak persze szurkát a víruslaborok elemzői is, egy további furmánnyal - ez sem újdonság, de azért csak egy nehezítő, lécemelő körülmény - **figyeli, valódi vagy virtuális gépen futtatják-e**. Ha észleli a SLDT utasításnál (ami a lokális leíró tábla tárolása), ha nem 0-t kap vissza, **akkor nem az eredeti kód fut tovább, hanem egyszerűen lefagy**.

Biztos mindenki ismeri a másik híres módszert, ami Joanna Rutkowska weblapján szerepel redpill.c néven. Aki egyébként ilyen jellegű **agyköszörülésekre vágyik, annak hasznos olvasmány lehet** Pavol Cerven Programvédelem fejlesztőknek című könyve a Kiskapu kiadótól, amiben olyan érdekességet is talál, hogy figyeljük, futtatnak-e debuggert a programunk mellett, mit tehetünk ellene, stb.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?

- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/938987

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.13. 13:51:18

Azért egy 57 milkás vérdíjnál talán már beficcennek a társtettesek...
biztonsagportal.hu/250-ezer-dollar-verdij-conficker.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.13. 13:52:09

Minden, amit tudni akartál a Confickerről, de sosem merted megkérdezni ;-)
isc.sans.org/diary.html?storyid=5860

Agyilag zokni - mítosz megerősítve

2009.02.13. 16:24 | Csizmazia István [Rambo] | 68 komment

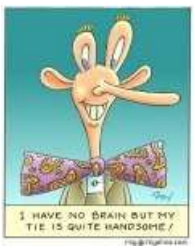
Címkék: jelszó password gyenge conficker

Nem tudni, hogy a kereskedelmi TV csatornák műsorszínvonala hozta-e az áttörést, vagy egyéb behatások is felelősök a szürkeállomány ipari méretű leépüléséért, mindenesetre **a jelszóválasztási fantáziátlanság az emberek többségénél katasztrofális**.

Az Errata Security vizsgálata alapján, amely több ezer, PhpBB felhasználó jelszava alapján történt, az alábbi képet festi elénk, következzen hát a siralmas, mítoszromboló valóság alant. Nem a fórumjelszavak kinyerésének módjára gondoltam, hanem **a "talált" jelszavak minőségére**.

Először is a nyertes lottószámokat ismertetjük: **az "123456" és a "password" a leggyakoribb választott jelszó**. Ennél azért talán már egy hintalónak vagy egy amőbának is több fantáziája van;-) És íme a Top10-es lista, a leggyakoribb találatokkal:

3.03% "123456"
2.13% "password"
1.45% "phpbb"
0.91% "qwerty"
0.82% "12345"
0.59% "12345678"
0.58% "letmein"
0.53% "1234"
0.50% "test"
0.43% "123"



Pedig hát egy jól kitalált karaktersorozat ingyen van, és **nem "letudni" vagy "kipipálni" való nyűgnek, hanem adatainkat védő, minket szolgáló hűséges Ivanhoenak** kellene felfogni a jelszóválasztási procedúrát. Alig pár napja csak, hogy a Conficker kapcsán (mostanában mindenről ez jut az eszünkbe...;-) a gyenge jelszavakról értekeztünk. Nyilván nem azt várja az ember, hogy mindenki atomtudós legyen, és a Harry Pottert sem tudná mindenki megálmodni, de ennél azért biztosan több kellene. Bár Muprhy szerint **minden jó valamire, ha másra nem, hát elrettentő példának**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés

- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/941060

Kommentek:

Biscione · http://axl-zizzenetek.blogspot.com/ 2009.02.13. 18:29:28

Az autóm alvázszáma az jó? Azt tudom fejből, az alkatészkeresés miatt...

keszvagyok 2009.02.13. 18:32:53

hehe, még jó hogy én a 654321-t preferálom, ördögi titokzatos vagyok :)

serwer 2009.02.13. 18:33:36

az 123456-ot én is sűrűn használom olyan helyeken,ahol csak én szerzek infót
ahol vissza is osztok, ott rendesen regelek
a netbanknál problémásabb a 123456 :D

Gyurma73 · http://www.karosszeria.net 2009.02.13. 18:46:20

ja én a 1234567 est használom ahol nincs fontos adat.
Amúgy mi az a"phpbb"???

kekeckecc 2009.02.13. 18:46:32

en svedorszagban most nyitottam bankszamlat, es a telefonos helpdesk meg ugyintezös kodvalasztasnal csunyan belefutottam a rossz szokasom következmenyeibe: en ugyanis szinten a nagyon bena jelszavak embere vagyok, (0000, 1234 stb). Itt viszont a rendszer allandoan kioktatott, hogy "kerjuk, kerulje a tul egyszeru szamkombinaciot mint pl. az 1234 vagy a szuletesi datumok": se ezeket, se ezeket visszafele, se az azonos szamokat, sem pedig a 9876-ot nem engedelyezte. En meg ott alltam a telefonnal, a bankban mar mindenki engem nezett, mire megtalaltam egy egyszeruen megjegyezhetö es elfogadhato nehezsegu kodot. (nem mondom meg, melyiket)

Kösz jól vagyok! Ne tessék aggódni! · http://tudtad.blog.hu 2009.02.13. 18:54:22

amennyi jelszót fejben kell manapság tartani, nem is csodálkozom, hogy ezek a legnépszerűbbek.

nyomasek_bobo · http://sopron.e-cafe.hu 2009.02.13. 18:59:28

@kekeckecc: a telefonszámod visszafelé?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.13. 19:00:46

Szia Gyurma73!

A Phpbb egy nyíltforráskodú közkedvelt fórumszoftver:
phpbb.hu/

WonderCsabo 2009.02.13. 19:08:42

Nekem sem túl bonyolult a jelszavam, de azért ezekhez képest kvantum-elmélet.

Parajka 2009.02.13. 19:09:25

Jót nevettem a letmein jelszón. Az enyém egy matematikai képlet.

repecs 2009.02.13. 19:15:09

Miaz hogy jelszó? Jelmondatkel nektek emberek. Pl:GeZaKeKaZeG

zsüber 2009.02.13. 19:16:42

az enyém egy szám. betűkkel leírva. elég hosszú, a jelszóminősítésen közepesként szokott vizsgázni.

Patreides · http://indavideo.hu/profile/Patreides 2009.02.13. 19:26:49

Ez most hogy is van?
Csak úgy lenyúlják a jelszavakat, vizsgálgatják, majd közzéteszik azokat?
Most akkor én hülyültem meg vagy a világ? :)

amatőr 2009.02.13. 19:29:47

hülye vagyok, ha egyszer kitaláltam magamnak egy 12 karakteres jelszót, és minden fontos helyre azt használom?
módszer: véletlenszám generátor, ascii kód táblázat, és csak egyszer kellett megtanulni, igaz vannak benne csak alt+numerikus billentyűzettel bevihető karakterek is :))

serwer 2009.02.13. 19:33:14

@amatőr:
nem vagy hülye,de nem okos dolog minden fontos helyre ugyanazt használni

májkölnájt 2009.02.13. 19:35:31

lelkészem jelszava:
Mat6:9-12

a miatyánk citátuma ugye, van benne nagy-/kisbetű, szám és spec karakter is, ő könnyen megjegyzi.

ponyvaregény fanok használhatják az Ez25:17 et jelszónak

papugaja 2009.02.13. 19:41:19

Hun van az "admin"?
Meg a "topsecret"?

kutty 2009.02.13. 19:54:52

Ugyan kérem, az ember üsse be az anyja leánykori nevét, és az első szeretője életkorát.
Lehetőleg keverve... :o)

BOB 2009.02.13. 19:55:29

Nekem a kutyam neve az. Kar, hogy nehezen hallgat a js4>)prQ]u;0aJm@ hivoszora.

Celtic 2009.02.13. 19:57:31

ENmeg a banki jelszonal azon buktam, hogy pontot tettem bele. kisbetu/nagybetu/szam lehet, irasjel nem....Igy aztan mehettem a bankba szemelyesen, hogy ujra aktivaltassam a jelszavam...

gothmog 2009.02.13. 20:01:24

A

"Tüze5en 5üt 1e a nyári nap sugára
az ég tetejéről a juhászb0jtárra
Fö1ö51eges d0l0g 5ütnie 01y nagy0n
Hiszen a juhásznak úgyis nagy me1ege vagy0n"

az vajon elég jó wifi jelszónak? Kicsit félek... :P

zsoltix 2009.02.13. 20:18:30

Arról nem szól a felmérés,hogy mit védenek ezekkel a jelszavakkal? Az se mindegy:)

Vattamás (törölt) 2009.02.13. 20:19:33

A válassz egy jó jelszót a legnagyobb marhaság, az összes biztonsági törekvés közül. Az embernek nem 1-2 jelszót kell megjegyeznie manapság, hanem féltucatot, minimum.
Na most ha ugyanazt az erős jelszót kezdi el használni mindenütt, az kész digitális öngyilkosság.
Ha mindenütt mást, akkor úgysem tudja megjegyezni őket és ha mégis, akkor majd jönnek a lejáró - kötelezően megváltoztatandó - jelszavak, stb, stb.
Előbb utóbb ménkű nagy káosz lesz belőle....
Én csak a bankkártyám pin kódját és a jelszómanagerem jelszavát tudom fejből, de ez elég ahhoz, hogy mindenütt erős minősítésű jelszót használjak, de sehol sem kétszer ugyanazt.

B.Tamas 2009.02.13. 20:20:57

Én 1s h4S0nló j3LsZ4v4k4T sz0Kt4M h4Sználn1. :) K3r3s3K 3gY ért3Lm3S zSót éS kB íGy d3kóD0lom. 3mB3r l3Gy3n 4k1 k1T4lálJ4.

zsoltix 2009.02.13. 20:31:27

@Vattamás: igazad van. A jelszó megjegyzése funkció nélkül sokan még a mailjüket se tudnák megnézni. Vagy pl ide írni:)
Őszintén szólva,halvány gőzöm sincs már,mi ide a jelszavam,az automatikus beléptetés nélkül írni se tudnék:)

Pomme 2009.02.13. 20:31:37

nekem nagy kedvencem volt egy időben a fika helyekre a nem123

zsoltix 2009.02.13. 20:32:03

@Vattamás: igazad van. A jelszó megjegyzése funkció nélkül sokan még a mailjüket se tudnák megnézni. Vagy pl ide írni:)

Őszintén szólva,halvány gőzöm sincs már,mi ide a jelszavam,az automatikus beléptetés nélkül írni se tudnék:)

Laslow · http://laslow.hu/ 2009.02.13. 20:40:04

Jelszóra szerintem ideális módszer: egy nem értelmes alapjelszó, kis/nagybetűvel és számmal, a szám lehetőleg nem a legvégén, a nagybetű lehetőleg nem a legelején, és minden egyes weboldalon a weboldal címe alapján valamit módosítani egy egyszerű algoritmussal. Így aztán sehol nem használod ugyanazt a jelszót, viszont minden weblapon ismerve a kiinduló jelszót és látva a címsorban a domaint, egy pillanat alatt kitalálhatod, hogy ide milyen jelszóval is tudsz belépni...

Így:
alapjelszó pl.: u7otVenone
algoritmus pl.: a 7-es után berakni a domain utolsó 2 karakterét.

freemail.hu jelszavad: u7ilotVenone
google.com jelszavad: u7leotVenone
stb.

Ha valaki meg is szerzi egy jelszavadat, az alapján sehova máshova nem tud belépni a nevedben.

2lkedő 2009.02.13. 20:44:04

Na, nezzuk, hany kodot kell megjegyeznem.
- Mobil PIN kod 2x, mert ket SIM kartyat hasznalok.
- 2x bankkartya pinkod
- telefonos PIN kod a mobilszolgaltatiougyfelszolgalatahoz 2x (2 szolgaltato)+1 telebank pin kod
- 2 kulonbozo riasztokod
- belepesi jelszo a a ceges notebookra es asztali gepre valamint a ceges szerverre
- PGP disk jelszo 2x
- belepesi jelszo a ceges emailre
-belepesi jelszo a magan emailre
- belepesi jelszo vagy 5 fele Gmail accountra + legalabb 10 fele forumra
- belepesi jelszo eBayre + legalabb 20 fele online webshopba
- belepesi jelszo es alairasi kodszo az internetbankba, amit par havonta le kell cserelni
- belepesi jelszo PayPal-ra

Hirtelen ennyi ugrott be, de biztos van meg par... ha biztonsagosan akrja csinalni az ember, akkor az osszesnek kulonboznie kell. Ennyi kulonbozo kodot megjegyezni viszont atlagember szamara lehetetlen.

Vattamás (törölt) 2009.02.13. 20:46:01

@Laslow: Ez csak akkor nem jó, ha ez a jelszó az adott oldalon (1)túl rövid, (2)túl hosszú vagy (3)meg kell változtatni.

dark future · http://www.andocsek.hu 2009.02.13. 20:52:59

Akinek sok (értsd: akár több tucatnyi) jelszót kellene megjegyeznie (pl. nekem, mert több helyen vagyok rendszergazda + a privát jelszavaim), érdemes egyetlen szimpla szövegfájlban (SIC!) tárolni, azt viszont titkosítani vmi nagyon brutál módon (pl. AES-256 + 15-20 karakteres jelmondat). Betitkosítva aztán nyugodtan fel lehet írni akár egy pendrive-ra is.

Az nagyon rossz taktika, ha valaki mindenhol ugyanazt (vagy max. 2-3-at) használja, mert vannak olyan helyek, szituációk ill.átviteli csatornák és protokollok, amik nagyon nem biztonságosak (pl. netkávézóban telepített keylogger, szimpla ftp használata, weboldalakon használt jelszavak stb.).

dark future · http://www.andocsek.hu 2009.02.13. 20:58:20

@Patreides:

"Ez most hogy is van?
Csak úgy lenyúlják a jelszavakat, vizsgálgatják, majd közzéteszik azokat?"

Nem muszáj lenyúlni (bár tény: egyszerűbb), hanem (leegyszerűsítve) összeírnak néhány száz "jónak ígérkező" jelszót, és megtesztelnek vele különféle rendszereket. Ha valamelyik bejön, akkor húznak mellé egy strigulát.

zRg 2009.02.13. 21:25:07

bakker, ezután a cikk után el fog terjedni az Ivanhoe mint jelszó...

laccc 2009.02.13. 21:26:27

"letmein" :D:D

smartdrive 2009.02.13. 21:29:22

****

dark future · http://www.andocsek.hu 2009.02.13. 21:50:38

@laccc:

Magyar változatban:

engeggyébe!

gitáros 2009.02.13. 22:10:17

@2lkedő: ebből azért pár nyugodtan lehet azonos...

A Hannibal Lektűr-attitűd · http://hannibal.blog.hu/ 2009.02.13. 22:11:24

@BOB: :O

gitáros 2009.02.13. 22:14:44

@B.Tamas: szótárral simán fejthető, percek alatt

naponta 3x 2009.02.13. 22:44:03

szakember barátom, min. 256 karakteres jelszót használ, verseket, dalszövegeket, ilyesmi. tud valamit.

dark future · http://www.andocsek.hu 2009.02.13. 23:14:31

@naponta 3x:

Jó szakember lehet; a legtöbb rendszer 15-20 karakternél csonkolja ill. nem is enged ennél hosszabbat beírni... Versszöveget is nagyon érdemes használni, főleg standard, szótári szavakkal...

keeroy · http://music.blog.hu 2009.02.13. 23:17:28

Bizony ez a top10 jelszó még sózva is pillanatok alatt szótáras törés áldozata lesz. Bár szerintem ezt az is tudja, aki ezeket írja, csak akkor meg nem értem, miért teszik sokan.

kékféltégla 2009.02.13. 23:34:11

@dark future:

ja én is megnézném, hány oldalon tudja bevésni a versikéit jelszónak.. meg amúgyis kábé hamarabb fel lehet törni szótárból egy versikét, mint egy tényleg jól kitalált jelszót..

Hivatásos beszólóművész 2009.02.13. 23:43:31

Legjobb az ha teljesen oda nem illő szót választasz.
Nem olyan fontosnak szoktam használni a segg és a fasz szavakat.
Ha kicsit bonyolultabb akkor kap egy 1fasz9-t a password.
A legdurvább a 1F2a3s4Z! :D
Persze csak a módszer a szemléltetett! :D

2lkedő 2009.02.13. 23:48:02

Nem kell komplett vers. Vegyunk egy olyat, hogy van valami kedvenc versed, vagy dalszoveged es hasznald a kezdobetuket.
Peldaul legyen a Toldi.
Egy csak egy legeny van talpon a videken->

1cs1Lvtav

Vagy legyen valami kulfoldi, amit fonetikus magyarra irunk at, hogy meg cifrabb legyen, a masodik es az utolso elotti nagybetu

Dire Straits: Sultans of swing
The band is blowing dixie double-four time you feel allright when you hear the music ring->

dBibd24tjfovjhdMr

na, szotarazza ezt valaki...

no mail, no problem 2009.02.14. 00:04:37

@gothmog: már nem jó, mert leírtad. egyes források óvanak az olyan szöveg használatától amit már leírtak, vagy kimondtak.

@naponta 3x: bocs, de már csak gyakorlati megfontolásokból sem hihető. egyrészt sok rendszer nem fogad el ennyire hosszú jelszót, másrészt az átlagos kétujjas gépelő ennyi szöveget minimum két, de inkább két és fel perc alatt ír be. ha nagyon jól nyomja, kicsivel több ujjal, akkor ez az idő levihető másfél percre. (bocs, de hazai felhozatalt ismerve nem feltélezem, hogy vakon gépel.) és ekkor még az kell feltételeznünk, hogy nem rontott, de az átlagos gépelő 250 karakteren már ront.

nitro1 2009.02.14. 00:07:11

Jelszóba sose rakj olyan karaktereket, amiket másfajta billentyűkiosztáson máshogy kell előhozni, mert hamar kilockolod magad. :-D
És az milyen már, amikor a rendszer azt mondja új jelszónál, hogy az új jelszavad nem lehet az előző 10 közül egyik sem. :-S
Na akkor jön a számozás...

boldiii 2009.02.14. 00:14:51

B.tamás: egy szótár alapú keresőprogram is tud elite írásmódot próbálni, és nem nagy kaland egy 60000 szavas szótár párszázezres bővítése elite írásmóddal. Tehát önmagában ez -noha erősít- csak illúzió, hogy jó jelszót adna. Ha a szóba raksz legalább néhány véletlen karaktert, akkor már bajban lennék, mint támadó!

2lkedő: A szavak kezdőbetűit összegyűjteni arra a néhányezer versre és dalszövegre, ami esélyes, egy tippre kb. 1 milliós szótárat eredményez. Ha pl. kódolt jelszó alapján kell vizsgálódni és feltörni, nos, pár másodperc alatt elvérzik a profi jelszavad. Megint: erősít, de önmagában kevés. Ha a jelszó végéhez adsz legalább pár véletlen karaktert, az már sokkal erősebb!

laslow: a domain-specifikus jelszavad jó ötlet, de mi van, ha valaki le bírja hallgatni három-négy jelszavadat, de nem az összeset, mert modjuk azok nem ssl-en mennek át. Szerintem rövid úton meg fogja tippelni, hogy mi lehet a banki jelszavad, és szívsz.

Szóval ezek az ötletek mind aranyosak, de ha legalább 1-2 számot vagy véletlen betűt raktok be a jelszóba, sokkal erősebb lesz a valóságban. És egy-két véletlen jelszót megjegyezni nem a világvége. (egyébként szerintem az cirbrixa5 megjegyzése könnyebb mint a 05a50aaa5a, mert az ismétléseket nehezebb megjegyezni)

2lkedő 2009.02.14. 00:26:48

boldii,

Ertem, es mekkora szotar kell a kulonbozo mas nyelvekrol fonetikusan atirt kezdobetukohoz, kulonos tekintettel arra, hogy mindenki ugy irja at, ahogy o maga hallja?
Ezert mondtam, hogy inkabb kulfoldi vers vagy zeneszam, es fonteikus atirassal, bizonyos szavak betuvel masok szammal, stb..
Nem hiszem el, hogy ez olyan egyszeru lenn, ahogy te mondod, mar csak azert sem, mert ahhoz tul sok dalszoveget es verset kene ismerni a vilag minden nyelven...

laccc 2009.02.14. 00:39:10

@dark future:

Vágom, csak annyira meglepett. :D

dark future · http://www.andocsek.hu 2009.02.14. 00:48:40

példa a tökéletes jelszóra:
n3Furgy3_l3!!

dark future · http://www.andocsek.hu 2009.02.14. 00:56:24

zenészektől láttam olyat, hogy zongorabillenytyűzetnek használták a klaviatúra felső két sorát (a számok a félhangok), és dallamrészleteket játszottak be rajta jelszónak (persze ritmusra :-)), lehetőség szerint gisz-dúrban :-)

no mail, no problem 2009.02.14. 00:59:33

@2lkedő: szerintem ne próbálj meg érvelni mellette, mert a nem szótári jelszevakat fel lehet törni brute force támadással. humánok ellen a dire straits-es jelszavad elég jó, gépi törés ellen meg nem.

szerintem kissé túlspilizták az egész jeszó kérdést a süket kockák, amikor elkezdték szuggerálni ezt a félkatonai stílusu erős jelszó mantrát. többnyire úgyis az a lényeg, hogy az egyik humán amatőr jelszavát minél nehezebben szerezze meg a másik humán amatőr. ehhez bőven elég, ha a jelszó nem a példákban szereplő kamu jelszó, és nem valakinek a neve a környezetedből, autód rendszáma, és hasonlók, továbbá elzavarod aki a jelszavad akarja megtudni. a többit intézze a szolgáltatás üzemeltetője, ez az ő dolga. .

a kockáknak azt is meg kellene érteni, hogy ha elég erős jelszóra kényszerítik a felhasználót, akkor annak az első dolga az lesz, hogy felírja egy cetlire. (szerintem ennél az 123456 is jobb.) vannak páran, akiknek a négyjegyű pin kód sem megy...

ha meg az nyomorult szolgáltató (pl. bank) annyira fontosnak érzi a jelszókérdést, ne tanácsot osztogasson az ügyfeleknek, hanem tanúsítványt, és tanítson meg szakszerűen kezelni. ne az én problémám legyen, hogyan törik fel más szutykát.

ave 2009.02.14. 01:17:33

Hat, PhpBB-s szajton nem adunk meg bonyi jelszot, leven ugysem vedunk semmi ertekeset... (Adminokat leszamitva)

theneverlate_Wizard 2009.02.14. 02:22:21

miért, hogy kell használni a tanúsítványt? azontúl persze, hogy download meg egrí?

(nekem az opera mindig panaszkodik a hazai (net lock kft)-s oldalakra)

Rob67 2009.02.14. 06:20:40

Azért van itt macera.
Én Angliában élek, itt vannak kártyáim, netbankom, de egy még Magyarországon is.
5 Bankkártya + 6 netbank = 5 pinkód + 6 password
Ok, megjegyezhető.
Csakhogy van olyan bank amelyik időnként - mondjuk havonta - kér új jelszót. Ez egy idő mulva komoly permutációt okoz már.
Két év alatt kiszámolható...
Na most ehhez add hozzá ha tényleg elfogadható és nem játékjelszót használsz, mint én magam.
Mi lesz tíz év után?

Ronald 2009.02.14. 06:37:01

Nekem a bankba is a kiskutyám neve a jelszó - mint a többi 100 helyen is.
Más kérdés, hogy a bankom nem utal egy fillért sem - amig nem irom be az SMS-ben kapott kódot.
Ez a fontos - a többi csak lószar - vagy gyerekjáték.

zsoci 2009.02.14. 07:41:34

Ennek talán az is lehet az oka hogy néhány paranoiás rendszerazda aki feleslgesen állít be bonyolult jelszót. Lehet bármit előírni, ha túl bonyolult lesz felírják. Ráadásul rengeteg helyen felesleges. Pl mi a francnak kéri a ebank minden tranzakció elött újra ?? Mi a fenének kell a bankártyás vásárláshoz összeghatár nélkül pin???

turif 2009.02.14. 08:27:32

a "secret" kimaradt. Meg az admin/admin és társai :) Vagy a password nélküli password is :D

Szürkemedve · http://www.medveutja.hu 2009.02.14. 08:31:45

Megoldás: keepass.info/

Néhány dologra nem alkalmas (pl. windows logon). Lényege: egy titkosított adatbázisban, amit egy mesterjelszó véd (na ez legyen hosszú és bonyolult, az enyém 38 karakter, kisbetű, nagybetű, írásjel. Egy kedvenc mondatom, amit nem szoktam hangoztatni.), tárolja a jelszavaidat, amik innentől teljesen megjegyezhetetlen randomgenerált cuccok is lehetnek.

Fel lehet tenni jópár mobiltelefonra is és innentől mehetnek bele a bankkártyák pin kódjai.

A mobilomon viszont kikapcsoltam a PIN kérést. Nem kell el/otthagyni.

DeMarco 2009.02.14. 08:44:24

Nagy ritkán rámjön a naplóírás. Általában nem tart sokáig, max. pár hónapig. Írtam naplót tizenévesen, huszonévesen is, mindig számítógépen. Természetesen minden napló file-t lejelszavaztam, hogy csak én férjek hozzá, más ne csámcsoghasson rajta. Ennek persze az lett az eredménye, hogy ma már egyik file-t se tudom megnyitni, mert fogalmam sincs az akkori jelszókról... Nem csoda, hogy az emberek többsége egyszerű jelszót választ, mert rengeteget kell megjegyeznie. Pin kód, riasztó kód, bankkártyák kódjai, sz.gépes kódok, weblapok kódjai, végtelen a sor. A magam részéről legalább 10 éve ugyanazt a jelszót használom mindenhová. Eddig még semmi problémám nem volt vele. Ha vki megszerzi sincs semmi gond, mert pénzhez nem fér vele, titkaim sincsenek amit megszerezhetnének. Igaz óvatos vagyok és a fő számítógépem nem csatlakozik netre. A netes gépen meg szinte semmi sincs. Így aztán nincs miért aggódnom.

Nagykócsag 2009.02.14. 09:14:34

Megnéztem, a jelszómenedzser programomban jelenleg 265db jelszó van felírva. Normál ember ennyit nem tud megjegyezni (negyedennyit sem).
Súlyosbítva ez azzal, hogy mindenhol más a követelmény a usernévre és a jelszóra is.

Nemhogy a jelszavakat, de időnként a userneveimet sem tudom megjegyezni mindenhol, sőt azt sem, hogy hova kéne beírnom.

Fűszoknyás őstermelő a svéd Aldiból (törölt) 2009.02.14. 09:29:29

És az baj, hogy a kutyám nevét adom jelszónak? Úgí hívom, hogy wuZ9k7Mas

Fedor · http://fedor.blog.hu/ 2009.02.14. 10:08:00

"sz3zam_taru1j"

:-)

blügy-blügy 2009.02.14. 10:11:49

nekem a telefon pinkódja 00000. Senki nem gondolná, hogy öt darab nulla, mert egy mezei user pinkódja 4 számjegyü

ReWriter · http://miazhogy.blog.hu 2009.02.14. 10:16:25

És mi van akkor, ha az űberbiztonságosnak hitt jelszó karakterei, valami általunk ismeretlen vers kezdőbetűire hajaz? Jön a szótár és megfejti?

payskin 2009.02.16. 03:31:22

@no mail, no problem: azért megnézném, amikor valaki brute force-szal feltöri azt a jelszót.

Van egy jelszóval védett Word állományom, aminek sajnos elfelejtettem a jelszavát és rohadtul kéne a tartalma. Jellemzően 8-14 karakter hosszú jelszavakat használok kis-nagy betűk, számok és írásjelek. Kipróbáltam az összes fellelhető brute-force-os programot: ÉVEK. Majd kölcsönkérek egy Cray-2-t valamelyik múzeumtól. ;)

Fűszoknyás őstermelő a svéd Aldiból (törölt) 2009.02.16. 16:28:08

@Balázs:
ha nagyon fontos, és megér 25 eurót, akkor:
www.decryptum.com/hu/index.html

Célkeresztben az AV cégek SQL adatbázisai

2009.02.17. 16:26 | Csizmazia István [Rambo] | 1 komment

Címkék: sql hacker kaspersky xss defender f secure injection unu

Az nem jó, ha a suszter cipője lyukas. Ennek fényében a biztonsági cégeknek kiemelten fontos, hogy weboldaluk ne lehessen áldozata semmiféle defacenek, vagy más webes támadásnak, hiszen ez azért valamilyen szinten rombolhatja a cégimázst, de akár adatokat is veszélybe sodorhat.

Nem lesz persze ettől egy antivírus program se jobb, se rosszabb, ha néha mégis sikerül fogást venni egy weboldalon - sőt **feltörthetetlen weboldal nem is létezik**. Alig fél éve mi is hírt adtunk, amikor a Kaspersky malájziai weboldalát elcsúfították. Most viszont úgy tűnik, **egy egész sorozat zajlik több folytatásban, és erről a HackersBlog weboldalon olvashatunk részletes, képernyőképekkel ellátotta beszámolókat**. Az első áldozat a Kaspersky weboldala volt, és az UNU nevű román hacker arról számolt be, hogy SQL befecskendezés segítségével sikeresen hajtotta végre a műveletet, és ott ajtó-ablak nyitva állt email címekhez, előfizetői adatokhoz, aktiváló kódokhoz. Meg sem lepődünk, hogy a cég cáfolatában az állt, hogy szemben a támadó állításaival mindössze az SQL táblák feltérképezése zajlott, semmilyen ügyfelekkel kapcsolatos, vagy egyéb érzékeny bizalmas információ nem került ki.

Ez azonban úgy tűnik, **ha így is volt, inkább szerencse kérdése volt**. Azt nem tudni pontosan, hogy a behatoló miért nem lépett tovább (időhiány, fehér kalap, bármi egyéb), bár látszólag valóban megtehette volna.

Alig telt el pár nap, máris **következő áldozatról** számoltak be, ezúttal a BitDefender portugál oldalát birkózták le, majd az F-Secure következett SQL és XSS trükközéssel. Ez utóbbi esetén is hozzáfértek ugyan a táblákhoz, azonban **állítólag ott semmilyen érzékeny adatot nem találtak**.

Az elkövetők szemlátomást azóta sem unatkoznak, mai postjukban pedig az International Herald Tribune weboldala következett, ahol az adatbázisban **már érzékeny adatok is szerepeltek**, emailcímek, loginek, jelszó hashek.

A kulcs talán az lehet, hogy **sok cégnél nem kezelik a helyén az ilyen adatellenőrzési hibákat, nem tartják elég fontosnak**, pedig az. Másrészről **nem megköszönik, hanem lekezelően, gőgösen vagy hozzá nemértéssel**, sokszor pedig egyáltalán nem válaszolva felingerlik a jószándékú figyelmeztetéssel hozzájuk forduló embereket, ami nagy hiba. A rossz szándékkal érkező sosem fog tanácsot adni, figyelmeztetni, könyörögni, hogy hallgassák meg, hanem egyszerűen porrázúzza vagy csak csendben ellopja a hiba révén hozzáférhető adatokat.

Számunkra pedig ez azt jelentheti, hogy **bizalmas ügyféladataink illetéktelen kezekbe kerülhetnek**, és/vagy egy megbízhatónak tartott weboldal kódjába bármilyen kártékony kód beilleszthető, ami aztán megfertőzheti a gyanútlan látogatókat. Már csak emiatt **sem szabad elhanyagolni vagy elbagatellizálni** az ilyen támadásokat.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/948358

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.02.18. 12:54:30

A BitDefendert még az ág is húzza, tévesen trójainak észlelte a winlogon.exe-t:
www.h-online.com/security/Bitdefender-and-GData-delete-winlogon-system-file--/news/112652

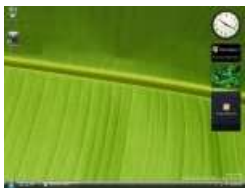
Antivírusok, amik már támogatják a Windows7-et

2009.02.18. 14:07 | Csizmazia István [Rambo] | 3 komment

Címkék: microsoft nod32 eset antivirus windows7 kompatibiltás

A Windows7 pontos megjelenési dátuma nem ismert, de gőzerővel dolgoznak rajta, és talán meglátszik majd rajta a Vista miatti csorbakiköszörülési szándék;-) Mivel már sokan aktívan bétáznak, nem árt tudni, **hogyan is állnak az antivírusok gyártói a kompatibilitással**.

Alig egy hónapja játszadoztunk mi is egyet a Windows7 bétára ráeresztett ESET Smart Security 4.0 bétával, ami a lehető legjobban végződött, és természetesen a NOD 32 programra is ugyanúgy igaz. Most egy olyan blogot találtunk, ahol temérdek **szabadidőben és kísérletező kedvben nem volt hiány**, így egy részletes összefoglalóban tekinthetjük át, ki vitte már át a lécet, és kinek kell még reszelnie a magasugró technikáján.



Antivírusok, amik már együttműködnek a Windows 7 Betaval:
AVG, Kaspersky, Norton, ESET NOD32, Avast, Avira, BitDefender

Akiknek még kell tenni az ügy érdekében:
McAfee VirusScan Plus, Trend Micro Internet Security Pro, eScan, AhnLab

A végeredményt pedig hamarosan, **nagyjából 2009. évvégén, vagy 2010. elején fogjuk meglátni**, ugyanis ez a Windows7 hivatalos megjelenésének valószínűsíthető dátuma.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Utaljunk pénzt a S.O.C.A.-nak
- Nyári tanácsok utazáshoz
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/950524

Kommentek:

Gratulálok mindkét csapatnak. A Nortont leszámítva nincs meglepetés, a profik hozzák a papírformát, ami viszont elképesztő, hogy a Vistával 99%-ban kompatibilis Windows7-re is sikerült egyes cégeknek vackot gyártani. Ideje lenne már egyszer átolvasniuk az UAC és társai részt az MSDN-ben - ha már a Vista megjelenésénél bealudtak.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.06. 20:26:03

Nem minden alakul jól a Win7 háza táján a mi szempontunkból. Az Autorunt végre valahára kiszedték, de erről meg úgy tűnik elfeledkeztek?!:
itcafe.hu/hir/ismert_fajltipusok_kiterjesztesenek_elrejtese_wind.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.15. 10:49:12

Fertőzött Windows 7 RC zombihálózatos mellékhatásokkal:
itcafe.hu/hir/veszelyes_windows_7_rc_warez_botnet_zombihalozat.html

Ez az iTunes nem az az iTunes

2009.02.19. 16:13 | Csizmazia István [Rambo] | 5 komment

Címkék: spam itunes hamis viagra feladó

Minden elektronikus levelezésben résztvevő kialakított már magának egy képet, egy szabályrendszert, mire érdemes figyelni, mire kell vigyázni. **Ezt vagy önként és belátva tette, vagy pedig a munkahelyi rendszergazdája, főnöke ösztökélésére változtatott**. A mai spam helyzetet tekintve azonban egyszerűen **nincs olyan levél vagy feladó, aminél ne kellene gyanakodni legalább egy picit**.

Hogy milyen remekül működik a bejáratott reflex - **azaz agy kikapcsol, kéz kattint** - azt jól példázza az a **kísérlet a baráti körből, amely az IWIW üzenetek mintájára, azt tökéletesen lemásolva, de a linket egy fiktív sajáttal helyettesítve** küldözgetett szét köztünk, figyelve a reagálásunkat. **Az eredmény ugye sejthető, a "[iWiW] Balázs ismerősnek jelölt" üzenetre szinte mindenki gondolkodás nélkül kattintott**, kiez-már-és-mit-akar-miért-nem-hagynak-már-békén-dolgom-van-na-jó-gyorsan-nézzük-meg alapon.

A hamis levélben aztán az a bizonyos link már nem a jól ismert helyre vitt, hanem a "Hehe, Ez egy adathalász levél volt. Megszívtad?!" kezdetű landing page tudatta, **hogy a delikvens nem volt elég elővigyázatos**, és sokkal rosszabb is történhetett volna.

Hogy ez a módszer már az elvi kísérletezéseken is túl van, arról már talán mi is írtunk, nem létező AdWords számla érkezett, fel nem adott futárküldeményünkre hivatkozó levél, látszólag nem kézbesíthető visszapattant levélnek látszó üzenet kártevőre mutató linkkel (Mail Delivery Notification) és hasonlók érkeznek, sőt néha mi magunk vagyunk a feladó :-). **Most egy újabb érdekesség bukkant fel, ami minden iPhone tulajdonost érinthet**, aki "küldföldiül" ;-) kap levelet.

Az közismert, hogy akár vásárolunk valamit, akár nem, **sőt még az ingyenes App Store alkalmazásokról is kapunk rendszeres időközönként 0.00 egyenlegű számlát**. Erre épít a mostani spamlevél, és itt még a nyelvi korlátok sem működnek. Levelünk belseje azonban cseppet sem hasonlít a szokásos számlákhoz.

Igaz, **szerencsére ez a mostani küldemény nem egy kártevőterjesztő oldalra, hanem "csak" egy kanadai gyógyszerész lapra mutat**: Viagra, Cialis és társai. Én a küldő helyében valamilyen tartozást tüntettem volna fel, és mellé a trükkös linket - de vélhetően csak idő kérdése, és lesz majd sajna ilyen is.

Szóval, **csak lassan azokkal a pavlovi reflexekkel!** Ahogy Fülig Jimmy vigyorgásáról sem szabad elhamarkodottan ítélni - mert az ilyen emberek, felépülésük után, sokat gondolkodtak a látszat megtévesztő benyomásairól, és elhatározták, hogy a jövőben senkiről sem vonnak le következtetéseket alapos tájékozódás híján - úgy **az "annak látszó" levelek is lehetnek időnként mások**, tehát érdemes nem kapkodni és jobban odafigyelni.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/953019

Kommentek:

// Gery Greyhound · http://gerygreyhound.tumblr.com 2009.02.20. 11:00:18

Éledezik a hazai spambiznisz? Én a héten már életemben először anyanyelvemen olvashattam Viagra-hirdetést:

noob.hu/07/0220/viagra_hu.jpg

De szeretnék Budapesten magyar spammert orrba rugdosni...

Lilieth 2009.02.20. 14:30:29

Szia,
ne haragudj, hogy ide írok, de már nincs jobb ötletem. A Nod-om egy módosult win32/PSW.LdPinch trójait talál, konkrétan két file-ban, az egyiket átugorja, a másikat meg ugyan engedi karanténba helyezni, de akárhányszor eresztem rá a vírusírtást, mindig ugyanúgy ott van. Próbáltam csökkentett üzemmódban is, bármilyen beállítás mellett csak és kizárólag a kihagyás gombot hagyja használhatónak. A file egy olyan könyvtárban van, amibe belemenni nem tudok, hogy töröljem. Tudnál segíteni?
Előre is köszönöm.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.21. 19:43:47

Szia Akutyamegamacska!

Ez egy jelszólopó fajta kártevő. Esetleg lehet, hogy ez a fájl az ideiglenes fájlok között van pl. a "C:\Documents and Settings\%username%\Local Settings\Temp\Content.IE5? Próbálj meg egy böngésző cache / átmeneti állományok törlést végrehajtani.

Ha nem sikerül így leszedni, akkor pedig érdemes lenne írnod a support kukac sicontact pont hu címre, vagy felhívni telefonon a supportos srácokat, ők mindenben segítenek, ha kell, akár lépésről lépesre részletesen távvezérelnek, mit kell tenni a mentesítéshez :-)

Lilieth 2009.02.22. 15:37:26

Köszönöm szépen :)

immortalis · http://immortalis.blog.hu/ 2009.02.24. 20:09:45

Szombat egész nap vírust irtottunk a gépemről. Rohadjon meg az összes.

Antivirus 2010 már a nyakunkon

2009.02.23. 15:33 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hamis antivírus 2010 antivirus rogue

Mikor a 2001 Ürodüsszeia című filmet néztem a 70-es évek elején a Corvin moziban, gyerekfejjel még reménykedtem, talán tényleg ilyen lesz a fejlődés, és már én is ilyen űrhajóval fogok közlekedni.

2001-ben aztán szembesültem azzal, hogy ilyen űrhajósdi még 2050-ben sem lesz sehol ilyen formában, hogy a magyarországi esélyekről külön már ne is beszéljünk (lesz, de csak a műanyag maketteket forgalmazó játékboltokban ;-).

Van viszont egy hely, ahol már javában készülnek a 2010-re, és ez nem szovjet-amerikai közös űrutazás előkészítése a Jupiterre, hanem a hamis antivírusgyártók futószalagjáról legördülő csalárd program kártevő formájában.

Úgy tűnik, sosincs elég korán elkezdeni a terjesztést, **máris megjelent és fertőz az Antivirus 2010**. Olyannyira, hogy már a How to remove... kezdetű útmutató közzététele is szükségessé vált. A hamis antivírus programok terjesztése egy **olyan új és jól jövedelmező iparággá** vált, amely nem csak a megtévesztéssel, a kiemelkedő jövedelem megszerzésével, az esetlegesen megadott banki azonosítókkal való visszaélésekről lett híres-hírhedt, hanem arról is, hogy **igen nehezen lehet a gépet megszabadítani a kéretlen kártevőtől**.

A mentesítéshez **sok esetben nem elegendő a futtatható fő EXE állomány törlése**, de a további programkomponensek és Registry bejegyzések eltávolítása is szükséges, ami egy átlagfelhasználó számára segédprogram vagy megfelelő tudás nélkül időnként meglehetősen nehézkes lehet. Nem kevésbé riasztó lehet számára egy nem létező vírusriasztási ablak vagy egy szimulált lefagyási (BSOD) képernyő. Ilyenkor **jöhet jól egy jó technikai támogatás, ahol a support csapat magyar nyelven, telefonon vagy e-mailben naprakészen tud segíteni** az aktuális fertőzés kiküszöbölésében.

Reménykedjünk, hogy az Antivirus 2011 nem a jövő héten fog megjelenni. **Atomot a hamis antivírus fejlesztőknek! ;-)**

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/960535

Kommentek:

Nincsenek hozzászólások.

A válság vámszedői

2009.02.25. 17:21 | Csizmazia István [Rambo] | 1 komment

Címkék: spam bank válság csalás kártevő megtévesztés

Ha pang a gazdaság, mindenki fogékonyabb egy kecsegtető álláslehetőségre, kedvezőnek látszó üzleti ajánlatra vagy egy alkalmi vételre. A rossz hír az, hogy **ingyen ebéd sajnos továbbra sem létezik**, ellenben leleményes csalók, kártevőterjesztők annál inkább.

Ha csak a szofisztikált magyar nyelvű spamekről van szó, úgy biztonságban vagyunk, nyelvi elszigeteltségünk miatt szerencsére az ilyesmi elég ritka. Ha azonban már az angol nyelvű üzeneteket nézzük, vannak hazai postafiókba érkező próbálkozások jócskán.

Lehet ez egy banki figyelmeztetésnek látszó üzenet, amely látszólag pont arra igyekszik rávenni bennünket, hogy **látogassunk el weboldalukra, amelyen megoldást ígérnek a hitelkártya tartozásunk alacsonyabb törlesztő összeggel való fizetésre**. Az oldal azonban bekéri az adatainkat, amely segítség vagy alacsonyabb fizetési részlet helyett azonnal a csalók kezébe kerül. Akik a PhishTank Sitechecker plugint használják, elkerülhetik a hasonló, már felismert csali oldalakat.

Ugyancsak reneszánszát élik a pénz helyettesítő kuponok is - egy mamutcombért kifestem a barlangodat ;-) - de amellett, hogy az eredeti cégek is túl sok adatot igyekeznek bekérni tőlünk, a fertőzött oldalak a **kedvezményes kupon letöltése helyett kártevőt, kémprogramot telepítenek a gépünkre**.

A harmadik esetben pedig **szemérmetlenül adathalászatra figyelmeztetnek bennünket egy hazug levélben**, és hivatkoznak a Federal Reserve Bankra. Aztán ha valaki kattint, **nem éppen egy banki oldalon találja magát...**

2009. akár tetszik, akár nem, a válság, a recesszió időszaka lesz. **Fel kell készülni, hogy trükkös csalók ezrei még jobban igyeznek majd egymásra licitálva megkaparintani a gyanútlan felhasználók pénzét, jelszavait**. Remélhetőleg talán mostanra már senki nem érzi tévesen úgy, hogy neki aztán nincs vesztenivalója. Ebben **a nehéz időszakban nem csak a hamis villanyóra leolvasót nem szabad a lakásba beengedni, de az elektronikus leveleink között is érdemes** hasonló szigorral és gyanakvással szelektálni.

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/965526

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.05.15. 12:54:38

Hamis sarokszelep, van új a nap alatt:
www.vfk.hu/?oldal=fooldal&id=hirek&art_id=53

Hamis rendszerüzenetek II.

2009.02.27. 13:01 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: social facebook megtévesztés engineering rendszerüzenet

Egy korábbi postban már mutattunk példát olyan rendszerüzenetnek látszó ablakra, amelyet éppen a kártevő jelenít meg. Mivel **nem várható, hogy a vírusok, férgek, kémprogramok a jövőben egy "Vigyázz, fertőző vagyok" feliratú táblával a nyakukban sétáljanak**, tendenciának is értékelhetjük az ilyen, hiszékenységre építő módszert.

Lassan ez is kinövi magát egy olyan rovattá, mint a "Kevésbé foglalkoztatott bébiszitterek" bemutatója. Ha nem is rendszerüzenet, de üzenet az is, amikor a hamis antivírus programok nem létező fertőzést mutatnak. **Azonban akkor és ott** a tapasztaltabbak rögtön látják, hogy a "Ki beszél most?" kérdésre **nem a Windows, hanem valami szánalmas alkalmazás próbálkozik**, amit **ráadásul nem is mi indítottunk szándékosan**. Vagyis a módszer lényege, hogy egy legitim alkalmazás legitimnek látszó üzenete jóval nagyobb eséllyel verheti át az áldozatot.

Emlékezhetünk, hogy a bevehetetlennek tartott OS X platform **sincs biztonságban akkor**, ha a hamis videokodek letöltésre invitáló ablakra maga a felhasználó nyomja entert, **maga telepíti azt, és gépeli be**, ha kell az adminisztrátori jelszót. És mivel **az idők végezetéig nem lehet arra építeni,** hogy a Mac juzerek azok kivétel nélkül tudatos emeber, akik sosem tévednek, sosem kapkodnak, sosem figyelmetlenek, ez előbb-utóbb ki fogja nyitni a AV piacot ebbe az irányba is, ami az emelkedő felhasználó szám miatt várható is.

Legutóbb arról olvashattunk, hogy a Facebookfelhasználók kerülhetnek veszélybe, ha figyelmetlenül kattintanak egy szintén rendszerüzenetnek látszó ablakra. A kártevő akkor **profilunk minden adatához** hozzáfér, és "jólelkűen" **felajánlja az "elromlott" profiladatok kijavítását, de ezzel magának a kártevőnek a továbbterjesztése történik meg**. Igaz, szerencsére valós károkozás nem történik, de a terjedés sebessége mindenesetre figyelemre méltó és egyben figyelmeztető.

A kocsmai verekedéseket megelőző három kérdés mintájára (Mivan? Mivan? Mivan?) **legalább ugyanennyi kérdést, illetve időt kellene magunknak is adni**, egyáltalán hihető-e, szokványos-e egy-egy ilyen rendszerüzenetnek látszó tárgy, és még ha esetleg az is, akkor sem kötelező rákattintani vagy begépelni abba az adatainkat.

Persze **az sosem valósul meg, hogy minden egyes felhasználó mindig minden programot, folyamatot, szándékot, üzenetet átlásson és értsen**, de azért törekedni kell rá, ahogy a buddhisták is törekszenek a teljességre, bár jól tudják azt elérni szinte lehetetlen.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/969189

Kommentek:

Nincsenek hozzászólások.

Sok kicsi trójai sokra megy

2009.03.02. 08:30 | Csizmazia István [Rambo] | 1 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az új esztendő februárjában a múlt havi listán debütált Conficker mellett **nem kevesebb, mint hat trójai program is szerepel**. Ez pedig továbbra is azt erősíti, hogy **megtévesztve bár, de mégiscsak mi saját magunk kattintunk** és telepítjük a kórokozók jelentős részét.

Az **ESET Magyarországra vonatkozó, több százezer hazai felhasználó adatai alapján** készült statisztikája szerint a toplista első helyezettje érdekes módon nem a Conficker féreg lett, hanem a Win32/TrojanDownloader.Swizzor trójai. Mielőtt ezt a kártevőt megvizsgáljuk, tegyünk egy icipici kerülőt a történelem órák világába, pontosan miért is hívjuk trójainak a megtévesztő programokat. A görögök építették azt a mondabeli híres, fából készült hatalmas lovat, **amelynek belsejébe a ravasz Odüsszeusz tanácsára a legbátrabb görög harcosok rejtőztek el**. A falovat a csatamezőn hagyták, majd hajóikkal cselesen visszavonulást színleltek. A trójaiak Kasszandra és Laokoón figyelmeztetése ellenére bevontatták a falovat a városukba, a hatalmas és bevehetetlen falak mögé. És ez lett a vesztük, mert **az éjszaka leple alatt a görög harcosok kimásztak a faló belsejéből**, megnyitották a város kapuit és a beáramló görög seregek sok évnyi hiábavaló háborúskodás után végül mégis elfoglalhatták Trója városát – igaz nem erővel, hanem ésszel.

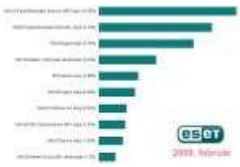
Ahhoz képest, hogy a megtévesztés eme példabeszéde már igencsak régi, a tanmesei csel ugyanúgy alkalmazható a modern körülmények között is. Csak nem isteni kiengesztelő szoborként, hanem **ingyenes alkalmazásként, hasznos utilityként, aranyos kölyökállatokat ábrázoló virtuális képeslapként, ingyenes antivírusként, könnyű internetes keresést segítő böngészőeszköztárként, vagy éppen lopott programok licenckulcsgenerátoraként** kell feltüntetni - de az elv ugyanaz. **Nem azt kapjuk, amire számítunk, hanem annál sokkal rosszabbat**.

A Trojan.Downloader.Swizzor trójai egy olyan régebb óta jelenlevő kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre, amely **többnyire reklámprogramokat töltöget le**, illetve ilyeneket telepít. A Swizzor terjedéséhez szinte minden esetben a hiszékenységet is kihasználja, sokszor olyan hasznosnak tűnő alkalmazásként álcázzák, mint például a Torrent letöltések sebességét optimalizáló segédeszközt.

Bár ezúttal nem került dobogóra, azért **továbbra is bérelt helye van a Conficker féregnek**, most a 7. helyet tudta bebiztosítani magának. Emellett persze új versenyzőket is üdvözölhetünk a páston, szám szerint hármat is.

A Win32/Kryptik trójai (vagy más néven Waledac) jó ismerős lehet annak, aki a **Valentin napi képeslapokkal kapcsolatos** vírusfigyelmeztetést olvasta. Pontosan ez a kártevő lapult annak az ártatlanul kinéző két kis kölyökkutyát piros szívvel ábrázoló weboldalnak a mélyén, amely üdvözlő kártya készítő programként hirdette magát.

Ugyancsak első ízben foroghat a helyezettek között az a Win32/Injector trójai, amely **adatokat igyekszik ellopni gépünkről, miközben orosz weboldalakról letöltött további szoftverkomponenseit rootkit technikával igyekszik elrejteni** a Windows szokványos fájlkezelő eszközei elől.



És végül, de nem utolsó sorban a szintén kéretlen reklámokban utazó Win32/Adware.GooochiBiz, amely működése közben **távoli webcímekre csatlakozik és onnan reklámokat tölt le, de emellett hátsóajtót is nyit a rendszerben**, melyen keresztül a távoli támadó később is könnyen hozzáfér a már megfertőzött számítógéphez.

Összességében elmondhatjuk, akár megtévesztéssel kerül olyan kártékony alkalmazás a gépünkre, amely nem az aminek mondja magát, akár kéretlen reklámokat megjelenítő mindössze „idegesítő" programról van szó, **jó lenne, ha számítógépünkön csak azok a programok futnának, amit mi szeretnénk, amiket szándékosan telepítettünk**. Ehhez persze szükséges az oly sokszor hangoztatott naprakész és frissen tartott operációs rendszer, szoftverkörnyezet valamint biztonsági programjaink. De – és talán ezt nem lehet elégszer hangsúlyozni – a **meggondolt és óvatos internethasználat és az alaposan megválasztott alkalmazások telepítése** is nagyon fontos.

Végül következzen a magyarországi toplista. Az ESET statisztikai rendszere szerint **2009. februárjában az alábbi 10 károkozó** terjedt a legnagyobb számban. Ők együttesen 44.95%-ot tudtak a teljes tortából kihasítani maguknak, vagyis ezúttal a szokásosnál nagyobb szeletet hasítottak ki a toplisták a tortából..

1. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége a februári fertőzések között: 10.86%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat töltöget le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a „csomagban". Emellett hátsóajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-nbf

2. WMA/TrojanDownloader.GetCodec trójai
Elterjedtsége a februári fertőzések között: 5.23%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.

Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

3. Win32/Agent trójai
Elterjedtsége a februári fertőzések között: 5.13%

Működés: .Ezzel a gyűjtőnévvel azokat rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.

A számítógépre kerülés módja: .a felhasználó maga telepíti
Bővebb információ: http://www.eset.hu/virus/agent

4. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a februári fertőzések között: 4.67%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

5. INF/Autorun vírus
Elterjedtsége a februári fertőzések között: 4.45%

Működés: INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

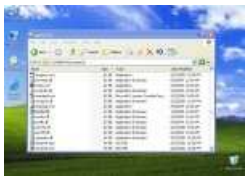
6. Win32/Kryptik trójai
Elterjedtsége a februári fertőzések között: 4.06%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.
Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/kryptik-gt

7. Win32/Conficker.AA féreg
Elterjedtsége a februári fertőzések között: 4.03%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call) vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: a felhasználó maga telepíti
Bővebb információ: http://www.eset.hu/virus/conficker-a

8. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a februári fertőzések között: 3.37%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyű leütés naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Tényekedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására és a jelszó adatok titokban való továbbküldésére fókuszál. A távoli támadó ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthat hozzá, amelyet aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

9. Win32/Injector trójai
Elterjedtsége a februári fertőzések között: 1.65%

Működés: A számítógépre kerülése után további kártékony komponensek letöltését kísérli meg orosz weboldalakról. Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Rootkit-szerű működése során fájlokat rejt el a fájlkezelő alkalmazások elöl (pl. EXPLORER, FAR MANAGER) még akkor is, ha ezek eredetileg nem rejtett attribútummal ellátottak. Fertőzésre utalhat a C:\ WINDOWS\ system32\ ntos.exe állomány jelenléte is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/injector-k

10. Win32/Adware.GooochiBiz alkalmazás
Elterjedtsége a februári fertőzések között: 1.5%

Működés: A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működése közben távoli webcímekre csatlakozik és onnan reklámokat tölt le. Sok kártevő vet be olyan trükköket, amellyel saját lelepleződésüket igyekeznek elkerülni. Az Adware.GooogchiBiz a tasklistában is nyomon követhető folyamatok közül a normál körülmények között is megtalálható iexplore.exe mögé igyekszik elbújni. Emellett hátsó ajtót is nyit a rendszerben, melyen keresztül a távoli támadó később is könnyen hozzáfér a már megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-gooochibiz

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/973076

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.03. 14:37:34

Szia Cotomm!

Pedig ott van. Például botnetes cucc a listában szereplő Kryptik is, amely a Valentin napi képeslapokban is szerepelt. Az elnevezésbeli különbségek miatt egy-egy kártevő az egyik cégnél Kryptik, a másiknál Waledac, a harmadiknál Zhelatin :-P

Kedvenc kommentjeink

2009.03.03. 14:46 | Csizmazia István [Rambo] | 3 komment

Címkék: blog vírus kocka antivírus

Új rovatot indítunk, amellyel **teljesen rendszertelenül**, de sőt, ha és amennyiben, valamint annál inkább, és különben is ;-)

A Zs kategória című blogban bukkantunk egy érdekes posztra, amely **a filmekben előforduló Kocka / Geek karakter sommás összefoglalóját adja**, a figura jellemzőinek pontos és élethű leírásával. A poszt maga is érdekes, sőt magán a blogon is található ezenkívül számos további szórakoztató bejegyzés, mi azonban most mégis a ZSsablon karakter: A kocka technikus bejegyzés **egyik kommentje miatt tűztük napirendre**, következzen DrGenya hozzászólása:

Kedvencem: Függetlenség napja
*Az öregedő kocka (micsoda szakítás a sablonokkal) a tök idegen lények tök idegen hardwerébe a tök ismeretlen op rendszerre valamilyen interfészen benyomja a rögtön flottul működő vírust, ami aztán az ezek szerint pángalaktikusan ismert halálfejjel hívja fel a csúnya földönkívüliek figyelmét, hogy oppá, baj van.**Tanulság, ha elindulsz leigázni a Földet, szerezz be előtte egy Chip Magazint, mert abban van ingyenes NOD32 :-D***

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/977495

Trackbackek, pingbackek:

Trackback: BuheraBlog 2009.03.04. 15:24:35

Kedvenc filmek/kommentekRambo posztján felbuzdulva úgy döntöttem, hogy én is írok egy kis kiegészítést a ZSkategória nagyszerű bejegyzéséhez, a filmekben megjelenített tipikus kocka informatikusokról. Az ihletet Mindfield kommentje adta:...Ez alól természe…

Kommentek:

cworm (törölt) 2009.03.04. 12:01:46

Nem akarom védeni a filmet, mert szerintem is hülyeség ez a vírus dolog, DE:
Ne feledjük, hogy a filmben már kb 50 éve ott volt a birtokukban az idegen űrhajó, szóval volt bőven idejük tanulmányozni az azon futó oprendszert, hardvereket, stb.:D Más kérdés, hogy ez az öregedő kocka valszeg nem ismeri a Zblorg programozási nyelvet, úgyhogy ebben az esetben ezen a ponton bukik a film.:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.10. 13:45:01

A Föld leigázására lehetőség van még PC World magazinnal is, hiszen abban is van ingyenes NOD32 ;-)

hatR 2009.03.24. 10:25:13

na, majd tudjuk akkor, hogy igazabol az eset, es az ingyenes probaverziok miatt lettunk leigazva :)

Bezáratta a német rendőrség a crackeroldalt

2009.03.05. 14:43 | Csizmazia István [Rambo] | 2 komment

Címkék: fórum kártevő kémprogram jelszólopás

A codesoft.cc oldalt mindenféle **jelszólopással kapcsolatos üzelmekre használták**, most pedig Baden-Württembergi rendőrség lecsapott.

A fórum kezeője és adminja egy 22 esztendős svájci fiatalember volt, aki többek közt a "Codesoft PW-Stealer 0.5" trójai kártevőt készítette és forgalmazta "tr1p0d" álnéven. A nyomozók most házkutatást tartottak nála, **lefoglalták a 2 TB-nyi anyagát** és minden ezzel kapcsolatos iratát.

A rendőrség már egy ideje figyelemmel kísérte a fertőzött gépekről kikerülő, illegálisan megszerezett **adatok áramlását, és eközben rátaláltak egy németországi szerverre**. Amikor pedig elemezték a hozzáféréseket ehhez a szerverhez, akkor sikerült azonosítaniuk két további gyanúsítottat, egy 25 éves és egy 27 éves férfit. Kettőjüket azzal gyanusítják hogy 2008 szeptembere óta 80 ezernél is több számítógépet fertőztek meg világszerte a Codesoft PW Stealer szoftverrel. **Az ellopott felhasználói adatokat, jelszavakat pedig a fórumon belül értékesítették**.

A csapat egyébként még a BlackHat oldalon is hirdette kétes szolgáltatásait, mostanra azonban a webhelyet már lekapcsolták.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/983036

Kommentek:

lolperec 2009.03.05. 19:06:55

@cotomm: jó kis parasztvakítás folyik a spamlink alatt, mindenkinek ajánlom! :D

Káposztakukac 2009.03.05. 19:07:12

most elképzeltem, hogy a magyar rendőrség hogy csap le az elektronikus bűnözésre...na jó, csak vicceltem :D

Legjobb support díjat nyert a Sicontact

2009.03.05. 22:47 | Csizmazia István [Rambo] | 4 komment

Címkék: technikai chip támogatás support nod32 eset győztes sicontact

A CHIP magazin az antivírus szoftverekhez társuló ügyfélszolgálatokat tesztelte. **A győztes a NOD32 vírusirtó forgalmazójának**, a Sicontact Kft.-nek support csapata lett.

A CHIP szakemberi a magazin tesztlaborjában állítottak össze egy számítógépet, melyet megfertőztek, majd szoftveresen is elrontottak, **hogy próbára tegyék, milyen segítségre számíthatnak az olvasók a különböző vírusirtó cégektől, ha megfertőződik számítógépük.** Az Avast, az AVG, a Norton, a Kaspersky és más vírusirtó cégek support csapata közül a **Sicontact munkatársai bizonyultak a legfelkészültebbnek**, egyedül ők tudták a fertőzött gépet lapzártáig megjavítani.

Idézet a magazin részletes értékeléséből:

*„Külön tetszett, hogy a Sicontact szakértői nem adták fel a problémás ügyféllel való foglalkozást, míg sok másik cégnél már régen az antivírus programgyártójának való hibajelentés küldését választották. (...) A Sicontact más területen is megelőzte a többieket, ez pedig **a távirányítós segítségnyújtás**: ha ügyetlenek vagyunk, akkor a cég munkatársai letöltetnek velünk egy programot, amellyel csatlakozhatnak számítógépünkhöz, átvéve az irányítást, és egyedül ők voltak, akik lapzártánkig képesek voltak megjavítani fertőzött gépünket."*

A részletes teszteredmények elolvasásához a CHIP magazin teljes cikke letölthető innen

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/983279

Kommentek:

cworm (törölt) 2009.03.06. 13:37:12

Kár, hogy a VirusBuster kimaradt a tesztből. ;P

r@ek (törölt) 2009.03.08. 10:48:51

szupport...

Az gyonyoru.. Csak gratulalni tudok...

!!szupport!!

Meg leirni is kinszenvedes igy! :-DD

r@ek (törölt) 2009.03.08. 10:50:05

Volt egy prog tanarom meg a hoskorban (Turbo Pascal rulla!) az mondta az Access-t "áccesz"-nek mindig :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.12. 15:09:57

@Cworm: Ezt a CHIP-nél lehet megreklamálni :-)

@Fiveeeee: Jogos a pont, kigyomlaltam a kinszenvedest.

Hibás frissítés okozhatott gondot

2009.03.06. 11:46 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hiba frissítés update support eset

Pár napja **egy hibás frissítés, a 3901-es csomag okozhatott gondokat egyes felhasználóknál**. Egész pontosan a lopakodás-ellenes, úgynevezett anti-stealth modulban volt a hiba, nevezetesen az 1009-es verziószámú em006_32.dat állományban. Ez a modul a felelős egyébként a rejtőzködő kártevők, például rootkitek hatékony felderítéséért.

Annyit tudunk, hogy **a 3-as verzió felhasználói lehetnek érintettek**, akár a NOD32 antivírust, akár az ESET Smart Security biztonsági csomagot használják. A vizsgálatok szerint az új, 4.0 termék, valamint a korábbi 2.7-es programverziók nem érintettek. Ráadásul ez a bizonyos modul nem is minden 3-as verziót használó gépen okozott gondot, hanem csak néhánynál, **pontos számokat nem ismerünk**.

Egyes problémás gépeken lefagyást lehetett tapasztalni. Ilyenkor újraindítva a rendszert, néhány esetben az ESS vagy EAV ezek után is változatlanul jelezhet modulbetöltési hibaüzeneteket. Ha a javított frissítés után a program működése mégsem javulna meg - ekkor a "0x101a update error" üzenet látható, akkor sajnos csak **az eltávolítás-újratelepítés segíthet teljesen kiküszöbölni** ezt a problémát.

Egy másik lehetséges megoldás lehet még, amit viszont **csak a tapasztaltabb felhasználóknak javasolnak**, ha SAFE módban indított számítógépünkön a "Program Files\ESET\ESET Smart Security" mappából letöröljük az összes "em0*.dat" állományt, ugyanis ezzel is rávehető a program a már helyes, javított modulok automatikus újratöltésére. A cég egy külön részletes útmutatót tartalmazó aloldalt is létrehotott a hibaelhárítása érdekében:
http://kb.eset.com/esetkb/index?page=content&id=SOLN2164

A kellemetlenségért **az ESET elnézést kért a felhasználóktól** és nagyon sajnálja a történteket. A **magyar forgalmazó Sicontact Kft. terméktámogatási csoportja pedig minden érintettnek igyekszik megadni a szükséges technikai segítséget** mind e-mailben, mind pedig telefonon.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/985026

Kommentek:

Nincsenek hozzászólások.

Megjelent az új NOD32 4.0

2009.03.06. 12:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: security új smart verzió nod32 eset 4.0

Az otthoni felhasználók számára **játékos üzemmódot és helyreállító CD készítésének lehetőségét**, a vállalati rendszergazdák számára pedig **beépített rendszerfelügyelet** tartalmaz az ESET termékeinek 4. generációja.

Angol nyelven már elérhető az ESET 4. generációs NOD32 vírusvédelme és integrált biztonsági programcsomagja, az ESET Smart Security. A vírus- és kémprogramvédelmet nyújtó NOD32-t, és az ezen kívül személyi tűzfalat és levélszemétszűrőt tartalmazó internetbiztonsági csomag **még hatékonyabb vírusfelismerés, gyorsabb ellenőrzési sebesség és továbbra is alacsony rendszerterhelés** jellemzi.

Mindemellett jelentősen bővült a szoftverek által nyújtott szolgáltatások köre is. Ezek közül a legérdekesebb a játékos üzemmód, valamint a helyreállító CD létrehozásának lehetősége. Az előbbi funkció segítségével teljes képernyős használat esetén a szoftverek figyelmeztetőablakainak felugrása letiltható. Ennek elsősorban a játékok és a prezentációk során van jelentősége. A **helyreállító CD segítségével pedig lehetővé válik a fertőzött rendszerek külső forrásból történő ellenőrzése**. Így olyan esetben is megtisztíthatók a számítógépek, **amikor egyébként a merevlemez kiszerelésére lenne szükség**.

A 4. generációs ESET szoftverek azt is képesek érzékelni, hogy a számítógép akkumulátorról vagy hálózatról működik-e, és ennek megfelelően időzítik az ütemezett feladatok végrehajtását. **Ez a funkció a notebookok esetében megnöveli az üzemidőt**. A vállalati felhasználók számára ezen kívül jó hír, hogy **az új termékekbe bekerült az eddig önálló szoftverként létező ESET SysInspector** rendszerfelügyeleti alkalmazás, mely lehetővé teszi az aktuálisan futó folyamatok és a rendszerösszetevők elemzését.

Az új funkciók mellett **az ESET szakemberei a programmodulok tökéletesítésén is sokat dolgoztak**. „A folyamatos fejlesztésnek köszönhetően a szoftverek új verziói a piacon jelenleg elérhető biztonsági szoftverekkel összehasonlítva kiemelkedően alacsony rendszerterheléssel rendelkeznek, így gyors betöltést és zavartalan működést biztosítanak” - emelte ki Csiszér Béla, az ESET magyarországi képviseletét ellátó Sicontact Kft. ügyvezetője.

Az **új szoftverek magyar nyelvű változatai néhány hónapon belül megjelennek**. Az ESET üzletpolitikájának köszönhetően azok a felhasználók, akik most vásárolják meg termékeket, vagy már rendelkeznek érvényes licenccel, egyaránt használhatják az aktuális magyar nyelvű változatokat, vagy a most megjelent angol nyelvű szoftvereket, és az új generációs programok **magyar nyelvű változatára azok megjelenésekor ingyenesen áttérhetnek**.

Az **új szoftverek angol nyelvű próbaverziója a következő linkről** tölthető le:
http://www.eset.hu/letoltes/proba
(A NOD32 antivírus próbaváltozatának letöltése regisztráció nélkül lehetséges, az ESET Smart Security próbaváltozatának letöltéséhez regisztráció szükséges.)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/985107

Kommentek:

Nincsenek hozzászólások.

A válság vámszedői II.

2009.03.09. 14:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: csalás kártevő kupon waledac kryptik

"Végre" mi is kaptunk a korábbi postban megírt **kéretlen kuponos spamlevélből**. Egyet már most jelezhetünk, nem lehetett vele olcsóbban vásárolni. **Hogy miért pont Eger**, az számunkra egyenesen rejtély.

Mint azt az első részben már jeleztük, a kiolvasott IP címből országonként testreszabottan jelenik meg a böngészőben a kuponos hirdetés. Nekünk az alábbi szöveggel jelent meg: **"Exclusive sale coupons and deals at over 1 000 stores in Eger, Hungary."**

Valószínűleg senki nem lepődik meg, a kedvezményes kuponra kattintás illetve a teljes impreszum összes linkje is a **"coupons.exe", "nocrisis.exe" vagy "sales.exe" kártevő állományt akarja letölteni** a gépünkre.

Ami viszont az alábbi eredményeket bírja produkálni a VirusTotal vzsgálatnál, szerencsére mindegyik esetben **detektál a heurisztika "a variant of Win32/Kryptik.JX"** jelzéssel. A magunk részéről ez a kuponosdi már alaphangon nem szimpatikus, de így pedig aztán végképp nem lesz a szivünk csücske.

A tanulság talán annyi lehet, sose kattintsunk olyan weboldalon, **amelynél minden felső és alsó link:** a Join us, a Contact us, az impresszum **és az összes többi is egyazon exe állományra** mutat.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/990871

Kommentek:

Nincsenek hozzászólások.

Hibás ESET frissítés ma hajnalban

2009.03.09. 14:32 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: frissítés support nod32 eset hibás

Ma reggel 5 óra 50 perctől **körülbelül 10 percen keresztül** egy hibás frissítés volt elérhető az ESET biztonsági szoftvereihez. A Magyarországon feltehetően kevés felhasználót érintő hiba elhárítása megtörtént.

A NOD32 antivírus 2.7-es, 3.0-ás, 4.0-ás, valamint az ESET Smart Security 3.0-ás és 4.0-ás változatainak azon felhasználói, **akik ma hajnalban 5 óra 52 perc és 6 óra között frissítették** szoftvereiket, azt tapasztalhatták, hogy a programok frissítése után vírusriasztás érkezik. A téves riasztást egy hibás frissítés generálta, mely után **a NOD32 antivírus és az ESET Smart Security tévesen Win32/Kryptik.JX kártevőnek** minősítette a Windows egyes rendszerfájljait.

A heurisztikai modul hibája a 3918-as vírusdefiníciós adatbázissal együtt került telepítésre. Az ESET néhány percen belül észlelte a hibás frissítést, és leállította azt. **A javított verzió a 3919-es sorszámú vírusdefiníciós adatbázissal ma hajnalban, 6 óra 30 perckor** került ki a frissítőszerverekre.

A 3.0-ás és 4.0-ás programváltozatok felhasználói úgy tudják ellenőrizni, hogy megfelelő frissítéssel rendelkeznek-e, hogy a jobb egérgombbal a programok tálcaikonjára kattintanak, majd **a névjegy menüpontban ellenőrzik a vírusdefiníciós adatbázis és a heurisztikai modul verziószámát**. A NOD32 antivírus 2.7-es változatának felhasználói a szoftver Vezérlőközpontjában, az Információ menüpontban tudják ellenőrizni ugyanezt. Amennyiben a 3919-es vírusdefiníciós adatbázis van telepítve, a programokat nem szükséges frissíteni. **Amennyiben ennél korábbi verziószámokat jelez a szoftver, érdemes frissíteni**, mivel a hibás frissítést az ESET már visszavonta, és a helyes, 3919-es (vagy ennél magasabb) verziószámú frissítést fogja telepíteni a program.

Azok a felhasználók, **akik ma hajnalban a hibás frissítést töltötték le, a számítógép bizonytalan működését tapasztalhatják**, ami annak köszönhető, hogy a NOD32 és az ESET Smart Security a tévesen kártevőnek minősített rendszerfájlokat **karanténba zárta**. Az ESET **még a mai napon kibocsájt egy újabb frissítést, mely a tévesen kártevőnek minősített rendszerfájlokat automatikusan visszaállítja a karanténból**. Azok a felhasználók, akiket érintett a hiba, és az automatikus javítást nem tudják megvárni, **jelenleg manuálisan tudják visszaállítani a blokkolt rendszerfájlokat**. A NOD32 antivírus 2.7-es változatának felhasználói kizárólag manuálisan tudják visszaállítani a blokkolt rendszerfájlokat.

A hiba Magyarországon valószínűleg kevés felhasználót érint. Az ESET szoftvereit hazánkban képviselő Sicontact Kft. ugyanakkor felhívja a figyelmet arra, hogy **a hibás frissítés által érintett számítógépeken nincs szükség az operációs rendszer újratelepítésére vagy más drasztikus beavatkozásra**, és kéri a felhasználókat, hogy a **+36 1 346 7048 telefonszámon vagy a support@sicontact.hu e-mail címen** vegyék fel a kapcsolatot a technikai supporttal.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/991375

Kommentek:

Nincsenek hozzászólások.

Frissítsük banki adatainkat - kéri az e-mail

2009.03.10. 15:07 | Csizmazia István [Rambo] | 5 komment

Címkék: spam apple adathalászat mobilme

Nos, erre a rövid válaszunk az lehet, hogy "nem"; a hosszabb pedig hogy "shanghaji táncosnő legyen az öreganyánk és baltával pucolja az ablakot, ha kéretlen levélben érkező linkre kattintva ilyet tennénk" ;-) Pedig az új divat elindult:a hamis **iTunes számla után** **itt a csalárd MobilMe figyelmeztetés**.

A beszámoló szerint néhány napja figyeltek fel arra, hogy MobilMe felhasználók olyan levelet kaptak, amely nem az Appletől érkezett. Bár a feladó látszólag a noreply@me.com, **a küldő valójában az Egyesült Királyságból küldte a gamma.oxyhosts.com szolgáltatón** keresztül. Kedvesen figyelmeztet, hogy **ugyan frissítsük már hitelkártya adatainkat, amelyek szerintük már lejártak**.

Másolt kinézet + figyelmetlen user = sikeres csalás
(hasonlóan, mint a szovjethatalom + villamosítás = kommunizmus ;-)

Mivel a figyelmetlen felhasználó bármilyen operációs rendszer előtt ülhet, ha maga kattint óvatlanul, akkor hiába nem Windowst használ. **Rootkitet éppenséggel lehet telepíteni bármilyen OS-re (Win, OS X, Linux, stb.), illetve ha adathalász oldalon begépeljünk banki vagy jelszóadatainkat, akkor platformfüggetlenül tudják a pénzünk lenyúlni**.

Még ha az Apple kérné is, SSL nélkül akkor sem jó ómen az ilyesmit kitölteni

Sajnos **várhatóan gyarapodni fog az ehhez hasonló esetek száma**, így már most érdemes lelkileg előre felkészülni a hamis AdWords, Facebook, iWiW, Vatera, stb. számlára, figyelmeztetésre, adathalász kísérletre. Ezért érdemes lesz a Pavlovi reflexeket a szögre akasztani, és a hivatalok valamint bankok által küldött levelek mellett **bármilyen más témánál is nyitott szemmel**, figyelmesen és gyanakodva eljárni.

Különösen pedig akkor ajánlott résen lenni, ha az adott oldalt csak az előző héten jegyezték be...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/993493

Kommentek:

Fedor · http://fedor.blog.hu/ 2009.03.10. 17:29:31

Bizonytalan vagyok. Én pont ma kaptam egy hasonló levelet, az volt az első gondolatom, hogy ez átverés. Viszont egyáltalán nem volt benne kattintható link. Szerintetek?

_____

-------- Eredeti üzenet --------
Tárgy: ELMŰ biztonsági frissítés
Dátum: Tue, 10 Mar 2009 11:35:28 +0100
Feladó: ELMŰ Ügyfélszolgálat
Válaszcím: elmu@elmu.hu
Címzett:

Tisztelt Ügyfelünk!

Igazodva napjaink internetbiztonsági elvárásaihoz és ügyfeleink igényeihez, internetes ügyfélszolgálatunk korszerűsítése mellett elvégeztük a rendszer biztonsági átvizsgálását és frissítését is.

Az új elvárások az ügyfeleink által beállított jelszavak biztonsági szintjét is érintik, ezért az online ügyfélszolgálat felületére történő következő bejelentkezése során automatikusan leellenőrizzük jelenlegi jelszava megfelelőségét. Ha a jelszó biztonságossága nem éri el
legalább a közepes szintet, meg kell változtatnia azt.

Új jelszavát úgy kell megadnia, hogy az megfeleljen az alábbi
elvárásoknak:

- Jelszó hossza: minimum 8 karakter
- Alkalmazható karakterek, melyek közül minimum 3 típus
használata kötelező:
o abc kisbetűk
o ABC nagybetűk
o számok
o speciális karakterek (például: .,/)

Amennyiben a biztonsági elvárásoknak megfelelően sikerült megadnia új jelszavát, a választott jelszó erőssége a grafikus ábrán közepes (sárga), vagy magas (zöld) minősítést kap. Piros jelzés esetén a választott szó nem felel meg a biztonsági kritériumoknak, ezért tovább kell próbálkoznia.

Kérjük, hogy látogasson el minél előbb weboldalunkra, és ha a rendszer jelzése szerint jelenlegi jelszava nem elég biztonságos, végezze el annak módosítását.

Együttműködését nagyon köszönjük!

Tisztelettel,

ELMŰ Ügyfélszolgálat

cworm (törölt) 2009.03.11. 09:59:30

Nekem igazinak tűnik, mert nincs benne link, szal nem próbálnak meg hamis oldalra irányítani, hanem csak azt mondják, hogy látogasd meg az oldalukat. Szerintem ez így jó.:) Bár erről lehet, hogy nem kéne levelet küldeniök, hanem bejelentkezéskor elég lenne közölni a cuccot.

A cikkre visszatérve: szerintem az, hogy valaki milyen platformot használ, az sokat elárul arról, mennyire konyít az informatikához, és szerintem azoknak a többsége, akik nem wint használnak, nem szopják be az ilyen típusú leveleket. Szóval még így is a wines felhasználók vannak kitéve a legnagyobb veszélynek, de nem az oprendszer miatt, hanem a tudásuk hiányosságai miatt.:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.12. 14:55:55

Szia Fedor!

Üdv a blogban :-)

Maga a levél nem tűnik csalásnak. Hogy miért kaphattad, az jó kérdés, nem regisztráltál véletlenül mostanában az E-ON weboldalán? Vagy kötöttél előfizetői szerződést, ahol az e-mail címedet is megadtad?

Lényeg a lényeg, ha valamilyen webhelyet meg akarsz látogatni, akkor ne a levélben kapott linkkel tedd, hanem a könyvjelzőből, vagy a jó kis Spee Dial Firefox pluginnel.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.12. 15:06:59

Hello Cworm!

Hát igen, lehet valamennyi icipici összefüggést belegondolni a platformba. Például a Mac azért nem olcsó, ha valaki ilyet vesz, akkor azt már nem véletlenül teszi, és talán óvatosabb ;-)

Ha Linuxozik, akkor szereti maga kézbe venni a dolgokat, és nem esik kétségbe, ha valami nem működik elsőre :-) És valszeg jobban hajlandó újat is tanulni.

Ha WIndows használ, akkor sem lehet dehonesztáló kifejezésekkel illetni, mert ugye hívhatják azt usert akár Bill Gatesnek is ;-), használhat CAD-et, SAP-t, Macromedia Flasht, CorelDrawt, stb, amik nincsenek más PC platformon. Persze azt aláírom, hogy mivel winuserből van a legtöbb, a "nem értek a géphez, de már annyira olcsó, hogy beteszek egyet a bevásárlókocsimba, hogy legyen nekünk is" típus nem Linuxot fog használni, és ugye a Win döntő többségben elő is van telepítve az új gépeken. Az Linux OS-sel ellátott noteszek alig pár éve kezdtek elterjedni, reméljük számuk majd tovább emelkedik.

A nagy kérdés ezekután már csak az, ha nekem az asztalomon van egy külön Windows, egy Linux és egy Mac gép is, akkor én most milyen user vagyok?! ;-)

cworm (törölt) 2009.03.13. 09:11:02

@Csizmazia István [Rambo]: Hát kérem akkor te super ultra power user vagy! :D

Windows frissítésre figyelmeztet az antivírus

2009.03.12. 16:19 | Csizmazia István [Rambo] | 3 komment

Címkék: frissítés biztonság patch javítás figyelmeztetés ms nod32 4.0 ess tálcaikon

Néhány napja jelent meg a 4.0 NOD32 és ESET Smart Security, amely számos újdonságot tartalmaz, például a helyreállító System Rescue CD lehetőséget is. Mi most ehhez képest **egy kisebb horderejű** új tulajdonságot mutatunk be, ami **ennek ellenére igen hasznos** lehet.

Reggel ágy, délben szék, este fogkefe - lassan ilyen kritériumoknak is meg kell felelnie egy minden veszély ellen hatékonyan óvó korszerű biztonsági programnak. Amit viszont **minden antivírus vagy kémprogramvédelmi eszköz használata mellett tudni kell**, hogy a mai exploitos világban **az operációs rendszer megfelelő karbantartása, a friss biztonsági javítások azonnal letöltése** és haladéktalan telepítése épp ugyanennyire elengedhetetlen.

Ezen segíthet, ha **a tálcaikon sárga színnel figyelmeztet**, valamilyen kisebb rendellenesség van rendszerünkben. Ha rákattintunk az ikonra, bővebb magyarázatot is kaphatunk.

Jó ötletnek tűnik ez az aprócska jelzés, bár alapvetően az a szerencsés, ha a Windows frissítések nincs letiltva, illetve azok fogadása automatikusan meg is történik. Sokszor **talán pont ennyi kellene csak**, hogy egy új sebezhetőséget kihasználó kártevőt elhárítson az ember.

Talán néhány felhasználónak ez adja majd a kellő impulzust a javítófoltok letöltéséhez. Bizakodjunk, azt nem tiltja a törvény ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/998077

Kommentek:

arvisura · turoczi.blog.hu 2009.03.15. 11:43:50

Köszönöm!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.29. 10:56:13

Állítólag a biztonsági frissítést mindenki megkapja, legyen a példánya bolti vagy lopott:
www.technet.hu/notebook/20090428/windows_mindenki_kap_a_biztonsagi_javitasokbol/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.13. 18:58:49

Másfél évig várt a Microsoft egy javítással:
index.hu/tech/2009/07/13/masfel_evig_vart_a_microsoft_egy_javitassal/

Legyen ön is bűnöző!

2009.03.16. 17:10 | Csizmazia István [Rambo] | 8 komment

Címkék: bbc kísérlet click botnet kódex etikai törvényesség

Nyilvánvalóan nem ez volt a szándékuk szerint sugallt üzenet, de az eset ennek ellenére komoly vihart kavart. Nem vették fél vállról az **"Ismerd meg az ellenséget"** mondást a BBC Click című számítástechnikai műsor készítői, akik illegális lehetőséget vettek igénybe, mikor **egy éles botnetet béreltek ki és mutatták be ennek használatát**.

Igaz, ami igaz, **a hatékony védelemhez valóban ismerni kell a bűnözők észjárását, technikai lehetőségeik határait**, és ilymódon sikerült is szemléletesen bemutatni a nézőknek, hogyan is megy ez. Mint emlékezetes, a **tv csatorna munkatársai egy chatszoba útján kibéreltek egy 22 ezres botnetet**, és azzal próbaképpen saját emailcímeiket megbombázták spamekkel, és egy előre egyeztetett saját célpont szervere ellen pedig DDoS támadást indítottak. Az akció teljes sikerrel zárult, már ami a szemléletes bemutatást illeti. **Remélhetőleg sokakban okozott "aha" élményt, és bepótolták az addig elhanyagolt Windows biztonsági frissítéseket e figyelemfelkeltés után**.

Viszont kétely maradt ezek után éppen elég. A BBC etikai kódex megsértéséről is sokan beszélnek, mert **bár a BBC nem akart törvénytelenséget elkövetni, mégis megtették azt**. Jogászok és biztonsági szakértők még hosszan el fognak vitatkozni pro és kontra, az érdemi történések linkjeit a későbbiekben majd kommentekkel bővítjük. Az pedig szintén kérdéses, hogy az esetleg jogszerűség vagy jogszerűtlenség mellett mennyire volt mindez etikus.

Az akcióval kapcsolatos erkölcsi kételyeket tovább fokozza, hogy a bemutató miatt a közszolgálati TV, azaz **az adófizetők pénze a bérbevett botnetes üzlet miatt közvetlenül a bűnözőkhöz került**. Egyes megközelítések szerint ez olyan, mintha gyújtogatást úgy mutatnák be, hogy közben egy épületet valóban le is égetnek a szemléletesség kedvéért, amire közpénzből egy gyújtogatót fogadnának fel.

Emellett teljesen jogosan felmerül a VírusHiradó cikkében az is, **ha egy célpont egyszer a bűnözők látókörébe kerül, azok akkor is felhasználhatják, megzsarolhatják, ha éppen nincs** is aktív fizető megbízásuk rá. Bekerülni könnyű, kikerülni szinte lehetetlen - tisztára mint egy BAR lista. Sőt **ezenfelül a megbízó is számíthat rá, hogy ha például a későbbiekben éppen polgármesternek jelöltené magát, korábbi törvénytelen megbízásának részletei sem maradnak majd titokban**.

A bemutató esetleges hátulütője lehet mindezeken felül még az is, hogy **éppen a törvénytelenségre hajló embereknek csinál kedvet a botnetbérléshez**, hiszen láthatták, **már 60 géppel is leültethető egy szerver**. És bár igaz, hogy spammelni és webhelyeket támadni is lehet egy botnettel, **a legnagyobb veszély mégis a kémkedés, a jelszavak és banki adatok eltulajdonítása** - szerencsére ezzel a riporterek most nem kísérleteztek a műsorban. A drogfogyasztást sem mutatják be közvetlenül a közszolgálati TV-ben részletesen, hogy hány fokos szögben érdemes a vénába szúrni a tűt, hol és mennyiért érdemes venni az olcsó és jó anyagot azzal, **hogy persze senki ne tegyen ilyet**. Szó ami szó, igencsak felemásra sikeredett végül az eredetileg látványosnak szánt számítástechnikai bemutató.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1005672

Kommentek:

nyomi 2009.03.16. 22:22:58

Vmiertelmes formatumban nem toltheto ez le? Egy linket vki esetleg :)
Erdekelne, hogy miket magyaraztak kozben. Es nemakarok poogarmester lenni

ftxpmj 2009.03.17. 00:35:08

A HírTV-n is adják ezt a műsort fordítással, szoktak benne lenni jó dolgok:
2009. március 17. kedd 13.05
2009. március 20. péntek 11.30
2009. március 21. szombat 13.05 és 21.30
www.hirtv.hu/?tPath=/musorok/&article_id=60289

ftxpmj 2009.03.17. 00:39:54

@nyomi:
vlc-vel vagy mplayerrel le tudod játszani meg menteni innen:
news.bbc.co.uk/media/avdb/news/uk/video/258000/nb/258376_16x9_nb.asx

subabubba 2009.03.17. 01:44:37

Sztem meg elég jól sikerült.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.17. 08:46:35

A HírTV-n meg lehet nézni az adást magyarul is:
Adás:
2009. március 17. kedd 13.05
2009. március 20. péntek 11.30
2009. március 21. szombat 13.05 és 21.30

Aki neten akarja:
mms://streamer.hirtv.net/hirtv.asf

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.17. 08:55:03

@Nyomi:
Én sem akarok polgármester lenni :-)

@Subabubba:

Szerintem is jól sikerült, de muszáj volt összefoglalni a történéseket, mert sokféle reagálás érte az adást. Igazábaól a mai világban minden infohoz hozzá lehet jutni, de azért szabályozni érdemes lehet azokat. Nyilván nem helyes az, ha a BÁRKI által elérhető Youtube-on gyerekpornó vagy részletes ajtófeltörési tanfolyam található. Ha ilyen ott felbukkanna, én is törölném. Ettől persze bizonyos warez oldalakon aki nagyon akarja, hozzájuthat. De ott is elképzelhető, hogy éppen az FBI tartja az oldalon ezeket honeypotnak, csalinak, és vadássza le utána az ilyen látogatókat

Mellesleg én például csípem az olyan Angliában és az USA-ban használt módszereket is, mikor kitesznek rejtett kamerával egy piros sportkocsit benne a slusszkulccsal, és fogják vele a tolvajokat, szerintem jó módszer, aki becsületes, az akkor sem lop autót, ha benne van a slusszkulcs.

nyomi 2009.03.17. 20:58:38

Koszia linkeket mindenkinek! A totem egesz jol lejatsza, ha vkinek az mplayer nem vinne linux alatt. nalam "size_confirm mismatch!: 22611 28271" elszallt az mplayer.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.06. 11:46:38

Tíz nap alatt 70 gigabájtnyi lopott adat:
www.technet.hu/notebook/20090505/lenyultak_egy_botnetet_orankent_56_ezer_jelszo/

Vigyázni kell a podcastokkal

2009.03.17. 14:36 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: apple itunes podcast malware account

Újabb trükk bukkant fel, ezúttal az Apple iPod, iPhone tulajdonosok életét keseríthetik meg az olyan kártékony podcastok, melyek fő célja az iTunes account adatainak illegális megszerzése.

Az ilyen audio fájlok felbukkanása új irányt adhat a visszaéléseknek. Az autentikációs ablakba begépelt felhasználói adatok kiszivárgása és illetéktelen kezekbe jutása jelentős kellemetlenségeket okozhat a gyanútlan letöltőknek.

Az Apple tulajdonosokat egyébként vélhetően egyre inkább érdemes lesz majd a jövőben támadni, hiszen egyrészt **egyre többen vannak, másrészt anyagilag nem a legszegényebb réteghez tartoznak, és végül, de nem utolsósorban iTunes használatuk miatt kötve vannak egy létező és vélhetően nem üres bankszámlához**, ami komoly motivációt jelenthet a bűnözőknek.

Elsőkörben tehát **mindenképpen érdemes a 8.1 iTunes szoftverre frissíteni**, ami megszünteti a fenti biztonsági rést. Ám a történetnek itt még biztosan nincs vége, a jövőben várhatóan lesznek még hasonló jellegű támadások.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1007297

Kommentek:

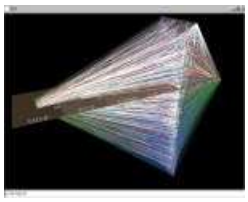
Nincsenek hozzászólások.

Weboldalak bénítása Oroszországban

2009.03.18. 15:22 | Csizmazia István [Rambo] | 1 komment

Címkék: weboldal orosz támadás homoszexuális ddos

Nemrég olvashattunk arról, hogy **orosz fiatalok vállalták fel nyíltan**, ők okozták az Észtországi "rendellenességeket" az Orosz-Észt konfliktus kirobbanásakor. Ha pedig valaki nézte a HÍR TV-n a BBC Click legutóbbi adását, láthatta, hogy **a DDoS támadás egészen maffiaszerű, védelmi pénzszerző tevékenységgé avanzsált, amely erősen sújtja az olyan weboldalakat, ahol fontos az üzletmenet** szempontjából az állandó online jelenlét.



Ilyen érzékeny webhelyek például **az online szerencsejátékkal vagy a fogadásokkal foglalkozó oldalak**. Ha egy ilyen vállalkozás webszerverét lebénítják, akkor jól kalkulálható veszteséget tudnak okozni. **Ha ehhez képest egy kisebb összegű védelmi pénzt kérnek a támadás elmaradásáért, akkor a megzsarolt vállalkozó sok esetben még mindig jobban jár**, ha fogcsikorgatva fizet, mintha fantomokkal hadakozva, néha a hivatalok értetlenségétől és szakmai inkompetenciájától kísérve mégis feljelentést tesz, aztán pedig elszenvedi a túlterheléses támadás miatt bekövetkező jelentős veszteségeket. **Amelyek később is bármikor megismétlődhetnek**.

Az üzleti konfliktusok ilyetén lerendezése, de a szimpla védelmi pénzszedés is jelen van napjainkban világszerte, és persze **emellett létezik még az ideológiai alapon történő célpont kiválasztás is**. Ehhez elég egy háborús szobrot áthelyezni, de sokan a másként gondolkodás, vagy a másság terepeit is igyekeznek ellehetetleníteni.

Egy friss hír szerint az **oroszországi homoszexuálisok weboldalai kerültek nemrég DDoS támadások kereszttüzébe**. Az egyidejűleg indított támadások az azonos neműek iránt érdeklődők körében népszerű, kereskedelmi weboldalakat bénítottak le, ezeket több napra le is kellett állítani, mert csak az "503 Service Temporarily Unavailable" hibazünet jelent meg. Az egyik oldal, a gogay.ru február végén **nyilatkozatot is adott ki a leállásról, melyet a 2 Mbit/sec méretű támadás okozott**. Azért vélelmezhetően ha Putyin olajérdekeltségeit vagy jelentősebb orosz állami bankok weboldalait kezdtek volna így napokon át támadni, **akkor vélhetően nagyon hamar kopogtak volna a tettesek ajtaján egy AK-47-essel**.

Persze a helyzet sokszor nagyon bonyolult. A NATO-nak is **ki kellett volna állnia az Orosz-Észt támadás esetében, mégsem tette**, mindenki ódzkodott a NATO tag Észtországot megvédeni, hiszen egyrészt körülményesen volt csak bizonyítható a támadás, másfelől **komoly háborús következményekbe is torkollhatott volna**. Inkább nem tettek semmit, sőt nem is beszéltek róla.

Nem vagyok érintve az orosz oldalakkal kapcsolatason, de nem lehet nem észrevenni, hogy **lassan a könnyen és névtelenül bevethető fegyvertár hétköznapi eszköze lett az elárasztásos módszer**. **Már biztonsági cégek weblapjai is áldozatul estek**, a szerencsejátékos oldalak pedig a rossz nyelvek szerint valóban fizetnek azért, hogy őket ne támadják. Várhatóan **a potenciális célpontok száma pedig egyre csak növekedni** fog.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1009464

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.19. 10:11:12

Ha nem röhögjük magunkat halálra már rögtön az elején az "internet cenzúrázása" részen, akkor az is simán elképzelhető, hogy a lenyúlt SQL adatbázisú, kártevőre mutató linkkel kompromittált weboldalakba a jövőben még egy-két ilyen fizetős linket is kap majd a haragos, a konkurrens cég weblapja.
index.hu/tech/blog/2009/03/18/napi_11_ezer_dollar_buntetes_linkelesert/

Nemzeti Zombitudatossági Hét Ausztráliában

2009.03.19. 14:16 | Csizmazia István [Rambo] | 22 komment

Címkék: biztonság zombi trójai tudatosság botnet féreg sophos conficker

A vicces cím ellenére komoly dologról van szó. A Sophos által kezdeményezett akciónak az az oka, hogy **Ausztráliában minden hatodik számítógép már egy botnethálózat tagja**.

A kampány legfőbb célja, hogy felhívja a figyelmet erre a káros jelenségre, erősítse a felhasználók biztonság tudatosságát és segítséget nyújtson a fertőzött gépek megtisztításában. Becslések szerint csak a Conficker féreg által megfertőzött, és ezáltal **botnetes hálózat tagjává tett számítógépek száma meghaladja a 10 milliót**. Egy ilyen megfertőzött számítógép aktívan résztvesz a spamküldésekben, webhelyek elleni DDoS támadásokban **anélkül, hogy a tulajdonos szélessávú internetkapcsolatában bármilyen jelet, vagy érdemi lassulást észlelne**.

A tapasztalatok szerint nem csak a kisebb vállalatok, vállalkozások számítógépei, hanem a **gyors és állandó internetkapcsolatok egyre kedvezőbb árai miatt kifejezetten a magánemberek vannak egyre nagyobb veszélyben**. Kellő szakmai ismeretek hiányában, illetve szakértő ismerős, barát, alkalmazott, családtag, stb. hiányában könnyű bekerülni a szórásba.

Egy OECD tanulmány szerint a fertőzött botnetes gépek száma évről évre meredeken emelkedik, **a fertőzött weboldalak száma is egyre növekszik**. A rosszindulatú webhelyek többsége továbbra is kínai, illetve amerikai szervereken hostolt oldal. Az eseményszervezők reményei szerint most igyekeznek minél többeknek segíteni kikerülni a botnetekből, illetve felvilágosítással és gyakorlati ismeretekkel segíteni a megelőző védekezésben.

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1011466

Kommentek:

gothmog 2009.03.19. 16:46:48

Conficker? Nem ez az a cucc, ami egy fél évvel ezelőtt kijavított hiba hátán jut be?

MILCSI 2009.03.19. 17:59:25

Ha nincsenek érezhető jelei,akkor honnan tudhatja meg a mezei felhasználó,hogy zombi lett?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.19. 18:22:16

Szia MILCSI!

Nincsenek érezhető jelei egy átlagember számára. De ha van rendes (nem Win) tűzfalad, a logban megtalálod a hálózati aktivitást. Még egyszerűbben is lehet nézni, ha nem futtatsz semmilyen szoftverfrissítést, böngészőt, levelezőklienst, de mégis van hálózati forgalom például a Feladatkezeőben nézve, akkor lehet gyanakodni.

Ha valaki használja a szentháromságot: vírusirtó, kémirtó, kétirányú tűzfal, plusz naprakészre frissít, akkor minimalizálja (nem kizárja, hiszen van nulladik nap, trójai, amikor te magad telepítesz kártevőt, stb.) az esély, hogy zombivá váljon.

adat 2009.03.19. 18:24:11

az a 10 millió valsz ezután is le fogja szarni, h zombi-e a gépe ha nem érez érdemi lassulást.

Skulo · http://politoxi.blog.hu/ 2009.03.19. 18:44:49

10 dolog amiből tudod, hogy zombi lettél:

1. Iszonyatos és legyűrhetetlen vágyat érzel arra, hogy emberi agyat/húst/végtagokat fogyassz.
2. Különös okból vonzódni kezdesz az alulöltözött szőke nőkhöz és fiúkhoz, a fiatal túristákhoz és öreg papokhoz, illetve ezek széttépésére és/vagy elfogyasztására érzel késztetést.
3. Bőröd megfakul, elszürkül és oszlani kezd. Rosszabb esetben végtagjaid, vagy azok részei hiányoznak. Kiesik gödréből a szemed.
4. Borszalmas, elviselhetetlen oszlás szagod lesz.
5. Különböző férfiak és nők (kigyúrtak és általában véve olyan hős kinézetűek) kezdenek téged és a haverjaidat lemészárolni az itt felsorolt tárgyak egyikével:
- láncfűrész
- tűzoltófejsze
- duplacsövű sörétes puska
- egycsövű vadászpuska
- MP5 és ennek változatai
- molotov koktél vagy fáklya
6. Templomba vagy megszentelt földre lépve kellemeltenül érzed magad, legszivesebben elmenekülnél, olyan sikíthatnékod támad.
7. Kellemes, dallamos hangod, torz, érthetetlen mormogássá változik.
8. Csak egy mondtatot vagy képes érthetően kimondani: "Brains! More brains!" (Agyat, még agyat!)
9. A szenteltvíz esetleg viszkető, égető érzést okoz a bőrödön (mármint ami még nem foszlott le), esetleg megéget.
10. Este a finom, puha ágyikó helyett kriptába, sírokba, vagy egyszerűen csak a föld alá mész aludni.

by
Skulo

]{udarauszkasz 2009.03.19. 19:10:22

hat.. ahogy elnezem, eleg zombi van a buszon, vonaton is....
a zombikor a teveken, radiokon keresztul fertoz, foleg fomusoridoben.
"a monika soban lattam hogy...."
aaarrgh.

]{udarauszkasz 2009.03.19. 19:12:02

Az ilyen zombikor ellen az ellenszer:
kis sikloernyozes, kis zuzos zenevel, vagy epp dallamos nightwishsel megfuszerezve.:)

zsu.zsi 2009.03.19. 23:05:37

Szia Rambo!

Bocs a láma kérdésért, de béna user vagyok. Előbb írtad, hogy a tűzfalnál a logban megtalálható a hálózati aktivitás. A Toolsban (ESS 4) a Log files alatt ki lehet választani a Personal firewall log-ot, erre gondoltál?
Mit jelent az, hogy "Detected DNS cache poisoning attack"??? A Source-nál van egy IP-cím, a Target-nél az én jelenlegi címem, tiszta piros az egész... Mi az az UDP protocol és ezzel ilyenkor mit kell tenni??????

MILCSI 2009.03.20. 10:34:26

Köszi Rambo :-)) a tűzfalam win, a kém Spybot,mert nagyon bevált, a vírusírtót pedig most cseréltem Nod-ot Avast-ra,mert a Nod időnként a legelemibb dolgokat sem találta meg...és megnéztem,nem fut semmi,mikor nem fut semmi :-)))
Sok játékot töltögetek,azért ijedtem meg,ahogy olvastam,hogy nincs jele...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.20. 15:45:40

Szia MILCSI!

A mondatom eredetileg arra utalt, ha valaki semmilyen biztonsági programot nem használ, nincs semmi jele. Ha már használunk, és rendszeresen frissítjük, és jól állítjuk be, akkor megtettünk minden tőlünk telhetőt.

Az Avast váltással kapcsolatban nem lehet, hogy a NOD beállításoknál nem volt minden kiválasztva (kéretlen alkalmazások keresése, veszélyes alkalmazások keresése, kiterjesztett heurisztika használata, stb.)? Ha ezek így állnak, nem nagyon lehet semmilyen "alap" dolog, amit nem észlel. Esetleg megköszönném, ha pár ilyen konkrét állományt elküldenél a MINTAK kukac SICONTACT pont HU címre, megnéznénk közelebbről.

Összefoglalva, szerintem nem neked van félni valód a botnettől, hanem aki nem használ semmit, és ráadásul nem is érdekeli ez az egész.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.20. 15:58:54

Szia Zsu.zsi!

Ha használsz tűzfalat, és nézed a logot, abban már csupa olyan dolog van, amit az 1. felismert, 2. beállításoktól függően blokkolt is. Piros színe maximum azért van, hogy a rengeteg sorból kilógjon az érdemi esemény, hiszen néha egymillió kutyaközönséges ICMP, UDP, PING stb. között kell keresni.

A DNS gyorsítótár mérgezés egy már régebbi, ismert támadási forma DNS szerverek ellen, és a te logodban ismétlem, csak egy sikertelen próbálkozási adatcsomagot jelent.

Ha ESS-t használsz, legjobb, ha automatikusra állítod a tűzfal működést, és akkor az a legjobb tudása szerint kérdés nélkül működik - szerintem te tedd ezt!

Vagy választható a Szakértő mód is, azonban akkor a felhasználónak kell rendelkeznie a ki- és bemenő adatcsomagokról, szabály alkotásról, ami valóban csak hozzáértőknek ajánlott. Ilyenkor minden szabályozatlan adatforgalomnál ablak jön fel, és dönteni kell. Ha valóban érdekel, mi az UDP, TCP/IP, meg lehet találni leírásokat, doksikat, könyveket a Google segítségével, de aki nem szakember, nem érdekli behatóan, annak nincs szüksége ezek beható ismeretére, az internetezés akkor is működik.

dJw_ · http://rendszergazdak.blog.hu 2009.03.21. 20:16:14

Nagy bolodnság lenne kötelezővé tenni a virusirtó / antispyware szoftverek vásárlását számítógépek vásárlásakor? Legalább cégeknél...

zsu.zsi 2009.03.21. 23:47:41

Szia Rambo,

ha ezek már blokkolt dolgok, akkor jó, csak hirtelen megijedtem, mert gyakran ismétlődtek és nem tudtam, hogy mik ezek.

Megnéztem a tűzfal beállítását, automatikuson van most is, úgyhogy nem bántottam :-)

Közben utánaolvastam a gyorsítótár mérgezésnek + protokollhierarchiának, nem mondom, hogy profi lettem, de egy fokkal már jobb a helyzet... a protokollhierarchiákat még majd olvasgatom kicsit... :-)

Ha valakinek mobil internet elérése van, akkor a DNS szerver a Voda/Pannon tulajdonában van? Csak azért kérdem, mert ha ez már régen ismert támadási forma, akkor a mezei felhasználó szólhat-e / van-e értelme, ha szól a szolgáltatónak, hogy gáz van a szerverükkel, csináljanak valamit?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.23. 11:58:52

Bárki szólhat, figyelmeztethet. Aztán, hogy valóban az ő gépükkel van-e bármi, illetve csinálnak-e valamit, az már egy másik kérdés.

zsu.zsi 2009.03.23. 21:29:37

Ezek az adatcsomagok, amiket észlel a tűzfal az internet szolgáltatóm DNS szerverétől jönnek, vagy ilyenkor valaki találomra bombázza az IP címeket?

Csak azért nem értem, mert ha ez egy DNS szerverek elleni támadási forma, akkor elvileg nem akadhatna fent egy adatcsomag sem a tűzfalon, hiszen az internet szolgáltatóm be tud jönni a gépemre...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.24. 09:23:09

Szia Zsu.zsi!

Az internetszolgáltató nem szűrögeti csak úgy önhatalmúlag a forgalmat, hanem van nekik egy jól bevált beállításuk. Általában ebben, mivel a DNS-nél vannak visszajövő UDP csomagok, ezeket a normál működés érdekében engedélyezni szokták - legalábbis a szervereken.

Amit te tehetsz a saját biztonságod érdekében az az, hogy MINDIG te állítód be kézzel azt a két megadott DNS szervert, amit a szolgáltatód ad meg, és nem hagyod, hogy a kapcsolat automatikusan maga adjon, ajanljon fel DNS szervert. Ezzel éredt el, hogy csak ebből a tartományból fogadj el UDP csomagokat. Ezt mg GPRS kapcsolatnál is érdemes megtenni. Ha ez meg van, akkor fütyülhetsz a logbeli hárított - ilyen jellegű - bejegyzésekre.

Plusz érdemes Firefox böngészőt használni, ehhez pedig a SHOWIP és a NETCRAFTTOOLBAR kiegészítőket telepíteni, mert akkor azonnal látszik az is, valóban azon a weboldalon vagy-e, amire menni akartál.

zsu.zsi 2009.03.25. 01:41:58

Szia Rambo!

Köszönöm a segítséget :-)
Megkérdeztem a szolgáltatótól a két DNS címet, szerencsére megírták az e-mailben azt is, hogy hogyan kell beállítani, úgyhogy sikerült :-)

Firefoxot letöltöttem, a két kiegészítőt is sikerült telepíteni, mégegyszer köszi :-)

Te be tudsz jelentkezni ide a blog.hu-ra akkor is, ha a Firefox-ot használod? Valami miatt nem enged be, csak Explorerrel. Próbáltam a javascript engedélyezést és a sütik törlését, de egyik sem használt :-(

MILCSI 2009.03.31. 08:48:15

Mindig automatikusan küldte a jelentést a Nod,mert félbamba felhasználó módjára az is ki volt pipálva :-)) hogy az általad írt címre ment-e,azt viszont nem tudom ...így,utólag már semmit nem tudok küldeni,mert teljes eltávolítást végeztem,nem csak kikapcsoltam,úgyhogy semmi nincs a gépen,ami Nod...legalábbis általam fellelhető formában :-)) a heurisztika és a veszélyes-kéretlen alkalmazás is minden keresésnél ment,mert annyi önkritikám azért van,hogy rendszeres segítséget kérjek a szomszédom fiától,aki a debreceni egyetemen végzős számteches...és ő halál türelmesen minden ilyesmit "megtanít" nekem...ezért vagyok csak félbamba (ami szerintem a legrosszabb kombináció :-PP)
De hogy tiszta legyen,mit értek alap dolgok alatt: már nem tudtam rendesen levelet írni egy online böngészős stratégiai játékban,mert hiába ütöttem le egyesével,nagyon figyelve minden billentyűt,a betűk fele hiányzott a levélből...olyannyira,hogy amikor először fordult elő,akkor billentyűzetet akartam cserélni,hogy biztosan tele van macskaszőrrel és elromlott :-)) akkor sem talált semmit,de tényleg semmit a Nod,bár előtte egy évig teljesen elégedett voltam vele...akkor hirtelen ötlettől vezérelve spyware Terminatorral írtottam az írtanivalót...aztán egyéb okok miatt új XP került a gépre (az egyéb ok természetesen a kísérletező kedvem volt,ami idegösszeomlást okozott a gépnek :-S) és újra Nod,ami kb. 2hónap után újra elkezdett semmit sem találni...és amikor újra jött a nem tudok levelet írni című történet,akkor már "rutinosan" eltávolítottam a Nod-ot,kerestem egy Terminatort,de nem találtam és úgy jött az Avast,ami éppen egy másik nagy híroldal 5. helyezettje volt a letöltési listájukon..majdnem egy órát dolgozott a telepítés után és tizenegynéhány találata volt,ami nem sok,de utána és azóta sincs semmi gondom...
És most kezdheted tépni a hajad,mert egy hozzánemértő felhasználó,hozzánemértő leírása következik :-)) egy olyan trójai is volt a találatok köz,ami meghülyítette a routert,így az egyik gépen volt net,a másikon egyáltalán semmi (csak akkor,ha kiiktattam a routert) valami elérési utat változtatott meg,amit nem is tudtunk visszaállítani,mert mindig visszaírta magát...ja és a "szokásos" feldobált warning kezdetű abalakok,amik idegen "vírusírtót" ajánlgattak...és erre nem jelzett semmit a Nod...az Avasttal minden mindegy,mert úgyis megint XP-csere lesz alapon nekiugrottam és bátor birka módjára szerencsém lett és azóta is száguld a gép (kivéve indításkor,mert akkor míg mindent leellenőriz a maga szája íze szerint,addig nyugodtan levihetem a szemetet :-))

MILCSI 2009.03.31. 08:50:32

Milyen szép hosszút írtam és a Szia Rambo és a köszönöm,hogy ilyen türelmes vagy mégis kimaradt belőle :-))) pedig relatíve jólnevelt vagyok...

MILCSI 2009.03.31. 17:46:15

Ja és a lényeg is lemaradt...tisztában vagyok vele,hogy a Nod nyer minden "versenyt", mert -a hozzánemértésem ellenére vagy éppen azért- mindent elovasok a vírusokról és a vírusírtókról...de valamiért nálam nem vált be...
Méregdrága LG,samsung és Panasosnic tv-im haltak meg pár napon belül...egy török összeszerelésű Comtec (nem röhög) tv pedig 7,azaz hét éve szolgál rendületlenül :-)) úgyhogy biztosan taszítom a jó márkákat :-)))

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.02. 10:24:38

Szia MILCSI!

Szerintem nem csináltál rosszul semmit, és az én véleményem az, hogy számítógépesen, de a sportban is, mindig mi magunk vagyunk a mérce. Ha saját magunkhoz képest tudunk javulni, fejlődni, akkor az nagyszerű, bárki is kapja a Nobel díjat, bármennyi is a világrekord.

Van egy jó kis diagnosztikai eszköze az ESET-nek, ez a System Inspector. Ez a 4-esben már benne van, de ha régebbi NOD32-öt használsz, akkor a weblapról tudot az SI-t letölteni. Ha valamilyen rendellenességet tapasztalsz a jövőben - például abnormális lassulás, idiótikus billentyűzet működés, akkor futtass egy System Inspector riportot, es küldd be a supportos srácoknak. Jó eséllyel azonnal megmondják, mi lehet a gond, és biztosan segítenek azt rendbetenni.

MILCSI 2009.04.05. 21:06:50

:-))) idiotikus billentyűzetműködés...ez nagyon jó :-)))

Nem tudom,kedves Rambo,hogy milyet használok(tam),mert bevallom őszintén,hogy a 30 napos próbaváltozatokat szoktam volt letölteni...remélem,nem jár érte verés :-))

Nicsak, ki kattint ott!

2009.03.23. 16:23 | Csizmazia István [Rambo] | 1 komment

Címkék: google malware hamis antivírus kártevő scareware

A hamis antivírus ipar egyre erősebb. Ha elhisszük - és nincs okunk rá, hogy kételkedjünk - a mondás igazságtartalmát: **"Érdek a világ ura"**, akkor nyilvánvaló, hogy egy alaposan kifundált működési terven alapuló, és gigantikus jövedelmet hozó üzletág **nem hogy megszűnni nem fog, hanem éppenséggel a terjeszkedés, a hatékonyság fokozása, valamint az ellenőrizhetetlenség érdekében tett lépéseivel** erősítve okoz a felhasználóknak egyre jelentősebb veszteségeket.

Az egyre bővülő számú, de **egyre rövidebb ideig élő domainek** feketelistázása messze nem elegendő a boldogsághoz, nem is beszélve azon kezdeti időszakról, amikor már terjeszti magát a kártevő, de a blokkolandó URL-t még nem vette fel minden cég (Finjan, McAfee, PhishTank, NetCraft, stb.). Van olyan trükkös megoldás is, hogy **ha azonos IP címről újra belépünk, akkor mindig egy másik kártevő állomány töltődik** le - nehezítendő a nyomozást. Bár a visszafejtéssel foglalkozó cégek folyamatosan bővítik az ilyen kártékony hostok listáját, de hosszú távon nem lehet győzni ezek lajstromozását. Igaz néha egy-egy csalárd domainregisztrátor elszámoltatása segíthet a kártevő áradat **ideiglenes csökkentésében**.

A fertőzött weblapok persze többfélék is lehetnek. Vagy külön erre a célre létrehozott jól csengő nevű, vagy egy karakter eltéréssel (elgépeléssel) valami ismert kifejezésre hasonlító önálló oldal, vagy - és **az utóbbi időben ez egyre gyakoribb - egy már meglévő oldal megfertőzésével, IFRAME beillesztéssel, fertőzött aloldal vagy banner létrehozásával de akár kártékony linket tartalmazó komment** beírásával is megtörténhet egy nagyforgalmú és ismert, minden gyanún felül álló webhelyen is.

A hamis antivírusnak az a jó, **ha nincs naprakész biztonsági szoftver a számítógépen**, amikor azt éppen megtámadja. Utána pedig már ő az úr, a fertőzés után már képes lehet blokkolni az antivírus gyártók weboldalait is. Mivel ez egy kiemelten jó kereseti lehetőség szinte minimális lebukási eséllyel, már csak az a kérdés, **hogyan lehet minél több kétes találatot a terjesztő oldalakra terelni**. És természetesen erre is akad jó megoldás.

Ennek lényege, hogy **figyelik a Google Trendsen, mik az aktuálisan legnépszerűbb keresési kifejezések**, és az ezeket a keresőszavakat "bambán" beépítik oldalaikba. Tehát abszolút nem számít, mi a téma, ahogy az iTunes számláról szóló levélnek sincs semmi köze az Applehez, itt az Obama, iPhone, meghalt Natasha Richardson vagy **bármi egyéb sláger kulcsszó is csak eszköz, hogy kattintható linket kínáljon**, aztán a felbukkanó figyelmeztető ablakok már elintézik a többit. Vagyis a lényeg, hogy hasonlóan a korábbi torrentes kalandunkhoz függetlenül attól, hogy mi mit keresünk, ők akkor is tudnak ajánlani "érdemi" találatot.

A Finjan kutatói elemezték, mekkor forgalom terelődik "mellékútra", és úgy találták, hogy egy **bő kéthetes peridós megfigyelése alatt körülbelül 1.8 millió látogató** lett kártékony tartalommal rendelkező, és a keresés szempontjából abszolút nem releváns linkre irányítva. **Ha csak kb. 10%-a telepítette a hamis antinvírus programot, és ha csak 1.5% fizetett a "teljes" verzióért, az akkor is durván 8000 EUR** (nagyjából 2.5 millió forint) keresmény. Természetesen a Google folyamatosan küzd a jelenség ellen, de ez nagyjából annyit jelent,

hogy utólag próbál takarítani.

A már korábban tárgyalt Conficker féreg hasonlóképpen próbált csatlakozni az azóta már tavaly novemberben megszűnt TrafficConverter.biz weboldalhoz, ahonnan szintén hamis antivírus kísérelt meg letöltődni az áldozatok gépeire. Egyes szakértők úgy látják, az oktatás, a **felhasználók képzése lenne a legfontosabb a számítógépes írástudatlanság legyőzéséhez**, hogy ne maguk a telepítsék fel a különböző kártevőket a gépeikre.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1019946

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.11. 08:43:27

Nem egyszerű a küzdelem a pallérozott elméjű bűnözők és az átlag felhasználó között, ha nemcsak diigitális írástudatlanságról beszélünk, hanem ilyen mértékű valódi írástudatlanságról is. Vajon mire kattintanak ezek az emberek? Hogy írnak alá banki szerződéseket?
index.hu/kulfold/2009/05/10/nem_tud_olvasni_es_irni_sem_30_millio_amerikai_felnott/

Kínai és kanadai egyszerre, mi az?

2009.03.25. 15:58 | Csizmazia István [Rambo] | 1 komment

Címkék: kína domain domén kanadai zombi botnet gyógyszerész

Hát a Kínában hosztolt "kanadai gyógyszerész" weboldal. Úgy tűnik, a botnetes, Confickeres tapasztalatok is határozottan megerősítik ezt, hogy a kártevők terjesztéshez használt domainek száma is explonenciálisan megnövekedett, és ebben oroszlánrésze van a gyenge kínai bejegyzési szabályoknak. **Nehéz megmondani, hogyan lehetne ennek útját állni**.

Ha megnézzük egy átlagos napi spam termésünket, utcahosszal vezetnek a kanadai gyógyszerész oldalak kéretlen reklámjai. Már írtuk korábban is, **ez lehet iTunes számla, de bármi más is, akár Amazon áruház rendelés** visszaigazolásnak látszó tárgy is vagy bohém ifjúkorunkból származó kollégiumi fotó.

Ha vesszük a fáradtságot, és elkezdjük megnézegetni a domaintools segítségével, **kik, hol és mikor jegyezték be az oldalakat, akkor azt látjuk, szinte kivétel nélkül Kínában**, sok esetben a szerver is ott üzemel, és mindössze néhány nappal korábbi a regisztráció dátuma. Ha elolvassuk a legutóbbi elemzést a Conficker (Downapup) féregváltozatról, akkor ott már 50 ezer doménből 500 véletlenszerűen kiválasztott botnet vezérlést látunk, és nincs okunk feltételezni, hogy **ezek számát na akárnák még tovább növelni, hiszen "bevált"** nekik. Az is egy jó elméleti számtan példa, ha minden kínai (> 1.3 milliárd) minden nap 10 új domaint regisztrálna, mennyi idő alatt lenne itt az internetes világvége ;-) A zavarkeltéshez azonban úgy látszik, **ennek a töredéke is elegendő**.

Ha esetleg el is tekintünk attól, hogy a rendelt gyógyszer vagy a placebó kísérleteknél "esett le" egy teherautóról, vagy a temérdek szabadidővel rendelkező és **szerfelett vicces fiúk készítették azt tevetrágyából és permetezőszerből**, a lényeg az, hogy **a rendelési oldalon várják a bankkártya adatokat a 3 jegyű biztonsági kóddal együtt**.

Ezzel pedig már tudnak mit kezdeni a bűnözők, **ezek birtokában vidám vásárlásba kezdenek, míg a gyógyszer oldalon ücsörgő "palimadár" még azt sem tudja, pontosan kikkel is áll kapcsolatban**. Igaz, **a becsapás miatti stresszre rendelhetünk még tőlük Cialist**, de hát addigra egyrészt a bizalom már oda, másrészt bankszámlánk vélhetően sikeresen leapasztva piheg.

Sok esetben az "áruházi" weboldalon még a Contact Us vagy FAQ menüpont sem mutat sehová. Ha valaki mindenáron rosszul akar lenni kétes eredetű gyógyszertől, azt ma már internet nélkül a helyi bolhapiacon is megteheti forintért ;-)

A kéretlenül érkező bármilyen feladótól, bármilyen témájú levelek és bennük szereplő linkekkel **a jóslatok szerint a botnet építők már április 1-re fókuszálnak**. És függetlenül attól, hogy egy ilyen linket emailben, MSN vagy Skype üzenetben kapunk, fertőzött aloldalon vagy fórum- esetleg blogkommentben látjuk, **egyáltalán nem szükséges, hogy a bolondok napja alkalmából mi magunk is kattintsunk ezekre**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1024695

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.07.02. 19:25:48

Hogyan készül rovatunkban ma a háztáji Viagráról lesz szó ;-)
index.hu/bulvar/2009/07/02/betonkeveroben_zuglaborban_keszul_a_hamis_viagra/

Váltságdíj az állományaidért

2009.03.26. 17:39 | Csizmazia István [Rambo] | 4 komment

Címkék: pro 2009 zsarolás kártevő ransomware filefix

Pénzt vagy életet? Szól az örökbecsű kérdés a Megkerült cirkálóban, de ha **"Pénzt vagy a számítógépen tárolt dokumentumokat" lenne a felvetés**, akkor már sokan nem mosolyognának ennyire Wagner úri derűvel. **A hamis antivírusok után, pontosabban mellett** itt a fájltitkosító és váltságdíj szedő kártevő.

A hamis antivírusokról **sokszor és sokat beszéltünk**, a lényeg, hogy böngészés közben egyszer csak felbukkan egy ablak, ami **nem létező fertőzésre figyelmeztet minket**, és ha valaki telepíti, akkor magát a kártevőt telepíti. Ez pedig egyrészt 50 dollárt kér, hogy nekilásson az "irtásnak", amit a pénz kifizetése után sem tesz meg, másrészt a megadott bankkártya adatokkal még **újabb összegekkel is megpróbálják lehúzni** a szerencsétlen áldozatot. Ha akad valaki, aki erről még egyáltalán nem hallott, az vagy remete egy erdő közepén, vagy a Holdról jött.

Azonban **eljött az idő reformokat bevezetni a bűnözők szerint is ;-)**, hadd növekedjenek még tovább a bevételek, és ez pedig egy új típusú "biztonsági" programmal lehetséges, amit eddig **FileFix Pro 2009 néven** ismertünk, de ide a rozsdás bökőt, hogy pár hónapon belül ebből is lesz egy tucatnyi különböző nevű változat. A lényeg, hogy telepítéskor a kuncsaft **.DOC és .PDF állományait elkódolja, amit aztán az 50 USD összegért hajlandó csak visszaállítani**.

Egyetlen kiválasztott állományt mutatóba helyreállít, hogy megmutassa, képes rá (naná, ő cseszerintte el). **Fizetni azonban nem érdemes**, ne hizlaljuk a bünözők pénztárcáját. Annál inkább sem, mivel már **létezik több ingyenesen letölthető segédprogram, amivel visszanyerhetjük dokumentumainkat**.

Ahogy a botneteknél is a számítástechnikai analfabéták járnak a legrosszabbul, várhatóan **pontosan azok fognak ennek is áldozatul esni, akik sajnos nem olvasnak ilyesfajta blogokat**. Kár.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1027012

Kommentek:

zsu.zsi 2009.03.27. 02:55:01

Szia Rambo,
számítástechnikai analfabéta vagyok. Ha tegnap megkérdezte volna valaki, hogy ugyan mondjam már, mi az a "ransomware", csak furcsán néztem volna rá, hogy mi a baj. A fenti írás miatt utánaolvastam kicsit, úgyhogy ma már azt mondom, hogy a kriptovirológia érdekes dolog. Jó a blogod, nagyon tetszik, írj még sokat :-)

Az RSA eljárásnál viszont jól elakadtam. Az addig oké, hogy a titkosításhoz egy nyílt és egy titkos kulcs tartozik, a nyílt kulccsal kódolt üzenetet kell a titkossal megfejteni, de hogy ehhez az RSA eljáráshoz hogyan kell kulcsot generálni, azt sajnos hosszas vívódás után sem sikerült lekövetni, elég bonyolult a cucc. Aki ilyet tud írni, az zseni, igazán használhatná jó dolgokra is a képességeit...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.27. 09:25:48

Szia!

Itt találsz okosságokat RSA-ról:
www.irt.vein.hu/~vassanyi/info/rsa/rsaleir.html
hg8lhs.ham.hu/tdk/tdk_prez.pdf

Ha csak használni akarod, elég egyszerűen lehet a Thunderbird levelezőben felvenni az Enigmail plugint, és akkor tudsz alárírt levelet, vagy kódolt üzenetet is küldeni.

Kártevő ügyben pedig ennél sokkal kifinomultabb dolgok vannak-voltak, például annak idején a OneHalf a merevlemez vége felöl el kezdte elkódolni a lemezt, és ha ezekután csak leirtottad, agyő adatok. Leitold Feri írta meg azt a OneHalf Killert, ami visszahozta az adatokat is. De mostanában is volt ilyesmi a Kaspersky toborzott kódfejtőket a GPCode-hoz. Ezekhez képest ez a FileFix csak ipari tanuló ;-)

A VVV 16-os epizódjában részletesebben is olvashatsz ilyenekről, a PCW Cikkek dobozban vannak a PDF linkek.

Egyébként aki érdeklődik, olvasgat, keresgél, az már m is analfabéta :-D Az a legszörnyűbb, ha valaki minden ilyenre csak annyit mond "nem érdekel, nem is akarom hallani". Ott aztán tényleg nehéz eredményt elérni. Marad a "saját kárán" való tanulás, a harmadik kifosztott bankkártya, a negyedik nevében felvett bannkölcsön, és 78 darab az ő nevére kikölcsönzött padlócsiszológép után talán elindul az úton ;-)

zsu.zsi 2009.04.02. 13:13:42

Szia Rambo!

Az RSA algoritmusával sajnos kellett foglalkoznom jó pár napig mire leesett a lényeg, mert korábban nem annyira izgatott a kis Fermat-tétel (sem) :-) Igaz így most sokáig tartott, de hát jobb később mint soha :-D

Régebben azt hittem, hogy egy kódolt üzenet visszafejtése mindig inverz művelettel történik, ha kódolni akartam volna valamit, eszembe nem jutott volna matematikai azonosságot használni... ügyesek voltak a kitalálói. Azt sem tudtam, hogy a https-nél is nyílt kulcsú titkosítást használnak... :-(

A VVV 16-ban írtál a Furkó AV weboldalának meta részéről. Utánanéztem, hogy mi az a meta. Azt szeretném kérdezni, hogy egy gyanús oldal HTML kódjában mit érdemes megnézni? Pl. ilyenekre gondolok:
- a metát a kulcsszavak miatt,
- Csali link szöveg
-
-
A scriptet szerencsére ki lehet kapcsolni... Ha az

zsu.zsi 2009.04.02. 13:22:59

Hopp, a fele eltűnt... :-D megpróbálom máshogy írni, úgy látszik nem szereti a böngésző :-DD tehát:
-a metát a kulcsszavak miatt
- kisebb mint jel a href="www.adathalasz.com" nagyobb mint jel Csali link szöveg kisebb mint jel /a nagyobb mint jel
- kisebb mint jel img src="url" /nagyobb mint jel
- kisebb mint jel script nagyobb mint jel
Azt akartam még írni, hogy a scriptet szerencsére ki lehet kapcsolni, így avval nincs nagy gond. Ha az img src=" után pedig futtatható file pl. .exe van, akkor mondjuk vili, hogy gáz van az oldallal. Melyik tag vagy attribute után írt szöveg lehet még necces?

A cikkben azt írtad, hogy ez a Furkó az MBR-ből indul. Amikor scannel az ESS4 akkor ugye a partíciós táblában is megnézi, hogy mi van ott?

Norton ügyfelek adatait tessék!

2009.03.28. 15:04 | Csizmazia István [Rambo] | 10 komment

Címkék: bbc név india cím adat bankkártya ügyfél 2009 norton adatszivárgás

Mostanában rendelt Norton Antivírust? Netán telefonon hosszabbította meg licencét? **Akkor ideje ellenőrizni bankkártyája forgalmát, nem hiányzik-e pénz róla**, mert szivárognak az ügyféladatok a Symantec házatáján.

A riport szerint az Egyesült Királyságban élő ügyfelek személyes adatai kerültek veszélybe, úgy mint név, lakcím, banki azonosítók. **Az inkognitóban ténykedő újságírók minderre egy indiai kereskedőnél bukkantak, aki pénzért árulta ezeket az adatokat**. A riporterek pedig próbaképpen bevásároltak. Három konkrét áldozatnál az is bebizonyosodott, hogy **az a közös pont bennük, korábban valamennyien telefonon keresztül hosszabbították meg Norton licencüket**.

Az indiai rendőrség azonnali vizsgálatot kezdett e4e nevű partnernél, és **a Symantec is a külsős Call Centerükben dolgozó üzletkötőkre gyanakszik**. A 4e4 azt nyilatkozta, több más cégnek is folyamatosan végeznek hasonló telefonos támogatási munkát, és eddig semmilyen panasz nem érkezett rájuk. Egyelőre várjuk a vizsgálat részletesebb eredményét. Újabb pont a "Harun al Rasid" vagy Mátyás király módszer mellett, így csak lehet jól megismerni a dolgokat.

Befejezésül pedig egy kis desszert. Az már csak hab a tortán, hogy a **weboldalukon van egy színes-szagos flash "összehasonlító": Norton VS az egész világ ;-)** Ha megnézzük az ESET Smart Securityvel párba állított Norton Internet Security 2009-t, akkor **például a boot időben ugyebár x százalékkal fényesebb a láncnál a kard**. Az pedig, hogy a boot időben kikapcsolt Early Loaddal nem teljesértékű a védelem, kit érdekel? **Reméljük, hogy nem ilyen "elfogulatlan" flash mozik alapján választanak majd biztonsági programot az emberek :-)**

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1028702

Kommentek:

marosy 2009.03.28. 18:10:31

Mindig is mondtam, hogy az indiaiak nem megbízhatók.

Sem Mihály 2009.03.28. 18:10:37

Há nemtom, a Noddal már volt szívásom vírusilag nem egyszer, amit aztán a Symantec Endpoint oldott meg (ez nem a Norton).

freeware2000 2009.03.28. 18:39:50

Nálunk a cégnél Symantec Corporate Edition van jópár éve. Mivel volt lehetőségem kipróbálni egy gépen több fajta védelmi programot, elmondhatom, hogy a kipróbáltak közül (NOD,AVG stb.) magasan a Symantec terhelte legjobban a gépet. Nem véletlenül adtak ki Gamer Edition, mert nem akartak emiatt ügyfeleket veszíteni.

Mostanában nem fordult elő, de évekkel ezelőtt jópár vírus átjött rajta, amit más vírusirtók nem engedtek be. (WIN2000)

A független teszteken rendszeresen megelőzik ingyenes szoftverek is.

El kellene már felejteni...

Algernon 2009.03.28. 20:01:50

A legújabb teszten www.av-comparatives.org elég szépen szerepelt a Norton, nem előzték meg az ingyenesek. Lassanként az, hogy ingyenes egy program, már nem enged semmilyen következtetést levonni a hatékonyságára, lásd az Avsat! utóbbi eredményeit.

intrusion 2009.03.28. 21:17:47

Én azt mondom teljesen elfogulatlanul, hogy a NOD32 nagyon a heurisztikában (az ismeretlen kártevők elleni védekezésben), valami zseniális heusztikus modult írtak alá. DE! Az adatbázis alapú felismerésben igen gyenge. Bár az is igaz, hogy mostanság mintha rákapcsoltak volna az adatbázis növelésére, ami meglátszik az AV Comparatives legutóbbi on-demand tesztjén. Csak el ne bízzák magukat, mert még van mit alakítani ezen. Az is jó lenne, ha megszüntetné az ESET azt a hibát, ha amivel elég sokszor lehet találkozni különböző netes fórumokon, hogy ugyan megtalálja a kártevőt, de eltávolítani már nem tudja. A felismerés nem elég, el kell tudni távolítani a vírust.

Én megmondom őszintén, nekem van egy három éves licenszem a NOD32-höz (amiből eltelt két év anélkül hogy használtam volna), de nem használom, mert még nem bízok benne. Majd ha az on-demand teszten meghaladja a 99 %-ot akkor és csak akkor beszélhetünk arról hogy felteszem. Tudom hogy az AV Comparatives tesztjei (és az összes teszt) nem fedik a teljes valóságot, de azért iránymutatásnak jó.

Most McAfee Total Protection 2009-t használok (előtte egy évig Avira párti voltam, de annak sok a téves riasztása), ami tartalmazza ezen cég legújabb fejlesztését az Artemist, pontosabb nevén, az Active Protectiont, ami állandó kapcsolatot jelent egy vírus laborral és a gyanús fájlokat ott is ellenőrzi. Az AV Comapartivesen 99.1 %-ot ért el és a teszt szerint a téves riasztása is megnyugtatóan kevés.

intrusion 2009.03.28. 21:26:04

@freeware2000:

Én linuxon használom a Symantec Antivirus Corporate Edition 1.07 Linuxot. Nem veszek észre teljesítmény csökkenést.

Windowsra (ha ragaszkodsz a Symantec termékekhez) otthoni használatra a Norton 2009-et, céges gépre a Symantec Endpoint Protection ajánlanám. Hidd el nekem, mindkét alkalmazásnak nagyon kicsi a rendszerigénye, nem egy több évvel ezelőtti

fejlesztésből kellene kiindulni és abból levonni konzekvenciát.

intrusion 2009.03.28. 21:33:49

@intrusion:

... elnézést lehagytam egy szót: ...nagyon JÓ a heurisztikában...

Sem □ ihály 2009.03.29. 15:24:24

@intrusion: Sajnos a linuxos nagyon disztrib-függő (az itthoni debian-ra pl. a régi (2.6.18) kernel támogatása miatt nemtom felrakni), az Endpoint viszont tapasztalatom szerint jópár szempontban magasan vezet a közszájon forgó (panda, nod, avast, avg stb.) megoldásokkal szemben.

phare 2009.03.29. 16:37:53

@Tromos Elek:

Ha ragaszkodsz a SAV-hoz, távolítsd el az új kernelt a synapticból és használj régit. Nem tudom hogy a Debianban van-e synaptic. Én Ubuntu 8.04-es gyári kernellel használom.
Vagy pedig.
Használd a Sophos Antivirus Linux 6.6-ot, ami a legújabb linux kernelt támogatja.

Sem Mihály 2009.03.29. 21:28:40

@phare: Van synaptic. Nem akarok régi kernelt, kell egy csomó dolog, ami nem megy vele. Jelenleg clamav-zek, de ez is csak azért, hogy a levelezőszerveren legyen vírusszűrés, egyébként nem kéne (de azért kössz a tipept :))

Mikor ír nekünk a bank személyzetise?

2009.03.30. 20:26 | Csizmazia István [Rambo] | 17 komment

Címkék: bank csalás raiffeisen adathalász

Hogy megkérjen minket, ugyan kattintsunk már az általa mellékelt Raiffeisen ügyfél belépési oldalra? A helyes válasz: never. **Hiteles ügyfél üzenet formájában ennek esélye a nullához konvergál**, ezért ha mégis kapunk ilyet, 110%-os bizonyossággal tekinthetjük adathalász próbálkozásnak.

Mintha csak Borat írta volna a levelet, "én lenni Matyar nép naty usankás baráttya, te pedig ide beleütögetni belépkedési kódolócskádat." Vagy nem volt épelmejű, vagy csak a magyar nyelvvel állt hadilábon a készítő, ezért **a levél láttán csak annak örülhetünk, hogy beválási esélye remélhetőleg kicsiny**: ha valaki egy ilyet hitelesnek gondol, annak talán ne is legyen bankszámlája ;-)

Megjelenésében és szóhasználatában vetekszik korábbi, az idiótaság feneketlen és mélységes bugyraiban könyékig kotorászó rekorderünkkel. Az adathalász levél **készítőinek szemlátomást mindegy, velük nevetünk-e vagy rajtuk**. A weboldalon pedig talán nem is lepődünk meg, hogy SSL-nek se híre, se hamva.

Szóval nem, **a bankok még mindig nem írnak nekünk magánlevelet, még a HR osztályról sem, hogy lépjünk be azonosítónkkal**. Továbbra sem dívik náluk a kevert használatú írásbeliség sem, amelyben tolmácsolt kérésükről magyar-orosz továbbá urdu nyelvjárással óhajtanának meggyőzni bennünket, különösen nem Windows-1251 cirill betűs karakterkiosztással írt ősmagyar levélben, amit eredetileg egy Microsoft Wordben formáztak. Reméljük, a jó moszvai nagynénjüket optimalizálják a továbbiakban, szigorúan online.

De legalább ezekben a miniszterelnökjelöltektől terhelt **zivataros napokban bumfordiságával szerzett nekünk néhány felhőtlen és vidám percet**, önfeledt mosolyt csalva orcánkra, amelyet oly ritkán kapunk meg, de kétségkívül megérdemlünk így hétfő reggel :-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát

- Gyerek-barát netezés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1034701

Kommentek:

gyík (törölt) 2009.03.30. 21:34:18

Nem is, ez tök komoly.

Én is a melóhelyemen az egyik raktárosi részlegi email címére kaptam ma egy ilyet. Akkor csak komoly lehetett.

A gond az, hogy nekem személy szerint a 3000 forintos Raiffeisen számláról OTP-re történő utalásnál is sms jelszót igényelt a tranzakció.
Akkor meg mit tudnak tenni? Arra is küldenek egy emailt, hogy ugyan már küldje el ide és ide? :)

WUT (törölt) 2009.03.30. 22:03:58

ezt én is megkaptam :) ezt kivételesen el is olvastam, de persze nem kattintottam. nagyon gagyi :)

heliox 2009.03.30. 22:15:43

Amíg az SMS-ben nincs benne, hogy milyen tranzakciót is hagysz jóvá (hova mennyit utalsz) addig akár át is tud proxy-zni. Az SMS nem kell, hogy átmenjen rajta, csak a kód amit begépelsz. Persze egy kicsit több programozás kell hozzá, de biztonságtechnikában ugye azt tételezzük fel, hogy amit meg lehet tenni, azt megteszik a rossz fiúk.

dark future · http://www.andocsek.hu 2009.03.30. 22:26:53

Az a szerencsénk, hogy ilyen ratyi minőségű egyelőre az online angol-magyar fordítás... :-)

ScrnSvr 2009.03.30. 22:30:40

Én már szinte hiányolom, ha reggelente nincs benne a Raiffeisentől egy hasonló levél, valamikor karácsonykor kaptam az elsőt, azóta hűségesen érkeznek. A bámulatos viszont az, hogy szinte naponta kitalálnak valami új trükköt.
Ja, és már ott lett eleve gyanús, hogy nem is vagyok RF-ügyfél :)

[imi] · http://twitter.com/forgoimi 2009.03.31. 00:46:34

elhihetitek, hogy simán van aki ráklikkel ezekre!!!

-= If =- 2009.03.31. 03:31:10

Megalol. Ha valakinek nem tűnnek fel a cirill karakterek, az nem itt nőtt föl az elmúlt huszon-harmincon-ötven évben... és ez csak a legszembeötlőbb, lamerek által is felfedezhető bibia levélben:) Akkó viszont minden okés, klikkeljen csak.
Énhátradőlök, és széles mosollyal az arcomon készítem elő a megfelelő eszközöket a romeltakarításhoz, meg a kasszát, mert minnyá cseng ám:)

kpityu2 2009.03.31. 06:15:12

Szerencsére én védve vagyok. Még ha tényleg a bank írná akkor is menne a kukába.

Astronomy Domine 2009.03.31. 06:48:30

Én rá szoktam ezekre klikkelni, aztán username/password: goddamned cocksuckers / fuckoffplease meg hasonlók. Hadd örüljenek.

Tapmancs 2009.03.31. 07:16:25

A helyes válasz: soha. Nem never.

pingwin · http://pingwin.blog.hu 2009.03.31. 07:57:38

kedves ismerosom ilyen esetekben fake user/pass parossal kedveskedik :)

MILCSI 2009.03.31. 08:10:41

Egy ilyenre még én sem mennék rá :-)) de a bankban az ügyintéző leányzók mindig szeretnének rávenni,hogy netbankoljak végre...de csökönyös szamárként ellenállok,úgyhogy tőlem hiába is kérnének ilyesmit,pláne ilyen csinos levélkében :-))

Flashzee · http://www.flashzene.com 2009.03.31. 08:43:21

Ja, sok hülye van!

Mária · http://maria.blog.hu 2009.03.31. 08:47:07

maria.blog.hu/2009/03/30/raiffeisen_banknak_alcazott_oldal

Tamas88 2009.03.31. 08:49:29

Azért az is szép példány lehet aki bedől ennek :)

gothmog 2009.03.31. 19:31:34

Én lenni orosz csodadoktor kezzemmel rátesz, mondani igaz ténylegesség. Te elhisz most.

dJw_ · http://rendszergazdak.blog.hu 2009.04.01. 20:40:45

napiszar -ra való :)

Lesz-e világvége április elsején?

2009.03.31. 14:40 | Csizmazia István [Rambo] | 29 komment

Címkék: internet jóslat világvége támadás conficker

Fiatalkorom egyik élménye, mikor japán tudósok megjósolták, állítólag akkora földrengés lesz, hogy a Gellért hegy belecsúszik a Dunába. Volt ismerősöm, aki erre a napra direkt szabadságot vett ki, **amit aztán az Alföldön töltött el :-)** Azóta megtanultam, csak a "brit tudósoknak" szabad hinni ;-) De vajon **mi lesz az új Conficker féreg világméretű támadásával?**

A tegnapi Index cikk összefoglalt sok mindent, és mi is többször postoltunk itt a blogban is a témáról. Emellett pedig **elolvastunk néhány kifejezetten témábavágó szakvéleményt** a várható fejleményekről, amiben azért részben jobbára mindenki csak találgat, de nincs okunk kétségbe vonni profi szakemberek véleményét. Hiába, **a jövő azért jövő, mert még nem ismerjük**. Tulajdonképpen az ilyen ismertetők is felfoghatók egy jól működő support tájékoztatási feladatának. Ezen írásokban az is jól látszik, hogy **nem valószínű, hogy az Apokalipszis négy lovasa vágtasson be minden számítógépre a földgolyón**, hanem főként azok a Windows gépek lesznek veszélyben, **ott várhatóak további hatások, amelyek már fertőzöttek és a botnet hadsereg részei**. Mindenesetre, ha szükséges, az ESET ingyenes Conficker eltávolítója letölthető innen.

Emellett érkezett hozzánk **egy közlemény is a Magyar Posta részéről**, akik óvatosságból önkéntes számítógépesmóratóriumot rendeltek el, miszerint és itt idézünk egy részletet, és ezúton köszönjük olvasónknak, hogy eljuttatta hozzánk. A levél igazi, személyesen ellenőriztem a hitelességét.

"... március 31-én 22.00 órától várhatóan 2 napig korlátozásokat vezetünk be a Magyar Posta Zrt. informatikai rendszereinek használatában. Az alábbiakban összefoglaljuk, hogy a fenti rendszerkorlátozások hogyan érinthetik az Ön vállalkozását, postai rutinját. Gördülékeny üzletmenete érdekében, kérem, olvassa el az alábbi tájékoztatót! ***A korlátozás idején a Magyar Posta külső e-maileket nem tud fogadni illetve küldeni sem..."***

Szerintünk tényleg nincs ekkora baj, Joanna Rutkowska kedvenc mondásával élve: április elsején "nem szakad le ránk az ég" :-) De **a védtelen, és frissítetlen Windows gépek tulajdonosai egye fene, azért retteghetnek egy icike picikét**, de csak lábujjhegyen...

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1037272

Kommentek:

szvid 2009.03.31. 15:57:08

Milyen jó, hogy Ubuntu Linux van a gépemen már lassan 2 éve! Az ilyen hírek nem hatnak meg különösebben. Úgy kell annak, akinek Windows van a gépén és ráadásul nem is vigyáz!

ezmegmi?? 2009.03.31. 16:09:06

windowsok futnak otthon, de teljesen nyugodt vagyok. nem esztelenul hasznaljuk ugyanis...

Alfonzhal 2009.03.31. 16:09:50

@szvid: És eddig mennyi időt töltöttél el ATI és SB driverek telepítgetésével?

Alfonzhal 2009.03.31. 16:11:43

@szvid: És eddig mennyi időt töltöttél el ATI és SB driverek telepítgetésével?

cworm (törölt) 2009.03.31. 16:18:26

ők legalább tesznek óvintézkedéseket. ha nem tennének és később esetleg baj lenne ebből a confickerből, akkor meg mindenki a postát szidná, hogy miért nem készültek fel, stb stb.

Romkocsmák homályában merengő főállású troll 2009.03.31. 16:26:59

@szvid: Ügyes gyerek vagy.

Fugu 2009.03.31. 16:41:16

márpedig vírusok nincsenek

_tracky 2009.03.31. 16:52:44

Hmm... eltűnt a hozzászólásom. röviden újra: találó volt az egyik cikkben az "ágyúval verébre" hasonlat. gondolom 3 gumi a tuti siker a hancúrlécen, nehogy teherbe essen a hölgyike. fő a biztonság.

a megoldás: néhány szakember a vicces "kikapcsoljuk a netet" dolog helyett. ekkora cégnél ez több, mint vicces...

egyébként tényleg: egy cégnél, ha minden eszközön naprakész a frissítés, és van szintén naprakész víruskergető, kell egyáltalán félni és imádkozni egy-egy ilyen hír hallatán? vagy húzzuk ki a dugót, hogy se ki, se be, és térdeljük le, és imádkozzunk?

szvid 2009.03.31. 17:24:27

@Grundaktiv Gergő: Ameddig a telepítés tartott, ugyanis egyből működött és működik máig is minden! Nem ATI kártyám van, de az se lenne gond, mert épp a napokban adta ki új driverét az ATI. Akik használják azok dícsérik!

Ronald 2009.03.31. 17:31:19

@szvid: Ha nem azzal keresed a kenyered és nincsenek ügyfeleid - akkor egyéb gonzo és partizán rendszerekkel is játszadozhatsz kedvtelésből.
Vagy hagyhattad volna DOS 6.2 alatt is - olyan "tudományosan néz ki " amikor kézzel írsz be mindent - mert a Norton is lámáknak való.
De szeretném én látni, ha egy munkát Word+Ph.Shopban+pdf.-ben kapsz meg kombinálva !, és abból kell hirtelen (1 óra alatt) nyomda alá küldeni egy kicserélt szövegű anyagot...mijalószart csinálsz akkor a Mobutu-dal?
Vagy megmondod az összes ügyfelednek, hogy vagy felhagy a windósozással a francba...vagy téged ne zargassanak többet ?
Mert a linuxos legények kemények ám....az első forintig, amit meg kéne keresni.

Rob67 2009.03.31. 17:53:48

Milyen előrelátó vagyok hogy munkára is meg othhonra is iMacet-eket vettem.
Ez a Windows dolog mindig is rémisztett.

cworm (törölt) 2009.03.31. 17:56:33

@Rob67: ezt kár volt ideírni, mindjárt kapod te is az oltást, hogy a mac-ek a legsebezhetőbbek.:)

boldiii 2009.03.31. 17:57:20

Nem az ágyúval lövöldözéssel van a baj, hanem hogy a verebet akarják elkapni. Nem azért veszélyes ez a féreg mert holnap több lesz az email vírus.

Az lesz a gond, és ez kedves ubuntus barátunknál is probléma, ha mondjuk DoS támadást kapnak a root dns szerverek, vagy a bix, vagy direkt szvid, vagy a posta. Vagy ha 12 millió gép merevlemeze törlődik, vagy kódolódik. Ettől még nyilván rövidesen megoldódna a helyzet a fenti események bekövetkezése után is, de azért tényleg komoly gondot jelentene.

szvid 2009.03.31. 18:01:58

@Ronald: Soraidból kitűnik, hogy soha nem láttál "élő" linuxot! Még a nevét sem ismered. UBUNTU a hivatalos neve a linux disztribúciónak amit használok. Jól jegyezd meg, mert egyre többen használják és még neked is hasznodra lehet.
Mivel nem ismered a linuxot így nincs miről vitatkoznunk.Minden állításod megcáfolható csípőből. Csak azért nem teszem, mert nem lenne korrekt részemről!

aqswdefr 2009.03.31. 18:04:19

Öö, ott nincs olyasmi, hogy központi kliens-menedzsment, vagy ilyesmi? Mondjuk arra a pár gépre lehet, hogy nem érdemes összerakni.

gothmog 2009.03.31. 18:12:42

@Ronald: És az neked miért is fáj?

"mijalószart csinálsz akkor a Mobutu-dal?"
Például internetet használ, (levelez, böngész, torrentez, csetez, emesenez), multimédia alkalmazásokat futtat (filmet néz, zenét

hallgat), dokumentumokat szerkeszt (szöveg, táblázat, prezentáció, pdf), fotókat editál (gimp), ilyesmi. A kicsit elvetemültebbek 3D-ben dolgoznak (Blender, Wings, Maya*)), és vektorgrafikát szerkesztenek (Inkscape, Xara Extreme)
Mindezt legális szoftverekkel, ingyen. (*kivéve a Maya, az fizetős)
Vírusok nélkül.

De legyen neked igazad, nyilván életszerű, hogy egy családi pécén pdf-psd-doc kombóból kell nyomdai munkát összedobni fél nap alatt.
(Egyébként megsúgom, csak azért nehezebb ez ubuntun, mert más szoftvereket kell használni, amiknek a megtanulásába időt és energiát kell fektetni)
Ja és Mobutu az közép-afrika, pontosabban Kongó (volt Zaire), míg az Ubuntu dél-afrika. Ne keverd össze.

KaPé 2009.03.31. 18:15:51

@aqswdefr: Pár gép? Ha jól tudom, jelenleg a Posta a legnagyobb foglalkoztató Magyarhonban, 30-valahány ezer emberrel. Nem hiszem, hogy csak pár gép lenne. Inkább pár ezer.

Dövan 2009.03.31. 18:22:35

Szerintem semmi sem lesz. Ugyanúgy, mint eddig.

Dövan 2009.03.31. 18:40:27

Tényleg, ott ahol már elseje van, ott már odab.ott?

gothmog 2009.03.31. 18:43:31

Amellett a conficker továbbra is egy 2008 októberében _javított_ windows hiba hátán képes bejutni a gépekre. (plusz hálózati megosztás, plusz pendrájvok, ha igazságosak akarunk lenni)

www.microsoft.com/downloads/details.aspx?displaylang=hu&FamilyID=0d5f9b6e-9265-44b9-a376-2067b73d6a03

Törpe minoritás 2009.03.31. 19:38:05

A Linux vallás. Onnan lehet tudni, hogy a vallásos embereknek nincs semmi humorérzéke.
(Amúgy Mobutu egy ember volt, nem ország...)

gothmog 2009.03.31. 20:04:51

@Törpe minoritás:
A zárójeles rész: olvasd már el amit íram, és próbáld értelmezni, lécci? Vagy leírom úgy hogy érthető legyen: "A _Mobutu_ név közép-afrikához, pontosabban a Kongói Köztársasághoz (volt Zaire) kapcsolódik, míg az _Ubuntu_ a dél-afrikai születésű Mark Shuttleworth-ön keresztül Dél-Afrikához. Érthető-e vagyok?

Egyébként tudom mi a humorérzék (egy különlegesfajta mérőműszer, ugyebár), csak ez úgy van, hogy a linux-júzereket szokták nagyarcúsággal, meg a többiek lenézésével vádolni, miközben én pl. soha nem használtam a "winfos" "mikrofos"-stb jelzős szerkezeteket (furcsa is lenne, minthogy időnként én is kénytelen vagyok win-t használni), ellenben Ronald kolléga megengedett magának valami ilyesmit.
De ha csak viccelt, akkor semmi gond. Ércsük. Haha.

aqswdefr 2009.03.31. 20:24:54

@KaPé: Nemmondod.

nius 2009.03.31. 20:35:56

A Postának vírus se kell, leszakad magától. Olyan mint az albán vírus.

Mindfield 2009.03.31. 21:05:00

De nem látják, hogy van ott valami odanemillő progi, ami menni akar kifele?

gothmog 2009.03.31. 21:17:59

@Mindfield:
De látják, csak nem sejtik... :)

Dövan 2009.03.31. 23:29:01

Nos, itt éjfél elmúlt, de semmi extra hálózati aktivitás nincs a szervereinken...

Egyelőre az innen kb 150 km-re lévő atomerőmű sem pukkant mert áram is van :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.02. 10:46:57

@Ronald:

Üdv a blogon :-)

Már mások is válaszolgattak neked, de én is szeretnék.

Kedves barátomat, Nagy Gábort tudom csak idézni, aki a saját könyveit maga is tördelte Tex/Latex rendszerben Linux alatt tökéletesre. Szóval a professzionális kiadványszerkesztésnek vannak hagyományai Linuxon is, nem csak Windowson illetve a legismertebb Mac OS X-n.

Mindenkinek más a munkája, más a munkafeladata, például a víruslaborban sokkal többen csapatják Linux alól, mint Win alól, de mégsem gondolnám, hogy szárnyaszegetten éreznék magukat :-D A kongói Mobutu Sese államfőnek egyébként abszolút semmi köze a dél-afrikai Michael Shuttleword féle Ubuntu disztribúcióhoz. Ez egy Debian alapú, és igen barátságos OS, számtalan ismerősöm gyereke, felesége, anyósa, stb (kutyája ;-) használja elégedetten, akik egyáltalán nem profi számítógépesek.

"De szeretném én látni, ha egy munkát Word+Ph.Shopban+pdf.-ben kapsz meg kombinálva !, és abból kell hirtelen (1 óra alatt) nyomda alá küldeni egy kicserélt szövegű anyagot" Mindenki azt tudja jól csinálni, amiben jártas. Más szavakkal: "Minden egyszerű, ha már eltöltöttél pár évet a hosszászokással." Semmi akadálya nincs, hogy a Word formátumú doksit készítsen, javítson valaki Linux alatt OpenOfficeban (itt direktben PDF-be is lehet menteni), de az AbiWord is használható. Bár Photoshop valóban nincs (bár van például Crossover nevű fizetős program, amivelbonyolultabb Windowsos programokat is lehet telepíteni, mint amit az alap WINE elbír), de van GimpShop, Xara Xtreme, Inkscape (ez amolyan CorelDraw szerű cucc), stb.

Szóval szerintem nagyon is használható ez a platform, inkább az olyan esetekben nem jó, ha AutoCAD-et, SAP-t, Adobe Flash készítést, vagy egyéb speciális dolgot kell megvalósítani, ezeket már én is Windowson csinálom.

gothmog 2009.04.02. 21:52:45

@Csizmazia István [Rambo]:
Amit még megjegyeznék ezzel kapcsolatban, hogy aki Photoshopot, Autocadet, Cubase-t, 3DStudiot (vagy más nagy értékű win-specifikus professzionális szoftvert) pénzkereseti célra használ, az
1. megvásárolta ezeket (ugye?), alkalmasint komoly pénzt ölt a kiszolgáló hardverbe is, így számára másodrendű kérdés a windows 30e körüli ára.
2. nem a munkára használt számítógépén fog -khm...- nem biztonságos weboldalakat látogatni, vagy hasonlókat cselekedni (ugye?), így számára másodrendű kérdés a windows esetleges (mellesleg kifoltozható) biztonsági kockázata. Főleg, mivel a win-t úgyis megvásárolta*, tehát rendelkezésére áll a windowsupdate, meg a hivatalos support.

(*a nem munkára használt gépre, és a gyerek meg a kedves házastárs gépére is -hiszen nekik is szükségük lehet az első forintra, amit meg kéne keresni-, ugye.)

Szenzáció! Magyarok írták a Confickert!

2009.04.01. 12:22 | Csizmazia István [Rambo] | 11 komment

Címkék: móka április elseje

Nem várt meglepetésre derült fény: két budapesti végzős egyetemista munkája a világszerte fejtörést okozó Conficker féreg és a köré épített botnet hálózat. A két letartoztatott fiatal az első kihallgatáson **elismerte ugyan, hogy valóban ők készítették a programot, illetve annak fő komponenseit, azt azonban tagadták, hogy ők irányították volna** a teljes bűnszervezetet is.

Kifejezetten pénzkeresési szándékkal fogott bele Á.E. és Á.B. még a tavalyi év elején a fejlesztésbe. Mivel mindketten **alapos programozói, és TCP/IP ismeretekkel rendelkeztek, és már a programfeltörésben is sok éves rutinjuk volt**, elhatározták, hogy új projektjükkel anyagilag is jelentős haszonra tesznek szert. Közelebbi részleteket nem tudunk, annyi azonban már kiderült, **a véletlennek köszönhető a letartóztatásuk**.

Bár **alapos hálózati ismereteik miatt az antivírus szakértőknek technikai eszközökkel nem sikerült elkapni őket** - hiszen minden kapcsolatnál többszörös proxy szervert és egyéb megtévesztéseket használtak. Végül **úgy sikerült leleplezni őket, ahogy Al Caponet is - a pénz irányából**. A Nemzeti Nyomozó Iroda vizsgálódott egy korábbi nemzetközi banki bejelentés alapján az FBI egy speciális banki csoportjával együttműködésben, akik országokon átívelő kétes tranzakciók után nyomoztak. Ennek keretében tartottak váratlan házkutatást egy Pest környéki családi házban még március 30-án, ahol **a tucatnyi lefoglalt számítógépen és mobileszközön a szakértők legnagyobb meglepetésére mindenféle titkosítás nélkül előbukkantak leleplező adatok, forráskódok, könyvelési listák, lopott bankszámla információk**. Számos hamis személyazonosságot is használva, külföldi chatszobákban árusították szolgáltatásaikat - ahova hamis, jellemzően különféle orosz neveken jelentkeztek be. Szakértelmükre jellemző, hogy **még saját fejlesztői környezetet is készítettek LIRPA néven**, amely minden részletében elképesztően kifinomult és jól használható keretrendszert biztosított nekik az anonim tényked éshez.

Több részletet egyelőre nem sikerült megtudni, a bővebb tájékoztatást későbbre ígérték az illetékesek.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1039268

Kommentek:

Plag 2009.04.01. 13:00:14

Ha ez fake, én ezzel nem szórakoznék, függetlenül, hogy április 1 van!

// Gery Greyhound · http://gerygreyhound.tumblr.com 2009.04.01. 13:08:45

Le van rohadva a Datanet, erről tud valaki valamit?

Éjszakai őrség · http://eo.blog.hu 2009.04.01. 13:22:55

A csávó tényleg úgy is néz ki, mint egy vírusíró gyerek, nem pedig mind egy drogdíler. :)

payskin 2009.04.01. 13:40:38

Á.E. és Á.B. 10/10 :-)

cworm (törölt) 2009.04.01. 14:11:44

LIRPA = APRIL :P

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.01. 14:27:31

Szia Payskin és Cworm!

Úgy látom, kezdenek helyrekerülni a dolgok.

TRf felülmúltad minden várakozásomat, még csak remélni sem mertem, hogy még ezek az aprócska nüanszok is megértő olvasókra lelnek majd :-D

dJw_ · http://rendszergazdak.blog.hu 2009.04.01. 20:35:58

már majdnem elhittem :) de megnéztem a képet és kizárt, hogy a csávó bármi is értsen az informatikához :DD

cworm (törölt) 2009.04.01. 20:45:08

na jó, de azért itt a blogon sokszor nem éppen a hírhez szorosan kapcsolódó képek vannak, sőt talán soha, úgyhogy ezt még fel lehetett volna fogni illusztrációként (amúgy is nagyon amerikaiasan néz ki az a ház:D). (Mármint úgy vettem észre, hogy csak a screenshotok szoktak a hírekhez kapcsolódni, persze valamennyire a többi kép is, de azokat nem konkrétan az adott hír miatt készítették:)
Remélem érthetetlen és sötét voltam:D
Igazából nem is tudom mit akartam ezzel mondani.

zsu.zsi 2009.04.02. 11:41:22

Szia Rambo!
Amikor tegnap délután olvastam, én is majdnem elhittem :-)
A harmadik bekezdés első mondata is sántított :-) Rendszerint nem szoktál így fogalmazni, az "és egyéb megtévesztéseket

használtak" tőled fura volt, mert korábban mindig részletesen el szoktad mondani, hogy egészen pontosan milyen megtévesztéseket használnak...
:-DDD

Anulu · http://salgoauto.hu/ 2009.04.09. 14:43:27

Nem tartom valószínűnek, hogy Pest melletti családi házba Los Angelesből szállnak ki a rendőrök. :D

Anulu · http://salgoauto.hu/ 2009.04.09. 14:55:46

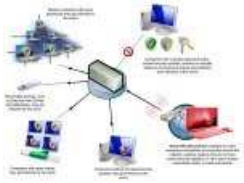
De áprílisi tréfának pont jó volt! :)

A szakértők szerint pánikra nincs ok

2009.04.02. 13:21 | Csizmazia István [Rambo] | 3 komment

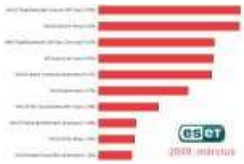
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET víruslaboratóriumának szakértői szerint április 1-jén megváltozott a Conficker féreg automatikus frissítési módja. A változás azt biztosítja, hogy a megfertőzött számítógépek hálózata minden esetben irányítható maradjon, de pánikra nincs ok.



A tavaly októberben megjelent, Conficker névre keresztelt internetes kártevő az elmúlt hónapok során világszerte több százezer számítógépre telepedett. Ilyen heves víruskitörésre évek óta nem volt példa. **A víruslaboratóriumok már korábban visszafejtették a féreg kódját**, így ismertté vált, hogy annak új mutációi április 1-jétől megváltoztatják működésüket. Ettől az időponttól kezdve **a Conficker egy 50 000-es webcím listából véletlenszerűen kiválaszt 500-at**, és megpróbál rájuk csatlakozni. Ilyen bonyolultságú infrastruktúrát eddig egyetlen kártevő mögé sem építettek a bűnözők. A szakértők szerint ugyanakkor a vészharangok kongatására nincs ok, mivel **a frissített vírusirtó szoftverek védelmet nyújtanak a Conficker.X névre keresztelt új variáns ellen is**.

*„Az ESET víruslaboratóriuma kiemelt figyelemmel kíséri a Conficker változatokat. A proaktív vírusvédelemnek köszönhetően termékeink eddig sikeresen azonosítani tudták a Conficker féreg legújabb variánsait, honlapunkon pedig **ingyenesen elérhető egy, a fertőzött gépek megtisztítására alkalmas víruseltávolító alkalmazás is**”* – emelte ki Csiszér Béla, az ESET NOD32 Antivirus magyarországi forgalmazásáért felelős Sicontact Kft. ügyvezetője. A szakértő hangsúlyozza, hogy április 1-je előtt **minden felhasználónak érdemes ellenőriznie számítógépét, és megbizonyosodnia arról, hogy telepítésre kerültek az operációs rendszer aktuális frissítései, valamint hogy a gépet védelmező vírusirtó szoftver az aktuális vírusdefiníciós adatbázist használja**. Ez a két tényező alapvető szerepet játszik abban, hogy a gép megfelelő védettséget élvezzen, **a Conficker.X azokat az elhanyagolt számítógépeket tudja megfertőzni**, melyek tulajdonosai nem törődnek a frissítésekkel. A féreg terjedésének teljes megállításához egyébként mind az 50 000 domaint le kellene tiltatni, de jelenleg nem létezik olyan szervezet, mely ezt megvalósíthatná.



Végül következzen **a magyarországi toplista. Az ESET statisztikai rendszere szerint 2009 márciusában az alábbi 10 károkozó** terjedt a legnagyobb számban. Ezek **együttesen az elmúlt havi frissítések 35.18%**-ért feleltek.

1. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége a márciusi fertőzések között: 5.65%

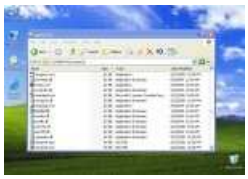
Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programba szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a „csomagban”. Emellett hátsó ajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-nbf

2. Win32/Conficker féreg

Elterjedtsége a márciusi fertőzések között: 5.62%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/conficker-x

3. WMA/TrojanDownloader.GetCodec trójai
Elterjedtsége a márciusi fertőzések között: 4.62%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

4. INF/Autorun vírus
Elterjedtsége a márciusi fertőzések között: 4.58%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

5. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a márciusi fertőzések között: 4.51%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

6. Win32/Agent trójai
Elterjedtsége a márciusi fertőzések között: 3.57%

Működés: Ezzel a gyűjtőnévvel azokat rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a rendszerleíró-adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat, illetve .exe kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

7. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a márciusi fertőzések között: 2.39%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására és a jelszó adatok titokban való továbbküldésére fókuszál. A távoli támadó ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthat hozzá, amelyet aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

8. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a márciusi fertőzések között: 1.49%

Működés: Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró-adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

9. Win32/VB.EL féreg
Elterjedtsége a márciusi fertőzések között: 1.43%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is. Árulkodó jel lehet a sal.xls.exe állomány

megjelenése a C: és minden további hálózati meghajtó főkönyvtárában.

A számítógépre kerülés módja: fertőzött adattároló (USB kulcs, külső merevlemez stb.) csatlakoztatásával terjed.
Bővebb információ: http://www.eset.hu/virus/vb-el

10. Win32/Adware.GooochiBiz alkalmazás
Elterjedtsége a márciusi fertőzések között: 1.32%

Működés: A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működése közben távoli webcímekre csatlakozik és onnan reklámokat tölt le. Sok kártevő vet be olyan trükköket, amellyel saját lelepleződésüket igyekeznek elkerülni. Az Adware.GooogchiBiz a tasklistában is nyomon követhető folyamatok közül a normál körülmények között is megtalálható iexplore.exe mögé igyekszik elbújni. Emellett hátsó ajtót is nyit a rendszerben, melyen keresztül a távoli támadó később is könnyen hozzáfér a már megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-goooochibiz

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1041279

Kommentek:

satie · http://321.hu/sas 2009.04.02. 14:21:13

Pánikra semmi ok, hisz ott a Linux, ami kényelmesebb is, és nem tudnak ártani neki a vírusok sem :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.02. 15:11:07

Hi Satie!

Na ja, és ez a pénzspórolás miatt még fokozódik is:
Élénk az érdeklődés a Linux iránt a gazdasági válság idején

itmania.hu/tart/cikk/e/0/41948/1/informatika/Elenk_az_erdeklodes_a_Linux_irant_a_gazdasagi_valsag_idejen

MILCSI 2009.05.03. 16:53:48

Linux,Linux...hiába,ha nem viszi a játékaimat :-PPP

A pofátlanság csimborasszója

2009.04.03. 21:59 | Csizmazia István [Rambo] | 1 komment

Címkék: spam kanadai kínai gyógyszerész

Napjaink spam üzeneteinek **döntő többsége valamilyen kínai eredetű kanadai gyógyszerész oldalra** mutat. **Egy apró kis momentum** azonban megszinesíti hétköznapjainkat, és feleleveníti ezenközben a kedves klasszikus paradoxont, amiben "minden római hazudik" mondja a római hadvezér. És akkor nehéz eldönteni, ha ez most igaz, akkor nem igaz az, hogy... viszont ha hazudik, akkor meg az sem igaz, hogy... Na jó, hagyjuk az egészet, beszéljünk másról :-)

Semmi különös újdonságot nem mutat a mai kéretlen levél sem, amit **a Gmail rendre szépen ki is tesz a spam mappába**. Mondjuk ahhoz is kellhet már egy speciális gusztus, hogy **valakinek megjöjjön a kedve egy "Ooxaj Uxaz" nevű linkre való kattintáshoz**, de hát Istenem, nem vagyunk egyformák, van aki felfelé sikít a hullámvasúton.

Az is közismert, hogy az ilyen kéretlen levélben szereplő **állítólagos hírlevél leiratkozást sem érdemes használni, hiszen ezzel csak megerősítjük, hogy igen, él a címünk**, és még több szemét érkezik a továbbiakban, hiszen a címjegyzékeket folyamatosan adják-veszik a feketepiacon.

A fehérköpenyes dokik képei is variálódnak a dizájnban (lassan már Fábry is tarthatna egy külön Dizájn center special editiont az ilyen weblapokból), nővérkével, nővérke nélkül, kutya és gyerek ezúttal nincs, láthatóan alulműveltek a sikeres kinézet tárgykörében;-) De egy momentum látszólag állandó, **az orvososnak látszó tisztes őszes halánték, amely megpróbálja "hitelesíteni"** a bálnazsírból, oposszumürülékből és kutyatáp-örleményből ;-) vegyített hamis készítményeket. Jó hír lehet a nagyközönségnek, hogy az ilyen kapszuláktól eddigi tapasztalatok szerint kísérleti patkányok mindössze 13.2 százaléka pusztult el laboratóriumi körölmények között, ezért a roppant kedvező árfekvés miatt érdemes lehet rendelni ; -)

Ami viszont végképp mókás, hogy **a weboldalak kinézetéhez szervesen hozzátartozik nemcsak a nemműködő**, de azért látható "Contact us" menüpont, hanem találunk itt - mindenki kapaszkodjon, paradoxon következik - **"Report spam" opciót is**. Vagyis a spam levélben érkezett linken található weboldalba szemérmetlenül gyárilag beépített spam feljelentő gomb illeszkedik szervesen :-O Ez pedig már annyira perverz, hogy ha nem sírnánk, nevetnénk...

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1043283

Kommentek:

dJw_ · http://rendszergazdak.blog.hu 2009.04.04. 12:02:02

no igen... némely spaminkább nevezhető tréfásnak, mint komolyanvenné bárki épeszű európai is... persze kérdés, hogy milyen hatékonysággal működik ugyanez a mail indiában, kínában, tajvanon... lehet hogy ők felfelé sikítanak? :D

Mindenről az jut az eszébe...

2009.04.08. 07:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam bank kéretlen gyógyszerész

Lassan **nem is lesz érdemes megnézni sem az e-mailek feladóját, sem pedig a levél tárgyát**, az eredmény szinte mindig ugyanaz: kikötünk egy gyógyszertárban.

A post címe egyébként egy régi viccből való, amelyben a nő elmegy a pszihiáterhez, aki egy négyzetet rajzol egy papírra, és megkéri a pácienst, hogy mondja meg, mi jut róla eszébe. "Bent vagyok a szobában, egyszercsak feltépi az ajtót egy nagy drabális szőrös mellű férfi, és nyomban a magává tesz". Az orvos hümmög, aztán rajzol egy háromszöget, és újra felteszi a kérdést. A nő máris válaszol: "Bent vagyok a sátorban, egyszercsak feltépi az ajtót egy nagy drabális szőrös mellű férfi, és nyomban a magává tesz". Csóválja a fejét a doki, de azért újfent rajzol, ezúttal egy kört. "Bent vagyok a fürdőmedencében, egyszercsak feltépi az ajtót egy nagy drabális szőrös mellű férfi, és nyomban a magává tesz". Az orvos elképedve kérdezi: Mondja asszonyom, magának mindenről ez jut az eszébe?! "Miért kérdi? Hát nem maga mutogat nekem ilyen képeket..."

Sose gondoltam volna, hogy ennyit fogunk foglalkozni az ilyen spam levelekkel, de valószínűleg másnak is tele a búrája és a postafiókja velük. **A gazdasági válságot meglovagolva ímmel-ámmal beleírnak a subject mezőbe egy kis "personal loan information", meg "Credit card balance transfer", és "Bank account blocked" szöveget**, de mélyen szánalmas módon kilóg a hatalmas lóláb, hiszen a szövegtörzs első sorában olvasható a "Subscribe to Men's Health today", azaz mosolygó **tisztes őszes halándékú doki bácsi ajánlgatja kínai szerveren hostolt "kanadai gyógyszerész" boltját**. Igenis **kérünk több mézet a madzagra**, legalább tegyenek úgy mintha Pam Anderson videóját ajánlgatná, vagy legalább valami ingyen diplomát vagy nyelvvizsgát kínáljon, aztán majd csak a linkre kattintva derül ki számunkra, hogy hohó, hát ez nem is az, aminek mondja magát ;-) Ráadásul fantáziátlanul többnyire mi magunk vagyunk a "feladók". Ilyen mukinyulas, **szinvonaltalan** hanyag munkát még nem látott a világ, **felhígult a "spammer szakma", egy percig sem lehet vitás**

Igaz, amikor más jut az eszébe, akkor a levélben már lehet például Conficker férget irtó állítólagos segédprogram vagy **hamis botnet eltávolító, amely aztán mentesítés helyett jól letölt további kártevőket,** illetve pénzt zsarol, és valljuk be, ez azért sokkal veszélyesebb. Akkor már inkább egy kis ungabunga vagy maradjon a patika...

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1052528

Kommentek:

Nincsenek hozzászólások.

Humán-e vagy?

2009.04.09. 18:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam captcha terjesztés 3d kártevő

Manapság, amikor a spamek és a kártevőket terjesztő e-mailek feladói john1638@yahoo.de, xhzgxzi@hotmail.com, és hasonlók, akkor ugye mindenkinek beugrik, hogy a rosszfiúk **tömegesen és iparszerűen regisztrálnak kamu címeket**, és tolják róla a kéretlen szemetet.

Ezt megakályozandó lenne **az egyik eszköz az a bizonyos Captcha**, amely a "Completely Automated Public Turing test to tell Computers and Humans Apart" azaz "teljesen automatizált nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére" szavak kezdőbetűi alapján kapta a nevét a keresztségben. **A hullámzó betűk, a betűhatárokat összemosó megjelenítés, a betűtesten keresztülfutó vonalak, a színezett, illetve raszterezett háttér** mind-mind amiatt kerültek a képbe, hogy az automatikus felismerést kizárva igazi hús-vér ember lehessen csak képes elolvasni ezeket a feliratokat. Elvileg. Mert furmányos és túlságosan ráérő emberek sikeresen kerülik meg technikailag a módszert, emiatt aztán **a fejlesztők is ötletelnek még újabb** és hatásosabb technikákon.

Talán az egyik sikeres próbálkozás lehet a már nem vadonatúj, de néhány helyen már élesben is felbukkanó úgynevezett 3D Captcha, amely nem OCR-ezhető betűket vagy számokat mutat eltorzítva - **gyakran annyira kretén vonalvezetéssel, hogy a felhasználó is csak 2 sör és 3 unikum után képes kiolvasni azt ;-)** - hanem például ábrákat jelenít meg, amelyeket **az egér segítségével kell egy készletablakból kiválasztva megfelelő sorrendben az üres négyzetekbe bemozgatni és kattintással rögzíteni**.

De az is egy izgalom lehet, ha a **pálcika emberekből kell kirakni az este a székelyeknél népi csendélet figuráit szorgalmas egérkattintások közepette** ;-) Az új eljárás elvileg újra feladja a leckét.

Nem szabad azonban lebecsülni az ellenfelet, amely már számtalanszor bizonyított, **és azt se feledjük**, a hadrendbe állított bérrabszolgák ellen ez a módszer egyáltalán nem véd meg.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1055337

Kommentek:

Nincsenek hozzászólások.

Nézik-e a rablók a Kékfényt?

2009.04.10. 18:59 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: frissítés oldalak conficker blokkolt

Milyen nagyszerű is az, amikor az antivírus tölt le frissítéseket magának. **És mennyivel kevésbé nagyszerű, ha ugyanazt teszi egy kártevő is**. Sőt, ha készítőik a szakirodalmat és a visszafejtési eredményeket is követik csillogó élénk szemekkel :-O

A bazi nagy bekészülés ellenére nem történt semmilyen látványos akció április elsején, viszont tegnap már tapasztalható volt, hogy **a Conficker féreggel fertőzött zombigépek új adatcsomagot kaptak**, és a frissítés néhány részlete is kezd kibontakozni.

Bevezetőként nem lehet eléggé hangúlyozni, hogy elég lett volna/lenne/lesz ha valaki **becsületesen lefuttatja az MS 08-67 biztonsági javítást, és lekapcsolja minden külső eszköz automatikus Autorun futtatási opcióját**. És szinte kivétel nélkül **mindegyik antivírus felismeri már**, elég (lenne) használni azt. Ennyit az ismétlésről, és annak női ágon való családtagjáról, a tudásról.

Újabb határidő is látszik, ezúttal május 3-án megkísérel majd eltávolítani moduljai közül a fertőzött gépekről, igaz erről pontosabb részletek még nem ismeretesek. **Az április elsejei tüske viszont tisztán látható** a Google Trends grafikonon. Elképzelhető, hogy később ezeknek a dátumoknak is lesz valamilyen konkrétabb jelentősége, vagy kihasználható előnye.

És frissült az a lista is, amely leállítani kívánt folyamatokat, illetve a blokkolt domaineket tartalmazta. Pontosabban ezek változások, először jöjjön az a lista, mely processzekkel bővültek a lelövendők:

dwndp
ms08
ms09

És akkor íme a másik, a blokkolandó domainek listája, illetve ezekkel egészültek ki a régebbi tételek:

confick
coresecur
doxpara
fsecure
honey
insecure.
iv.cs.uni
ncircle
nmap.
qualys
secunia
snort
staysafe
tenablese

A régi tételeket már ismerjük, **aki ProcessMonitort vagy ProcessExplorert használ, az nem a barátjuk**. Mazsolázzunk most az újdonságokból néhányat - a teljesség igénye nélkül. Akik figyelemmel kísérik az eseményeket, emlékezhetnek rá, az nmap fejlesztői külön változatot készítettek, amely a felderítést segíti, ez nem tetszik a bűnözőknek. Szintén nyilvánvalóság, hogy a Secunia honlapja hatékonyan segíti a Windows biztonsági frissítések és az alkalmazások új változatainak nyomonkövetését, **tehát ezt is veszélyesnek ítélték.**

De ugyancsak érdekes azoknak, akik olvasták Mikko Hypponen bejegyzését az F-Secure weblogban az április elsejei várakozásokról. Itt a kulcsmondat:

"Don't tell anybody, but users who can't access f-secure.com because of this can surf to www.fsecure.com instead." **Ennek ezúttal vége, hiszen ők is olvasnak internetet**, árgus szemekkel kísérik az utánuk történő nyomozást.

A végére hagytuk azt a weboldalt, amelyet szintén méltoztattak letiltani. A Conficker féregről szépen összeszedett információk mellett talán azért vált számukra veszélyessé a honlap, mert egy frappáns ötlettel egy óvodás is letesztelheti az oldalukon, fertőzött-e a gépe.

Tehát száz százalékos biztonsággal **kijelenthetjük, hogy figyelemmel kísérik a róluk szóló elemzéseket**, ezért lassan lehet üzenni is nekik majd az ilyen cikkekben. Persze csak vigyázva, hogy semmi sértő ne legyen benne ;-) **Reméljünk, mi nem bosszantottuk fel annyira a készítőket**, hogy az antivirus.blog.hu címet is bannolják majd ;-)

Ettől függetlenül **ezúton kívánunk minden kedves Olvasónknak Kellemes Húsvéti Ünnepeket!**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1057321

Kommentek:

Nincsenek hozzászólások.

Támadás a király ellen

2009.04.14. 15:27 | Csizmazia István [Rambo] | 2 komment

Címkék: internet kábel szabotázs

Ha valaki terrorista hajlamú, esetleg Matuska Szilveszter babérjaira tör, és kevésnek találja az SQL befecskendezés, kémprogramok és botnetek, illetve DDoS támadások lehetőségeit, az **az internet megbénításához tud keményebb eszközökhöz is** nyúlni.

Rezgett a léc már az észt-orosz konfliktusnál is, vajon harci cselekmény volt-e vagy sem, de a Kennedy gyilkossághoz, az olajszőkítéshez hasonlóan a titkolózás, a hosszú titkosítási időszak miatt ezt sem fogjuk megtudni soha. De létezik módszer - **még ha egészen eddig nem is tapasztaltuk meg** - az infrastruktúra fizikai elemei ellen is, és ez a megfelelő időpontban végrehajtva **igen érzékeny csapást lehet mérni** a civilizációra.

Néhány napja tapasztalatot gyűjthettek a tárgykörben San Francisco lakói, ugyanis céltudatos **vandálok április 9-én éjszaka átvágták a földalatti száloptikás hálózat telefonos és internetes kábeleit**. Az esemény **semmiképpen nem lehetett véletlen, hiszen több különböző, összesen 4 helyen is megtörtént a kábelek elvágása**, illetve maga művelet sem volt egyszerű, hiszen azt speciális technikai előkészületekkel és a kábelek vastag védőrétegei miatt csak több órás munkával lehetett végrehajtani.

A helyzet cseppet sem volt vicces, hiszen **az érintett körzetekben kórházak és bankok váltak működésképtelenné, megszűnt a pénzautomaták működése, a vészhívó (rendőrség, mentők, tűzoltók) telefonok is elnémultak**, ki tudja hány tragédiát okozva ezzel.

Stratégiai helyszínek esetében (hadügy, pénzügy, egészségügy, államigazgatás, erőművek, stb.) kiemelt figyelem szükséges. **Mostantól kezdve ilyenfajta új veszéllyekkel a gyakorlatban is számolni kell, és jobban kell vigyázni a fizikai infrastruktúrára**. Igaz, a károsult AT & T már kitűzött egy százezer dolláros (kb. 22 millió forint) vérdíjat az elkövetőkre, de **ez bizonyosan töredéke lehet csak** a javítás költségeihez, illetve a kiesett időszak kárához képest.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1064391

Kommentek:

cworm (törölt) 2009.04.15. 09:54:27

Valószínűleg a kábelgyártó/javító cég vágta el a kábeleket, mást nem tudok elképzelni, hogy kinek milyen haszna származhatna ebből...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.16. 09:46:09

Minden elképzelhető. De lehet olyan cég is, aki karbantartásra vagy őrzés/védésre tett ajánlatot, amit mégsem kértek. Lásd maffia módszerek a szórakozóhelyeken: verekedés, berendezés összetörése, majd védelmi pénz szedés vagy hivatalos megbízás fejében saját maguk távoltartása. Minden esetre megszületett itt a Proof of Concept, érdemes lesz kábelnyiszatoló berendezéseket forgalmazó webáruházat nyitni :-)

Még több kávét a nyomozó uraknak

2009.04.16. 13:22 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: microsoft eszköz nyomozás jelszavak cofee

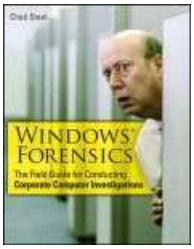
Az Interpol azt tervezi, hogy a bűnüldöző szervek közt **még szélesebb körben használni fogják a Microsoft által kifejlesztett COFEE programcsomagot**, amely egyfajta USB kulcsos nyomozói eszközkészlet.

Maga a rövidítés a **Computer Online Forensic Evidence Extractor elnevezésből származik**, és valamiféle törvényszéki online számítógépes bizonyíték kinyerő alkalmazásnak fordíthatnánk. A 2008-ban megjelent és USB meghajtóról futtatható csomagot akkoriban **15 ország - köztük az USA, Németország, Lengyelország, Új Zéland - mintegy kétezer bűnügyi tisztviselőjének** küldték el, és segítségével akár a helyszínen is értékes bizonyítékokat lehetséges összegyűjteni. Az USB kütyü segítségével sokkal gyorsabban és hatékonyabban lehet a merevlemezek tartalmában vizsgálódni, a **hálózati aktivitásról adatot gyűjteni vagy éppen a rendszerben használt jelszavakat visszafejteni.**

Most jócskán kiszélesítik az eszköz használatának körét, és immár 187 tagországban fogják munkára a "kávét". Ez egyrészt hasznos lehet, hiszen **a digitális bűnözés minden évben egyre több támadást** abszolvál, **még több számítógépen pedig még több bizonyíték** összegyűjtése válhat szükségessé. Másrészt remélhetőleg szakmai képzéssel is fog járni, mert volt korábban néhány olyan **meghökkentő eset, ahol a monitort is lefoglalták**, illetve olyan torrentes trackerszerver került lefoglalásra, amin aztán kihúzva, elszállítva, steril környezetben nem igazán lehetett jogsértő tartalmakat bizonyítékul találni. Magunkközt szólva ha valaki fizetős torrenten pénzért árul lopott tartalmakat, az ne sok megértésre és jóindulatra számítson senki szemében. És ha már ilyeténképpen vargabetűsen elkanyarodtunk sajkánkkal a fősodortól, itt a helye ennek a jó kis mondatnak is :-) *"A világon minden prostituált, pedofil, orgazda, gyilkos, perverz, tolvaj, betörő, kábítószer kereskedő börtönben lehet már, ha van kapacitás torrent szerverre vadászni."*

Visszatérve főcsapásirányunkra egy korábbi interjúból egyértelműen kiderült, a COFEE összeállítás csak nyilvánosan is elérhető segédprogramokat tartalmaz, és állítólag nem kerüli meg a Vista Bitlocker titkosítást sem. (Azért **aki magának az operációs rendszernek a beépített titkosítását használja megfelelően erős thirdparty program helyett, az elgondolkodhat**.) Talán arra a feladatra szánhatták, ahol maga **a vizsgálódó nem ért különösebben a számítógéphez, de mégis tömegesen el kell végeznie valamiféle adatgyűjtést**, hiszen magára valamit is adó szakértő fegyvertárában inkább olyan eszközök lapulnak, mint az Ophcrack, Hiren's Boot, és hasonlók.

Emellett itt is igaz, hogy **a professzionális bűnszervezetben tényked, kártevőket iparszerűen terjesztő réteg nem fog ettől a hírtől ambruskyrit elkövetni**, hiszen jobbára alternatív operációs rendszerrel és fejlett titkosítással védelmezik adataikat.



Mindezek ellenére, **ha valakinek COFEE fronton van bővebb személyes tapasztalata, bátran kommentezzen ide róla**, például kaptak-e el vírusírót ennek az eszköznek a segítségével; vajon csak Internet Explorert támogat-e, vagy alternatív (Fox, Opera, stb.) böngészők cachében is bír kutakodni; mit talál egy alapos CCleaner után; mennyire használható, valamint hogyan miért és egyáltalán ;-)

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1068103

Kommentek:

Nincsenek hozzászólások.

Itt járt Ricky Martin

2009.04.17. 11:36 | Csizmazia István [Rambo] | 2 komment

Címkék: link komment 2009 and hamis vírusirtó search kártevő destroy

Egész pontosan nem járt itt, sőt sajnos nem is személyesen, illetve hát szóval izé hmm khhm tisztelt Bíróság.... mindössze **hozzászólásaival emelte szerény blogunk színvonalát rickymartin1969@gmail.com e-mailcímről** és így tette tiszteletét tegnap délután az oldalunkon.

A mindenféle koncepció nélkül érkező és **saját weboldalát népszerűsítő Spider Net nevezetű kommentelőt nem zavarta, hogy angolul irkál ide**, igen valószínű, hogy a Google segítségevel talált ránk, és talán a Translate nyersfordítása alapján gondolta úgy, hogy érdemes lesz elhelyeznie tíz darab kommentet saját reklámozgatásával. **Szerencsére brit tudósok már egy ideje felfedezték a Delete gombot ;-)**

Egy spamellenes weboldalon el is kezdték már feltérképezni a március vége óta bőrébe nem férő indiai jóember által használt juzernevet és IP címeket, így vélhetően máshol is próbálkozott már hasonló akciókkal a Mike123 nevű félig állati, de félig sem emberi lény ;-)

Az általa reklámozott kártevőt tartalmazó weboldalt szándékosan nem linkeltük be, nem szándékozunk ezzel is növelni egy ilyen csaló és kártékony programot terjesztő weboldal nézettségét. Sajnos az is benne van a dologban, hogy valóban létezik egy hasonló nevű valós és jól működő Spybot Search and Destroy alkalmazás, **aminek a nevéből átvettek egy kicsit, arra hajazva, így alaposabb lesz a megtévesztés**. A VirusTotalos vizsgálat eredmény azonban természetesen megmutatjuk.

A kommentelő jó édes anyukája talán maga sem értette rejtélyes és hosszan tartó csuklási rohamainak valódi okát, midőn panaszával felkereste mind területileg illetékes háziorvosát, emellett három külön magántanárt és specialistát, valamint egy csodatévő gyógyfüves öregasszonyt is. Talán ha sejti, hogy fiacskája beletrollkodott idióta firkálmányaival a kommentjeink közé, esetleg felsejlett volna valami egy határozott "Aha" élmény képében a tudata hátsó szegmensében.

Van viszont egy **jó kis mondás, melyet még Moldova György: Égi szekér című könyvében** olvastam: *"A díjugratásokon van egy szabály, hogyha a versenyló bukik és nem tudta befejezni a futamot, egy akadályt mindenképpen átugratnak vele, mielőtt levezetnék a pályáról; nem viheti magával egy kudarc emlékét."* Nos mi is pozitívan gondoltuk befejezni a postot, már csak **Ricky Martin iránti tiszteletből is - ezért egy vidámabb végkicsengéssel fogjuk lezárni** a mai irományunkat, íme:

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1070215

Kommentek:

Vargnatt 2009.04.17. 14:28:41

Ja, a tegnapi poszt után az a komment nekem is erősen gyanús volt, ezért nem is néztem meg a belinkelt oldalt, csak a phishtank.com-on néztem meg, hogy nincs-e bejelentve adathalászatra. Bár nem talált semmi infót róla, azért sejtettem, hogy valami nem stimmel a címmel.

Amúgy nem kellett ehhez GoogleTranslate, az antivirus elég nemzetközi kifejezés, gondolta, itt biztos lesz pár delikvens, akik ráharapnak a csalira. Azt nem tudhatta, hogy a hozzá hasonló salakanyag-keverőket már rég kibeszéltük itt :)

Egyébként gratula a bloghoz, a kedvenceim között van, már nagyon sok hasznos és érdekes (és humoros) infót olvastam itt, köszönet érte!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.20. 16:13:49

Szia Vargnatt!

Közben a Zindexesek is megigérték, kitörlik ezt a juzert. Van egyébként valami ördögi abban, hogy "ismeretlen linkre nem kattintunk", és közben épp egy ilyen biztonsági bloghoz (is) beszúrják a szemetüket. Gondolom a Barbie babás, a Kutyuli-mutyulis, meg a Kevésbé foglalkoztatott bébiszitterek blog is kap azért belőle :-)

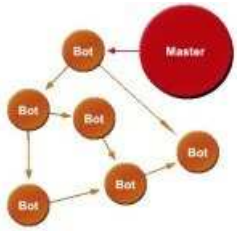
Mac Mester irányíthatja a Mac botnetet ;-)

2009.04.20. 19:39 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac os x zombi botnet

Akik eddig **kizárólag a Windows gépek sajátosságának gondolták az elzombiasodást**, azoknak most intő jel lehet, hogy Winek eddigi egyeduralma mellett felbukkant az első OS X-es gépeken futó iBotnet is.

Bár a problémák 99.9%-át megússzuk, de azért nem jelent teljes védettséget az alternatív operációs rendszer használata. A figyelmetlen felhasználó itt is kattinthat és telepíthet szinte bármit. A mostani hír szerint pedig egy már korábbi kártevő **új variánsa immár p2p és botnetes tulajdonságaira figyeltek fel kutatók** - DDoS támadást lehetett indítani a segítségével. A korábbi változat volt az, amely az év elején **lopott (kalóz) Apple iWork 09 illetve Photoshop másolatokkal terjedt**. Akit érdekel a dolog bővebben, olvassa el az alábbi blogbejegyzést - mi mindenre képes a PHP kód :-).



Az természetesen **nyilvánvaló, hogy ezidáig sokkal kevesebb kártevő létezik az Apple gépein, de** senki nem garantálja, hogy a számuk nem indul gyarapodásnak. Azt is tényként kezelhetjük, hogy nem minden felhasználó van tisztában a veszélyekkel, használjon bármilyen platfomot. És érdemes lenne az újabb fejleményekre legalább odafigyelni, nem pedig hivatalból letagadni azokat, vagy homokba dugni a fejünket. Az ESET szakembere, Randy Abrams személyes kommentje a hír kapcsán egyébként ez volt: **"Azok, akik elfelejtik a múltat, arra itéltetnek, hogy megismételjék azt."**

Egy dolog biztos, ahogy egyre jobban terjed és minél több Mac gép lesz, annál nagyobb az esélye annak is, hogy valamilyen szinten itt i megpezsdül a kártevő készítők fantáziája. A mostani botnet hálózat **feltételezett mérete egyelőre mindössze pár száz, esetleg ezer leh ennek ellenére komoly figyelmeztetést kaptunk**, amivel a jövőben számolni kell.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1075469

Kommentek:

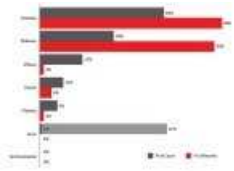
Nincsenek hozzászólások.

Erre hajtottak a bűnözők 2008-ban

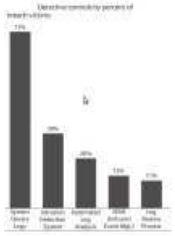
2009.04.21. 13:47 | Csizmazia István [Rambo] | 1 komment

Címkék: statisztika incidens kártevők verizon adatlopás

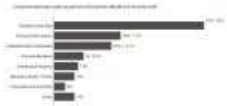
Kiadta az éves jelentését a Verizon, amelyből kiderül, mik voltak a főbb tendenciák, események, **milyen adataink sérültek, hogyan és miképpen kerültek illetéktelen kezekbe leginkább**.



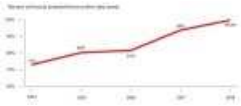
A cég már 2004 óta ad ki hasonló éves értékeléseket, melyeket saját, első kézből szerzett adataik alapján állítanak össze. A mostani 2008-as esztendőre vonatkozó számok sem adnak okot bizakodásra, hiszen a címlapon a **"285 millió ellopott adattétel"** szerepel. Noha az adatok elleni támadásoknál most sem kicsi a belsős forrásból induló akciók száma, inkább a kívülről indított események száma növekedett. A fő csapásirányok közt találhatjuk az online adatok elleni támadást, a célok között pedig senkinek **nem okoz meglepetést, a pénzt vagy közvetlen nyereséget hozó személyes, banki vagy egyéb** információk automatizált megszerzése dominált. **Egész háttériparág üzemel már a lopott bankkártya adatokkal** történő visszaélések mögött. A táplálkozási lánc **csúcsán a statisztikák szerint a rosszindulatú hacker tevékenység és a kártevők terjesztése** szerepeltek.



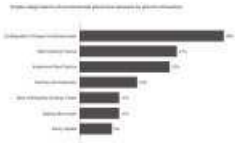
A logok jelentősége minden incidens esetén kulcsfontosságú



A személyes és pénzügyi adatok a favoritok, és válság miatt ez így is marad



Az adatok mögé azért a számítógépek egyre növekvő számát is oda kell gondolni



Javasolt gyógymódok és köpönyegek eső után

A jelentés olyan szempontokra is kitér, hogy a vállalatok általában hogyan védekeznek ezekkel szemben: hibátlan konfigurálás, rendszeres frissítések, szakmai továbbképzések, tanfolyamok, stb. Nem meglepő az sem, hogy **kiemelik a logok elemzésének fontosságát, és a különféle behatolásvédelmi eszközök jelentőségét**. Egy azonban biztos: a jövőre megjelenő hasonló összefoglaló címében egy **x > 285 millió** szám fog szerepelni - sajnos.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1077518

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.05.06. 19:41:20

A gazdasági válság látszólag nem hat a biztonsági cégek eredményeire:
newsroom.mcafee.com/article_display.cfm?article_id=3513

Érezd a ritmust, vedd át az ütemet!

2009.04.22. 17:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google teszt captcha forgatás tervezet turing

Dübörög a hangfalból egy üzenet. Illetve ez **az üzenet inkább a monitoron közlekedik, és a fejlődés útján ez a Google szakemberei által elképzelt modell is egy újabb állomás lehet** a Captchak evolúciós sorában.

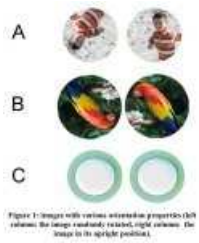
Gyorsan elintézzük a kivételt: irodákba zsúfolt, fillérekért dolgozó indiai bérrabszolgák ellen **természetesen és sajnos** nem véd, de felvázolhat egy utat a jövő "humán-e vagy" kérdésére. A publikus szolgáltatást az erőforrást rendelkezésre bocsátók nem szeretnék, ha **nem hús-vér emberek, hanem gonosz automata szkriptek használnák vagy terhelnék le**. Meg ugye a xvbuads533461@ kezdetű **címekről sem akarunk spam és kártevőhegyeket kapni**.

Human vagy robot, ez itt a kérdés, akkor nemesb-e a Captcha, ha tűri...

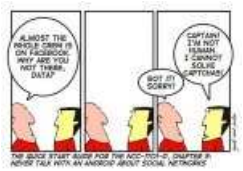
Azon kevés alkalmak egyike, amikor a Delirium Tremens hasznos is lehet

Egyszer már írtunk a 3D ábrákról is, most pedig ábrák minta szerinti elforgatását kell elvégezni egérrel. Ez a megoldás is érdekes és látványos, azonban nem szabad elfeledkezni arról, hogy például próbálgatással is megérheti megfejteni a delikvensnek, mert az ugyebár ingyen van, ideje meg van temérdek.

A Google tervezete szerint a pacalpörköltös tányér alfaszögben történő elforgatása hozza majd meg a kívánt eredményt ;-)



Bűvös kocka után bűvös Captcha



A megfelelően forgatott ábráknak **lehet még egy érdekes biztonsági momentuma**: nem lenne szerencsés, ha azokat is (például 10-20-100-360 féle?!) felindexelné a Google, mert akkor máris elkezdenék gyártani hozzá a reCaptcha programokat (amit enélkül és így is;-). Mindenesetre **ez a forgatásos módi is egy biztató ötlet**, meglátjuk, hogyan válik be a gyakorlatban, ne mondják majd rá, hogy "nincsen rajta Captcha" :-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1077997

Kommentek:

Nincsenek hozzászólások.

Felnyomott Feliratok.hu * Frissítve

2009.04.23. 11:25 | Csizmazia István [Rambo] | 22 komment

Címkék: kína feliratok kártevő iframe exploit roxy átirányítás

Korábban is említettük, hogy szinte bármilyen weboldalt meg lehet fertőzni, de ha valaki célzottan szeretne nagy kárt okozni, keresve sem találhatna jobbat a feliratok.hu lapnál **egy kártékony IFRAME exploit beágyazására: főleg fiatalok látogatják, akik közül sokan még nem annyira veszik komolyan a számítógépes biztonságot**.

Tavaly ősszel már volt hasonló IFRAME-s mizéria **a Roxy rádió honlapján, ahol szintén kártevő terjesztésre használtak fel egy beágyazott IFRAME blokkot**. Mivel még mindig sokan Internet Explorereznek, használnak hmm-kmm kétes eredetű Windowst (amit ugye nem frissítenek), és sokan még mindig egyáltalán nem használnak biztonsági programokat sem (há' a windows tűzfala mié' nem teljesen jó?), és persze noch dazu a Roxy is főleg a kevésbbé paranoiás fiatalok érdeklődésére tarthat számot. **Feltételezhetjük, hogy nem csak a topicnyitó faragott rá** (mi egyébiránt nem használunk ilyen közönséges, vulgáris és alpári szalonképtelen szakkifejezéseket mint "megszívta", és hasonlók ;-). Az is egy érdekes közjáték, hogy a HUP Drupalos topikjába akkoriban ohne zsineg be lehetett szúrni egy ilyen még aktív kártevőre mutató Iframes sort, szűrés vagy formai átalakítás nélkül. (Inputellenőrzés, inputellenőrzés, inputellenőrzés - mondotta Lenin ;-)

További apró érdekesség még, hogy miután a napokban megújult a www.roxy.hu, az új weboldalra (www.roxy.hu/website) történő átirányítást **eleinte még egy IFRAME tag végezte**, de szerencsére vagy rájöttek maguktól, hogy ez nem túl praktikus, vagy elegen figyelmeztették őket rá; esetleg tanultak a múltból és saját károkon - lényeg a lényeg, ma már ezt az átirányítást látjuk:

```
<html> <head> <title></title> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-2"> <meta
http-equiv="refresh" content="0;url=http://www.roxy.hu/website"> </head> <body> </body> </html>
```

Ennyit a múltról, **következzen a határtalan jelen, amikor is a feliratok.hu oldalról induló mirrorok kerültek sorra távoli testvéreinknél**, ami miatt az innen nyíló lapok HTML kódjában ilyesmit láthatunk:

Nem látszik túl bizalomgerjesztőnek, **még ha kajában esetleg szeretjük is a kínait, a titkon beágyazott Iframe-ben bizton utáljuk**. Ha olyan Windows alatti gépről nézegetjük, amin **az ESET Smart Security 4.0 fut, szerencsére az ilyen szokatlan beágyazásra** üzemszerűen jelent:

Továbbá ha rendes ;-) webböngészőt használunk, több forrásból is **kaphatunk figyelmeztetést**, íme az egyik.

A bűnös weboldal egy kínában Legjobb Rajmund által bejegyzett, de Litván szerveren működtetett valami. Talán lassúak voltunk - éjjel háromkor jött a riasztás, és reggel hétkor már rajta voltunk az ügyön - de ma reggelre letölthető kártevőt már (sajnos - hál' Istennek, a nem kívánt törlendő) nem sikerült fognunk ;-) Persze azért látható, **minden az eredetileg beszúrt litecartop.cn oldal továbbirányításán múlik**, ami időről időre változóan máshova irányíthat, esetleg figyelheti és naplózhatja az IP-ket, és mindig máshova küldhet, stb.

A tanulság talán annyi lehet, hogy egyrészt az "óvatosság nem bizalmatlanság", valamint az **"én itten kérem csak megbízható webhelyeket látogatok, ezért nem is eshet semmi bajom tisztelt Bíróság, zblorghhh"** szlogen újfent eredményesen cáfolva, Myth Busted!

*** * * FRISSÍTÉS * * ***

Közben Windowsos kollégánk sikeresen blokkolt NOD32-vel egy LOAD.EXE nevű vadállatot, amelyet a karanténból előbányászva az alábbi képet mutatja a VirusTotalon:

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1081465

Kommentek:

raly 2009.04.23. 13:18:16

nekem még most, csüt. délután is beriaszt a Nod feliratok subs és a felirat.it.cx/ linkekre kattintva. Eleve sajnálatos, hogy ez a top-top szolgáltatás ilyen szürkezónás módon üzemel. Állami támogatást a feliratok.hu -nak!!!

Gugli666 2009.04.23. 13:21:22

Itt mar elkezdték kitárgyalni a problémát:
sgforum.hu/listazas.php3?azonosito=SuperSubtitles&id=1009631225

raly 2009.04.23. 13:24:25

@Gugli666: valóban, és ahogy mondják, a mirror.donsystem.hu/ működik, csak csúnya

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.23. 13:24:39

Érdekes, hogy már tegnap este óta jelzik az ottani juzerek, és nem történik semmi :-O
sgforum.hu/listazas.php3?azonosito=SuperSubtitles&id=1009631225

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.23. 13:25:41

Hehe, Gugli666 Overdosi orrhosszal előbb találta meg :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.23. 13:31:44

Szia Raly :-)

Van alapja amit mondasz, a sok önkéntes ingyenes munkáját meg egyesek durván lenyúlják:
index.hu/kultur/2009/03/30/ismeros_sorok/

Egyébként és is néztem pár részt a 24 órából, és annyira megtetszett, hogy később megvettem. Az volt aztán a nagy megdöbbenés, amikor a boltból hivatlosan vásárolt feliratnál J és LY tévesztések tömkelege röfög kifelé :-O Lehet találgatni, hogy ezt is honnan lopták ;-)

nanehogymá 2009.04.23. 14:16:45

Antivir detektálja? Nem merem megnyitni! :)

nanehogymá 2009.04.23. 14:25:57

ja, most nézem, ez hülye kérdés volt, hiszen ez a weboldal a NOD32-t tolja reklámban

Vargnatt 2009.04.23. 14:41:26

Azért félelmetes, hogy azt a kártevőt 40-ből csak 4 program ismeri fel... Nem is tudtam, hogy a Microsoft védelmi programja ilyen jó (a Virus Totalon ez most melyik programjuk amúgy, a Malicious Software Removal Tool, vagy a Windows Defender, esetleg valami más?)

grizzancs 2009.04.23. 15:49:38

naes magatol feltelepiti a virust a bongeszo, mi ? hol elunk, 98ban?

edző bá 2009.04.23. 15:54:21

hellaz

friss avast is jelzi

btw. a cucc úgy terjed (sajnos ügyfelünknél is előfordult), hogy nem közvetlenül a weboldalt törik fel, hanem előzőleg egy kliens gép fertőződik meg egy spyware-rel, majd ha a fertőzött gépről ftp-n keresztül belépnek szerverekre, akkor az ott található php, html, stb állományokba véletlenszerűen beíródik ez az iframe.

a domain sok esetben más (pl. lotmachines.cn, stb), illetve nem csak a fájl végére appendálja, hanem például a body tag mögé közvetlenül.

na, csak gondoltam érdekes lehet. üdv.

Kixx 2009.04.23. 17:08:33

Mondanám, hogy a beágyazott javascript-be és a .js-ekbe is beírja magát.

Elég brutál...

dark future · http://www.andocsek.hu 2009.04.23. 18:11:59

@edző bá:

Ja. A Total Commander kódolatlan (ill. csak gyengén kódolt) ftp-jelszavait lopják le, tehát még csak be sem kell ftp-zni sehová. Az új (7.5) TC-ben már normális titkosítással lesznek letéve a jelszavak.

MILCSI 2009.04.23. 18:23:05

Nem kattintottam semmire,csak a képeket nézegettem,mint gyerekkoromban a meséskönyvben,mert egy huncut szót sem értettem a félig-meddig szakmai szövegből...de a humorod továbbra is magával ragadó :-)))
Az analfabétaságom védelmében elmondom,hogy véletlen sem szoktam ilyen helyeken kóborolni...

gabest1 2009.04.23. 18:50:59

mi kell nézni? van rajta egy pdf és egy swf, meg valamit installálni akar, jó lenne több konkrétum, a user és a víruskeresője közti interakción kívül másról nem szól a czikk, pedig az ördög a részletekben...

lifelike 2009.04.23. 19:02:28

a felirat.hu egy bena oldal
10 eve is ciki volt mar az egesz ahogy kinez meg ahogy mukodik
most se jobb

P. A. 2009.04.23. 19:38:50

Csak a mirror.donsystem.hu/old/ mirror fertőzött, a többi mirrorral nincs semmi baj. Használjátok /old végződés nélkül, vagy ha nem tetszik a design, itt egy másik mirror: supersub.freesitespace.net

Pszt! 2009.04.23. 20:08:08

Az Avast kiszúrta nekem is tegnap, figyelmeztetett, és leállította a kártékony kód letöltését.

@lifelike: Nem is arról volt szó, hanem a feliratok.hu -ról. Egyébként ott nem a kinézet a lényeg, a működésével nem tudom mi a bajod.

undertow 2009.04.23. 22:33:04

@Kixx:
index.*
main.*
default.*
ezeket szereti. tudom, két hete én is pucoltam az egyik adminisztrált domainről :)
ez egyébként a szelídebb verzió, van javascriptes obfuscated testvére is. azt egy fokkal nehezebb automatizálva kipucolni...

dojle · http://blog.webpozitiv.hu 2009.04.24. 12:35:18

amúgy itt van egy teljes leírás a hogyanokról, megelőzésről és javításról:
blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.26. 21:41:20

@Edző bá:
Köszi szépen a részleteket.

@Dojle:
Wow, klassz, korrekt és alapos munka, köszönöm. (y)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.15. 09:51:00

Van még itt egy olyan mellékkörülmény, hogy csak a 7.5 Total Commanderben oldották meg azt, hogy az FTP kapcsolatok jelszavait kódolva tárolja. Emiatt a korábbi változatok támadhatóak voltak, érdemes tehát egyrészt a 7.5 betara frissíteni, és a használt FTP jelszavakat pedig hirtelen felindulásból jól lecserélni.

Szoftveres csalás a köbön

2009.04.24. 11:25 | Csizmazia István [Rambo] | 5 komment

Címkék: szoftver csalás hamis visszaélés nod32 antivírus

Ha valaki a hírkeresőt rendszeresen olvassa, a Győzikével és más "celebekkel" kapcsolatos hírek elején sokszor láthatja a "borzalom", "meghökkentő", "szörnyűség" és ehhez hasonlatos kifejezésket a hivatkozott linkek címében. Lehet, hogy ezúttal nekünk is élni kellett volna ezzel, mert egyesek elég **durva támadást indítottak az egyszerű felhasználók ellen, amely nem csak vírusvédelmi szempontból lehet nagyon veszélyes, de pénzügyi zsarolás és a tisztességes fejlesztő cégek jó hírnevének lejáratára is**, amit semmiképpen nem szabad eltűrni.

Eljött a hamisítók aranykora. Ezúttal egy olyan átverésbe futottunk bele, hogy Juszt "Ne hagyják magukat átverni, megkárosítani..." László csak jelenthet nekünk ;-) Korábban már írtunk olyan letöltési oldalakról, ahol a weboldal gazdái nem törődöm viselkedése miatt családra programok kerülhettek letöltésre, sőt még kitüntető plecsniket is szerezhettek vagy ezek képét tüntették fel hamisan. Nem tudni, hogy a letöltő oldal gazdái esetleg brit uralkodói testőrnek képzelték-e magukat, **mindenesetre nem végezték az elvárható gondossággal a saját valódi feladatukat**, az biztos. De itt még talán inkább véletlen hanyagságról, sem mint tudatos rosszindulatról lehetett szó.

Sajnos azonban úgy tűnik, a korábbi hamis AVG weboldal csak a jégyhegy csúcsa volt, vagy egy koncepció főpróbája. **Elindult egy masszív szoftver csalási hullám, benne ezúttal a 2009-edition.com weboldallal**, de sajnos biztosra vehetjük, hogy más domain neveken és helyeken is fogunk még e jelenségel találkozni a hamis antivírus biznisz folytatásaként.

A csalók weblapjukat letöltési oldalnak álcázzák, és neves gyártók friss (vagy általuk frissnek gondolt) verzióit ajánlják letöltésre. Itt aztán bekérik az adatainkat - ami némely ingyenes letöltésnél érthetetlen is. A tovább gomb viszont **minden esetben kizárólag fizetős, bankkártya megadós lehetőségre visz tovább**. Próbaképpen megnéztük a crossplatform és ingyenes 1.26 változatnál járó Audacity programot: hát nem odahazudnak egy nem létező 2009 Editiont? Sőt számos programnak ezenfelül külön kamu weboldalt is készítettek.

Parasztvakítás ezerrel. Jön a köd, a füst, mint az Omega koncerten, szerencsétlen felhasználó pedig át lesz verve

És **megpróbálnak az ingyenes, mások által írt programért pénzt szedni a teljesen kezdőktől, akikkel még az ingyenes Mozilla Firefoxot is van képük pénzért letöltetni.** Ha ezt a csalást nagy léptékben elkezdik majd a botnetek teríteni (ez új, ma még nincs tömeges, ezzel kapcsolatos How to Remove találat a Google alatt "2009 Edition" kulcsszóra), sokan lesznek az áldozatok között.

Sajnos a többi programnál is hasonló a helyzet, tapasztalatlan felhasználók még esetleg örülnek is egy ilyen "jól összeszedett" csokornak. **Végiglépkedtünk a NOD32 4.0 szintén nem létező "2009 Edition" fantázianevű letöltési képernyőin**, és a szomorú képek után úgy tűnik, itt majd az ügyvédeknek is lesz mit focizni a témában. Nem tudni, a többi cég (Google, Avast, Panda, Foxit, Microsoft, Apple) mit tesznek majd, de **ezúttal van mire reagálni** a bűnözők ipari méretűvé duzzadt támadásán.

Az úttörő ahol tud, segít...adatot szolgáltat

No Spyware, No Adware, No Viruses - No persze :-)

A bankkártya ellenőrzési funkció viszont tökéletesen működik

Sajnos valóban nem lehet minden program mellé egy közlekedési rendőrt állítani, de **tanulságként jegyezzük meg**, hogy sose hagyatkozzunk ellenőrizetlen letöltési helyekre, kizárólag a gyártó weboldaláról töltsük a használni kívánt megbízható szoftvert. Azt már nem is merem tanácsolni, hogy telepítés előtt végezzünk lenyomat (MD5, SHA-1, SHA-512, stb) ellenőrzést is, pedig ha így haladnak a dolgok, előbb-utóbb ez lesz egyedül az üdvözítő megoldás :-O

Mindenesetre a **kezdő felhasználók valódi segítése, okítása a szűkebb környezetben még jobban üdvös lenne** a sajnos néha előforduló RTFM, a Google a te barátod és hasonló taplóságok helyett. Mindenki volt újonc, senki nem ért rögtön mindenhez, és **a ráfordított türelmes magyarázó segítséget remélhetőleg talán ő is továbbadja majd egy későbbi emberkének**, ahogy a Mennyei próféciákban azt írják. Dum spiro spero!

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1083334

Kommentek:

A nép fia 2009.04.24. 15:20:59

Egyszer én is majdnem belefutottam egy ilyenbe, de ahogy írod is, pöppet gyanús lett, hogy egy ingyenes program letöltéséért már kéri is el a bankszámla számomat...

ReWriter · http://miazhogy.blog.hu 2009.04.24. 16:01:31

De miért korlátozódnak csak az ingyenes szoftverekre? Árulhatnának feltört fizetős progikat is.

// Gery Greyhound · http://gerygreyhound.tumblr.com 2009.04.28. 18:20:25

Ez a szöveg a legviccesebb:

"get access to free step-by-step tutorials with over 200$ of free software"

Tehát még ki is írják, hogy 200 dollár értékű _ingyenes_ szoftver... És ezt így hogy? :))

Mondjuk aki az IE7-et pénzért letölti, annak nem csak megterhelném 100 dollárral a kártyáját, de mgé a világ összes létező trójaiját is rásóznám. Ingyenes bónusz ajándékként.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.15. 15:39:23

Ha már csalás, ez is ötletes:
itcafe.hu/hir/amazon_itunes_csalas.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.08.03. 09:42:29

Amíg erre van palimadár, sosem ér véget az ilyesmi :-D
www.hirextra.hu/2009/08/03/elkepeszto-csalas/

Cipőt a cipőboltból, Tamiflut pedig honnan is?

2009.04.27. 20:20 | Csizmazia István [Rambo] | 7 komment

Címkék: spam kanadai csalás sertés influenza kártevő kéretlen gyógyszerész

Karácsonyra fenyőfás virtuális képeslap, Valentin napra szerelmes üdvözlet, **minden ünnep és esemény megkapja a maga támogatását a spammerektől, a kártevő terjesztőktől**. Ez nagyjából annyira evidens, mint a korabeli **cipőt a cipőboltból** reklám. A Mexikóból indult sertésinfluenza nyomában **a kártevőterjesztők és nyerészkedők seregei is megkezdték az akcióikat.**

A hamis Viagra és Cialis világhódítása után megjelentek az első spamek és hirdetések, amelyek olcsón kínált "megbízható" Tamiflu gyógyszert, illetve egyéb a védekezéshez ajánlott kiegészítőket ajánlanak. Hogy magának **a járványnak mi az oka, azt nem tudhatjuk**, talán az összeesküvéselméletek szakértői kiderítik, hogy esetleg a politikusok a tudósok segítségével szándékosan így akarják-e megtizedelni a túlnépesedett lakosságot - majd kiderül.

Mi is "szerencsésen" megkaptuk az első ezirányú kéretlen küldeményt, íme az első maszkok a védekezéshez. Amíg a tudósok kitalálják az ellenszert, addig mindenki dolgozzon a túlélésért. Mindenesetre **nem csak a spammerek, de a hamisítók is aranykorra ébrednek**, amikor már Kína izraeli narancsot hamisít, bármi megtörténhet ;-) Bár várhatóan meg fog emelkedni a hamisított gyógyszerek kampánya a postafiókunkban, korábban összefoglalt tanácsaink fényében **továbbra sem ajánlatos innen rendelni ezeket**.

Jelentem, én még egyelőre jól vagyok, Röf-röf, hapciiiii! ;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1089691

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.29. 09:51:44

A válságon, mások kiszolgáltatott vagy helyzetén nyerészkedőket senki nem kedveli túlzottan, de van amikor nem ilyen élesen jön elő ez, Örkény Egyperces novellákból jutott eszembe ez, ami jelezte a háború végének másnapján, visszazökkent az élet a régi kerékvágásba:

"De már másnap, az Operával épp átellenben, egy romház kövein megjelent egy cédula:
'Hozott szalonnával egérirtást vállal doktor Varsányiné.'"

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.29. 09:53:00

Anélkül, hogy magát a veszélyt elkomolytalankodnánk, itt egy naprakész összefoglaló oldal a veszélyekről, a friss hírekről:
sertes-influenza.info/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.29. 14:23:52

A nemzetközi helyzet fokozódik:
biztonsagportal.hu/spamekben-is-terjed-sertesinfluenza.html

MILCSI 2009.04.30. 19:22:05

Ez szerintem csak a Föld szokásos népességszabályozó próbálkozása...kétesélyes: vagy sikeresen szétterjed a sok utazás miatt vagy megfékezhető...az előbbi csúnya lenne,de logikusan gondolkodva "jobban járna" vele az emberiség...egyszer olvastam egy cikket a túlnépesedésről,aminek az volt a lényege,hogy ha nem élne ember a veszélyes helyeken (földrengéses övezetek,árterek,vulkánok környéke,ivóvízhiányos területek,viharzónák) és csak úgy termelne mindent (élelmet,energiahordozókat), hogy ne sziplyozza ki a természetet, akkor a mai emberiség ezredrésze férne el kényelmesen a bolygón...ez talán túlzó becslés,de egy feleződés nem ártana az éleminőségnek...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.30. 20:03:47

Könnyen elképzelhető, én is gyanítok ilyen magasabb rendű Földi próbálkozásokat. Sajnos kevesen élnek környezettudatosan, szerintem még a rendszeres kézmosás is sokaknak emeltszintű feladat ;-)

Azt tudtad, hogy általában a születendő fiúk-lányok aránya 53-47% szokott lenni, mert sokáig a fiúknál a csecsemőhalandóság magasabb volt, mint a lányoknál. Ez az arány egyszer borult fel úgy, hogy a tudósok, orvosok sem értették az okát: 1945-ben a háború után 75% fiú született, akkor és csak akkor. Mintha érezte volna, hogy pótolni kell valamit a háború áldozatai közül.

MILCSI 2009.04.30. 21:15:13

A kézmosásról a Hofi jutott eszembe: vidéki "palota",benne csicsa fürdőszoba és a mosdó szépen leterítve csipketerítővel :-)))
Ezt a nem-arány felborulást tudtam,mert biológus vagyok...és az ilyesmikről mindig azAlapítvány sorozat ugrik be: Gaia...ha nem is annyira tudatos a dolog,de valami van benne...legalábbis remélem :-)
Az emberiség fő baja,hogy sebezhetetlennek és mindenhatónak képzeli magát (néha én is :-PPP) és ahogy kicsiben,úgy nagyban is azt hiszi,neki minden JÁR...

MILCSI 2009.05.09. 11:34:50

Ezt pedig most találtam...

www.stop.hu/articles/article.php?id=489701

Tálcán kínált adatok

2009.04.29. 17:59 | Csizmazia István [Rambo] | 4 komment

Címkék: biztonság facebook adatok twitter közösségi munkahely sophos

Egy friss felmérés szerint **a munkavállálók túlságosan sok személyes adatot**, információt adnak meg magukról **a közösségi portálokon**.

A mindenhol kiemelt kulcspozíciónak számító rendszergazdák szerint a munkavállalók több mint fele (egészen pontosan 62.8 százalékuk) ad meg magáról túlságosan részletes személyes információt, amellyel közvetve **már a munkaadók érdekeit is veszélyeztetik**. Az adminisztrátorok szerint a munkaidőben végzett közösségi oldalakon történő tevékenység kevésbbé szolgálja a munka hatékonyságát, és erőteljesen veszélyeztetheti a cég biztonságát.

Egy jottányit sem lehet csodálkozni ezen az álláspontón, hiszen egyrészt sok igazság is van benne, másrészt **a rendszergazda szempontjából ez a leglogikusabb válasz**. Számos támadás előkészítése alapul a közösségi webhelyen a nagy nyilvánossággal felelőtlenül megosztott információn, és ezt a támadók előszeretettel ki is használják. Mind az adatszivárgások, mind a spam- és malware **támadások egyre inkább begyűrűznek a Facebook, MySpace, Twitter, LinkedLine oldalakra is**.

Bevett trükk például, hogy a valódi kiszemelt áldozat innen kinézett online barátja számára küldenek előbb egy olyan kártevőt, amellyel annak jelszó adatát eltulajdoníthatják. A **Sophos által megkérdezettek 21 százaléka már kapott a közösségi oldalról adathalász levelet vagy kártevőre mutató üzenetet**.

Hogy egy munkahelyen **hol a megfelelő kompromisszum** a totális tiltás, és az ésszerű használat között, azt nem tudjuk. Azt azonban mindenképpen érdemes szem előtt tartani, hogy ha valaki a munkahelyén is belép, a vállalati **proxyban természetesen otthagyja a nevét-jelszavát**. És persze néha az otthoni használatnak is lehetnek a munkahelyen jelentkező veszélyei.

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1093572

Kommentek:

Flashzee · http://www.flashzene.com 2009.04.29. 20:09:13

De gáz ez! Mindenki csak óvatosan!

janikahhh (törölt) 2009.04.29. 21:05:43

EZ az egész "közösségi portál" mánia a hatalom kézbentartásának eszköze. Gondoljatok bele: Jóskapista ÁVH ügynök regisztrál, utána szabadon nézegetheti, hogy ki kivel mit és hogyan... a sok lúzer meg még a vércsoportját is feltölti, ha rákérdeznek...

MILCSI 2009.04.30. 21:21:25

Nincs baj a közösségi oldalakkal,csak ésszel-mértékkel kell használni...ha nem írod ki az adatlapodra,hányas zoknit hordasz,akkor nincs baj...de alapvetően itt is egy közösségi oldalon vagyunk,nem? Iwiw,Face,Inda,egykutya...ha valaki rosszindulatúan közelít és a kedves felhasználó bamba,akkor itt is megtalál...aki hülye,az meg az is marad,mint tudjuk :-)))

elinor 2009.06.26. 00:57:53

Szerintetek mit ne adjon meg az ember egy közösségi oldalon? Lakcím, telefon, e-mail ugye ezeket alapból nem, de az, hogy mikor születtem, milyen nyelveken tudok, az fönt van a szakmai adatbázisokban is, akkor minek titkoljam el itt?

Tudjuk hol jártál, kit hívtál, mit írtál

2009.04.30. 18:53 | Csizmazia István [Rambo] | 12 komment

Címkék: mobil telefon gsm kémprogram

Ezer szónál többet ér egy kép - szokták mondani, és még ennél is beszédesebb lehet egy jó kis videó demonstráció. **Ha féltékeny partnerünk vagy korábban zord munkaadónk** váratlanul kedvesen ajándékmobillal kínál, jusson eszünkbe ez a riport.

A KSL.TV megirígyelte a BBC Click! botneteket bemutató adását, és ők is kísérletezésbe fogtak. Belecsaptak hát a lecsóba és egy alkalmazottnak **egy kémprogrammal ellátott mobil telefont adtak pár napra**, de természetesen előtte tájékoztatták mindenről.

A filmen jól látható, hogy nem csak az összes beszélgetés, SMS, MMS ellenőrizhető így a kémkedő által, **de a banki egyenleg, az e-mailek és a bejárt útvonal fizikai koordinátái - akár Google Maps támogatással - is nyitott könyv lesznek**.

Korábban már mi is riogattunk ilyesmivel, de az kissé olyan Kandós laborgyakorlatra emlékeztetett inkább, ezért **most jobban értékeltünk ezt az életszagúbb változatot :-)** Ha esetleg régebben még szélesen vigyorogva megmosolyogtuk a telefonra készített antivírus és kémprogramirtó alkalmazásokat, **lassan ideje lesz hozzászokni ehhez a gondolathoz**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1096095

Kommentek:

dark future · http://www.andocsek.hu 2009.04.30. 22:07:09

Ebben sszerintem igazából csak egy nagy okosság van: miként tud úgy kommunikálni a telefonom, hogy ne vegyem azt észre. A többi már részletkérdés. A Google Maps meg egyenesen parasztvakítás.

longlife · http://testepitescsakitt.blog.hu 2009.04.30. 22:33:53

nem rossz...

atleta.hu · http://www.atleta.hu 2009.05.01. 03:31:08

Nagyon szeretnetek antivirus szoftvert eladni minden mobil tulajnak (ugy ertem altalaban ti, virusszagertok), hiszen olyan sokan vannak, de ennek tovabbra sincs semmi koze a virusokhoz meg a frgekhez sem. Majd akkor szolj, ha ilyet latsz. Addig csak annyi a nagy eszrevetel, hogy
1., az okostelefonok valojaban halozati kapcsolattal felszerelt szamitogepek (v.o.: "a telefon telefonalasra valo" :))
2., egy szamitogepre szoftvereket lehet telepiteni. (Folyomanya, ha nem figyelek ra, akkor mas akar olyan szoftvert is telepithet ra, ami nekem nem jo es nem is tudok rola)

Namost a feltekeny szeretot eloszor is ki kell rugni, de ha mar mobilt ad a kezedve, akkor koszond megszepen, majd frissitsd rajta a szoftvert ("flasheld ujra"). Nyilvan ne hagyd a telefont mas kezebe keveredni es ne elj egyutt olyan emberekkel, akiknel tartani kell attol, hogy bepoloskaznak.

Ez ellen a viruskergeto meg a spyware ellenorzo sem fog megvedeni, mert azt nem fogod minden alkalommal ujratelepiteni. Marpedig ha nem teszed meg, akkor nem bizhatsz benne, hogy az meg azt csinalja, amit te gondolsz. Vegulis az egeszbol csak egy ikont latsz...

Ha mar parazgatni akarunk, akkor elmondom, hogy a hivaslistat es az SMS-eket siman ki lehet olvasni a legtobb telefonbol telepitett alkalmazasok nelkul is, bluetooth kapcsolaton keresztul. Marpedig ez boven eleg egy feltekeny partnernek vagy eszetlen szulonek. Egyszeruen csak ossze kell parositani a ket keszuleket, es utana ha a kozelben vagy, akkor le lehet huzni rola ezeket az informaciokat. Vannak is ilyen szoftverek a piacon, es ez ellen a viruskergeto sem ved.

szalmaegér 2009.05.01. 07:09:14

Ami ebből az egészből tényleg érdekes, hogy 2006 végén ezt is magyar cég fejlesztette ki elsőként, az ő licenszelt termékeiket lehet itt ott megvásárolni a nagyvilágban.

Ma már Mo.-n is kapható, bár nem olcsó mulatság. www.octospy.com
Viszont működik.

Ma ez a cég többféle változatát kínálja ennek a terméknek, sok egyéb alkalmazási móddal.
Ami viszont nagyon fontos, hogy előtte tanulmányozzátok az adatvédelmi szabályzatot, mert ezt a szoftvert használni csak úgy szabad, hogy tud róla a teló tulaja is.
Én a gyerek miatt vettem, bár bevallom, ő nem tudta:)
Rossz érzésem volt, úgy gondoltam, nem a legjobb társaságban van. Pár napon belül kiderült, hogy túlreagáltam a dolgot. NA mindegy, a szoftver marad a telóján. Biztos, ami biztos...

BKV reszelő · http://praxisfree.blog.hu 2009.05.01. 08:59:38

@szalmaegér: Ha az énapám vagy anyám lennél, pofánbasználak ennél a résznél, az biztos.

lifelike 2009.05.01. 09:11:54

@BKV reszelő: boldog csaladban elsz te is, az latszik...

szalmaegér 2009.05.01. 09:34:33

@BKV reszelő:
Vállalnám a pofánbaszást, ha ez lenne az ára, hogy a gyerekem nem kerül börtönbe azért, mert olyan gyökerek a haverjai, mint te.
Nem várom, hogy ezt te is megértsd, hiszen ahhoz ész is kellene, neked meg, ahogy elnézem, nem sok jutott.

blügy-blügy 2009.05.01. 09:52:57

iPhone-on már magam is néztem, hogy a google maps térképén merre autózok. Biztos el lehet küldeni ezeket a koordinátákat, ha valaki ért az okos telefonok programozásához

MILCSI 2009.05.03. 15:49:59

@atleta.hu: és miért lenne gond,ha valaki,aki antivírus szofverek eladásával foglalkozik,az azt szeretne eladni? De szerintem itt erről szó sincs...ez egy blog,ahol valaki,akinek az írások alapján ez a szakmája és úgy tűnik,a hobbija is, szeretne segíteni azoknak,akik ezt igénylik és értik...nem értem,miért kell mindig mindenből irigységi érdést csinálni...ha ez alapján a cikk alapján tízzel több vírusírtót adnak el,az neked nagyon fáj? ha pedig nem tetszik,amit itt olvashatsz,olvass mást...
Bocs mindenkitől az offért...

Aimie Cross 2009.05.05. 23:38:11

Sziasztok! Nagy gondban vagyok, most kaptam egy mp3at, új, ahogy csatlakoztattam az USBt az AVG riasztott h Trojan.Horse.PSW.Agent.YOM van rajta, ami annyit tesz h az mp3mal egyidejüleg megjeleik egy kamu cd meghajtó is (AMT_CDROM és ez van benne: AMT.sn , autorun.inf , start.exe - természetesen védett), ami autorun indul, a helyzet odáig fajult, hogy nem tudom a zenei számokat sem átküldeni az eszközre, mert ez az izé megfertőzte a start.exe-t az AVG semmit sem tud tenni.
Próbáltam egy erre készült Panda vakcinát, de nem állította le az autorunt- ahogy kellett volna.
Kérlek segítsetek

csodafenevad 2009.05.11. 08:20:12

@Aimie Cross:

fordulj nyugodtan az ESET magyarországi terméktámogató csapatához. Az elérhetőségünket megtalálod az eset.hu oldalon.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.11. 08:40:26

Szia Amie Cross!

Bocs, hogy csak most írok.

Amit én tennék:
- kikapcsolnám azonnal az Autorunt, itt találasz útmutatót.
www.us-cert.gov/cas/techalerts/TA09-020A.html

- futtatnék egy teljes keresést valami nem AVG programmal, ezt akár egy 30 napos NOD32 próbával is megteheted, letöltés innen:
www.eset.hu/letoltes/proba

- és lehetőség van telepítés nélküli online scanre is, például innen:
www.eset.hu/viruslabor/onlinescan

Ha ezek megvannak, szólj, hogy használt-e, hol tart éppen most a dolog. Sok sikert!

Felhívás keringőre

2009.05.06. 22:08 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hacktivity előadások 2009

Kedves kötelességemnek teszek eleget, mikor teret és helyet adok a következő Hacktivity felhívásnak. **Aki indíttást érez sérülékenységekkel kapcsolatosan előadást tartani**, az a jelentkezés részleteit elolvashatja lentebb.

HACKTIVITY 2009 - Pályázati felhívás előadás tartására
Időpont: 2009. szeptember 19 - 20. (szombat – vasárnap)
2009. szeptember 19. és 2009. szeptember 20. között kerül hatodik alkalommal megrendezésre a Hacktivity 2009 konferencia. A Hacktivity konferencia hagyományosan az információbiztonsági szakma hivatalos és alternatív képviselőit hozza össze a terület iránt érdeklődőkkel, kötetlen, de mégis ismeretterjesztő és néha mélyen technikai formában.
Amennyiben előadóként kíván részt venni a Hacktivity 2009 konferencián, úgy kérjük, szíveskedjék elküldeni tervezett előadásának pontos címét, valamint maximum 1000 karakterrel leírt tematikáját a cfp@hacktivity.hu címre, legkésőbb 2009. június 10-ig. A tematika összeállításánál kérjük, vegyék figyelembe, hogy egy-egy előadás időtartama 45 perc.

Miért érdemes előadni a konferencián:
- Ez Magyarország legrégebbi független IT biztonsági konferenciája, itt előadni rangot jelent
- Mert a sikeres előadók az elmúlt évek tapasztalatai alapján nem egy állásajánlatot kaptak
- Több CPE pont bizonyos minősítések esetében
- Itt a marketing „bull sh¬#@t” nem nyerő

A Hacktivity Programbizottsága a beérkezett tematikák alapján dönt az előadásoknak a konferencia programjába való felvételéről. Azok az előadók, akiknek az előadása bekerült a programba, jogosultak utazási költségtérítésre, Hacktivity 2009 előadói póló viselésére, valamint a konferencia szervezői egy éjszakára szállást biztosítanak számukra.
Kérjük, hogy **csak olyan előadás javaslatot szíveskedjék beküldeni, amelynek témája kapcsolódik a Hacktivity szellemiségéhez**, azaz az infokommunikációs technológiák sérülékenységeit mutatja be a támadó szemszögéből, és ezek kivédésének módozatait is bemutatja. Kérjük továbbá megadni, hogy előadása az alább felsoroltak közül melyik témakörhöz kapcsolódik. Amennyiben előadása nem kapcsolódik egyetlen témakörhöz sem, konzultálni lehet az Programbizottság **szakmai felelősével, Krasznay Csabával (cfp@hacktivity.hu)**.

A rendezvényre készítünk konferencia kiadványt. Az egyes előadások tematikáját nyomtatott formában adjuk közre. A kiadványokat a konferencia minden résztvevője a regisztrációnál veheti majd át. Az előadások prezentációit a konferencia után a rendezvény honlapjáról lehet elérni. **Célunk, hogy az előadások videóváltozata szintén elérhető legyen a honlapon.**

CISA, CISM és CISSP vizsgával rendelkező látogatóink és előadóink részére idén is CPE pontigazolásokat állítunk ki.

HATÁRIDŐK:
2009. június 30. - Előadás-javaslatok beküldése a tematikával, a cfp@hacktivity.hu címre
2009. július 30. - Az elfogadott előadók értesítése és a konferencia programjának publikálása.
2009. szeptember 10.- Nyomdakész prezentációk beküldési határideje, a cfp@hacktivity.hu címre

A Hacktivity 2009 Konferenciával kapcsolatos további információk a http://www.hacktivity.hu címen találhatók meg.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1107008

Kommentek:

Nincsenek hozzászólások.

Hacker ugyan, de nem bánt, mi az?

2009.05.08. 21:28 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: konferencia hacking ethcial

Profi szervezés, profi előadók és előadások, teltházas nézőtér - röviden így jellemezhetjük mindazt, ami tegnap az Aréna Plázában, pontosabban annak mozitermében lezajlott Ethical Hacking konferencia 2009.

Második alkalommal vehettünk részt az Ethical Hacking konferencia eseményen, és a színvonalat ha lehet, sikerült még tovább emelni, csiszolni a tavalyihoz képest, lehet, hogy ehhez a GDF hallgatók előtti korábbi főpróba is hozzájárult.

A szokásos helyszínen, a Cinema City Arénaban gyűltek össze a résztvevők, akiket **Fóti Marcell (NetAcademia) és Pap Péter (Kancellár)** köszöntöttek. A beígért érdekes előadások nem csupán szóvirágok maradtak, érzésre mindenki egy végletekig kimunkált, élvezetes prezentációkat vezetett elő. Péter elmondta még, **jó lenne egy olyan általános hozzáállás a cégek részéről is, hogy ne tartsák szégyellni valónak, ha egy pentestet végeznek el náluk**. Ez egyáltalán nem negatív, vagy titkolnivaló dolog és teljesen normális, ha erre és a feltárt hiányosságok befoltozására rendszeres erőfeszítéseket tesznek. **Keleti Arthúr (KFKI)** pedig mindenkit nagy szeretettel invitált meg a közelgő, **szintén itt rendezendő Informatikai Biztonság Napjára**.

Az első előadó **Tim Pierson (EC-Council, Network and Security Technology Expert)** volt, aki a penetration test szükségességéről és fontosságáról beszélt. Bemutatójában **egy virtuális gépbe való bejelentkezés is szerepelt** alulnézetből, és láthattuk, mennyire kinderspiel a bejelentkezési jelszó ellopása annak, aki tudja pontosan mit és hol keressen.

A következőkben **Deim "Ago" Ágoston (Linux Support Center)** lépett a pástra, és a tavalyi Ciscos trükkök után **ezúttal IDS megkerülési technikák szerepeltek a repertoárjában**. A bemutató lényege nagyjából úgy summázható, hogy az IDS vagy IPS nem egy olyan megoldás, amit az ember feltesz a gépére, elindítja, aztán "dolgozzanak a gépek" jegyében elfelejti és hátradől a székében. **Kizárólag annak érdemes ilyet használnia, akinek van elég szakismerete és ráfordítható ideje** az ezzel kapcsolatos adminisztrációkra.

Az ilyenkor szükséges PH értékek után **Mizsányi Attila (NetAcademia)** következett, és **bár valószínűleg mindenki hallott már publikus és privát kulcsokról**, vélhetően sikerült így is olyan részletekről és finomságokról fellebbenteni a fátylat, ami adott új információt. Az mindenesetre biztos, hogy a működésről szemléletes képet kaphattunk, és az RSA atyjairól is megtudthattunk egysmást.

Egymás mellett, de a különbözőségek kihangúlyozásával helyezte párhuzamba a fehér és fekete kalapos hackelés jellemzőit két KFKI szakember, **Gajdov Gábor és Imre Zsolt**. Szerezzünk admin jogot és "hulljon az ölünkbe" a konkurencia adatbázisa - foglalhatnánk össze a bemutatott törekvéseket. Nem csak a "jó pap holtig tanul" volt ebben fontos, hanem a szemléletbeli különbségek is jól nyomonkövethetők voltak. Tanulságként annyi vonható le, nem szabad, hogy egy pentest egyszerű gondolkodás nélküli "push the button, run the tools, get the money" folyamattá silányuljon, ebben inkább a támadóra kell hasonlítani, aki élvezi és totálisan érti, mit és miért tesz rendszerünkkel.

Ebéd után **Illés Márton (BalaBit)** a tűzfalak és a titkosítás összefüggéseiről rántotta le a leplet, és a bemutató végén mindenki elgondolkodhatott, hogy az eddig ördögtől valónak tartott **Man in the Middle módszer önmagában egyáltalán nem csak rossz célokra használható fel, hanem időnként jól és megbízhatóan szolgálhat bennünket**.

Akik voltak a tavalyi Hacktivityn, emlékezhetnek **Barta Csabára (PricewaterhouseCoopers)** és sajátfejlesztésű sérükénységfelderítő programjára. Ezúttal egy új, saját készítésű rootkittel "örvendeztetett" meg minket, és **kaphattunk egy kis ízelítőt a számítógépes szakértők nyomolvasói és nyomrögzítési technológiáiból** annak kapcsán, hogyan mentik el a memória tartalmát speciális segédeszközök segítségével.

Némi kávé infúzió után a tavalyi Social Engineering téma után egy szintén fontos és érdekes területet mutatott be **Novák Zsolt (Regulation Consulting)**: hogyan és mire kell figyelni egy munkaadónak, **ha minimalizálni szeretné az emberi kockázatokat a cégen belül**. Az élvezetes előadásban láthattuk, milyen kulcsfontosságú munkaköröket célszerű mindenképpen szétválasztani, továbbá milyen szempontoknak kell(ene) jelentős szerepet játszania a munkaerő felvételnél, illetve a munkavállaló távozásákor mire kell(ene) nagyon odafigyelni.

A záróelődásban végül, de semmiképpen nem utolsósorban **Borsi Katalin és Zsíros Péter (NetAcademia)** mutatták meg, hogy egy pongyolán megírt öt soros C programon is lehet fogást venni, ha valaki támadni szeretne, sőt ezek a lehetőségek egy kis buherálás után szinte nagyobb teret biztosítanak, mint azt eleinte az ember gondolná. Egy kis Metasploit frameworközés és Ollydebugolás után **tetszőleges kód futtatása vagy egy új admin jogú felhasználó létrehozása is eszközölhető, ha az ember tudja, mit és hogyan bűvészkedjen egy egyszerű string bevitel kapcsán**.

Összefoglalva: érdekes és élvezetes bemutatókat láthattunk, voltak benne vadonatúj dolgok, illetve ha valami ismert és régebbi téma volt ugyan, akkor is sikerült hozzáadni valami olyan pluszt, amiért mégis érdemes volt végiglépkedni a felvázolt gondolatmeneteken. **Reméljük, jövőre is hasonló jókat írhatunk majd a következő Ethical Hacking konferencia kapcsán.**

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Android kémprogram persze csak a mi érdekünkben
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1109319

Kommentek:

Nincsenek hozzászólások.

Felpörgetve

2009.05.09. 13:52 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: lada nod rally támogatás eset túraautó mentőmotoros

Találtunk néhány ESET NOD32-es matricával **közlekedő, száguldozó, rallyzó kétkerekű, vagy éppenséggel négykerekű járművet** és ezeket a képeket most közkinccsé tesszük.

Első állomásunk Brazília, ahogy **a helyi ESET képviselet az egyik támogatója az ottani autósport egyik kiemelkedő eseményének**. Az egyik Ferraris csapat pilótáját, Francisco "Chico" Serrat sponzorálják, meg külön weboldalt is készítették a témának. Képeinken a versenyző meze és **az általa vezetett túra autó bemutatója** látható.

Természetesen hazai berkekben is látni hasonlót, alábbi **képeinken egy rallys kocka Lada következik**.

Végül, de semmiképpen nem utolsósorban a Magyar Mentőmotoros Alapítvány háza táján járva látunk NOD32-es matricákat. Ennek az az oka, hogy **az M0 és M3-as utakon működő motoros mentőszolgálat** egyik főtámogatója a magyarországi Sicontact Kft. A jól felszerelt motorokkal az orvosok dugó esetén is **percek alatt a baleseti helyszínekre tudnak érni, és hatékonyan tudják ellátni** az elsősegéllyel kapcsolatos teendőket. Ha nagy a baj, akkor pedig riasztani tudják a helikopteres szolgálatot.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával

- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1095779

Kommentek:

Nincsenek hozzászólások.

Válságban is erősödnek a hamis antivírusok

2009.05.11. 17:45 | Csizmazia István [Rambo] | 2 komment

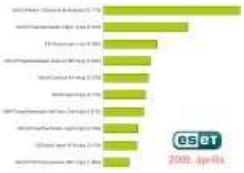
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET víruslaboratóriumának szakértői szerint **jobban kellene vigyázni az internetezés közben saját magunk által elfogadott és telepített alkalmazásokkal**. A válság miatt ugyan **folyamatosan erősödik a nyomás rajtunk**, de pontosan emiatt végre itt lenne az ideje a tudatosabban kezelni a védekezést is, magyarul még jobban kellene vigyázni a gépünkre, valamint a pénztárcánkra.

Magyarországon továbbra is a Virtumonde végzi a legnagyobb pusztítást. Az ingyenes .mp3 tartalmakat, különféle 2009-es fantázia nevű vírus- illetve kémprogram elleni keresők letöltését ígérő károkozót a gyanútlan felhasználók saját maguk telepítik számítógépükre. A Virtumonde elsősorban kéretlen reklámokat jelenít meg a megfertőzött gépeken, így böngészés, vagy az operációs rendszer **használata közben felugró üzenetekkel találkozunk**.

Emellett **a hamis antivírus programok – amelyből már több ezer féle létezik** – igyekeznek pénzt is kicsalni az áldozatoktól, 50 dollár körüli összegért teljes funkcionalitást ígérve. A csalók azonban csak a pénzre mennek, a gép az összeg átutalása után is fertőzött marad. **Újabban már „Antibotnet 2009" és ehhez hasonló becsapós neveken is felbukkan a kártevő**, meglovagolva ezzel a botnetes híradásokat. Érdekes momentum, hogy ezúttal **nem csak nálunk, hanem az Egyesült Királyságban, Izraelben, Németországban, Olaszországban illetve Svédországban valamint Szerbiában is ez a kórokozó végzett az első helyen áprilisban**.

Ennek a hónapnak talán az lehet a legnagyobb tanulsága, hogy egyrészt **elengedhetetlen részként kell a Windows alatti számítógépeknél az antivírus programra gondolni**, másrészt pedig ahogy az ember az autó-, televízió készülék, vagy más műszaki cikkeknél is alaposan utánanéz a minőségnek, a márkáknak, ugyanígy itt sem ajánlatos a neve nincs védelmi programok használatának. Ezzel ugyanis nem csak annyi a veszély, hogy esetleg nem vagy nem jól működik egy TV, nem zenél az MP3 lejátszó, hanem **gépünk megfertőzésével folyamatosan adatok szivároghatnak a bűnözők felé, tudtunk nélkül botnet hálózatba kényszeríthetik gépünket, illetve banki és jelszó adataink ellopásával komoly pénzügyi károkat szenvedhetünk el a jövőben is**. Válság idején (is) kötelező a megbízható antivírus program, saját érdekünkben **ne ezen sóroljunk!**



Végül következzen a magyarországi toplista. Az ESET statisztikai rendszere szerint 2009. áprilisában az alábbi 10 károkozó terjedt a legnagyobb számban. Ezek együttesen 40.25%-ot tudtak a teljes tortából kihasítani maguknak.

1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége az áprilisi fertőzések között: 10.17%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

2. Win32/Wigon trójai
Elterjedtsége az áprilisi fertőzések között: 6.30%

Működés: A Win32/Wigon trójai kártevő család a számítógépre jutva különböző fájlokat hoz létre a Windows\System32 alkönyvtárban, ezek egyike a WinCtrl32.dll. Ezek segítségével készít el további kártékony állományokat a helyi gép TEMP mappájában, és eközben a rendszerleíró adatbázisban is módosításokat végez. A bejegyzések segítségével eléri, hogy a fertőzött DLL állomány törlése utáni rendszerindításkor az ismét visszakerülhessen. Tevékenysége során elindít egy szervizfolyamatot is a fertőzött gép memóriájában.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/wigon-ck

3. INF/Autorun.gen vírus
Elterjedtsége az áprilisi fertőzések között: 4.00%

Működés: INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

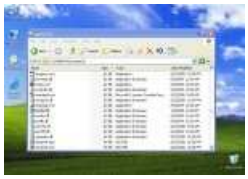
4. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége az áprilisi fertőzések között: 3.49%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat töltöget le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a „csomagban". Emellett hátsóajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-nbf

5. Win32/Conficker.AA féreg
Elterjedtsége az áprilisi fertőzések között: 3.32%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call) vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt
Bővebb információ: http://www.eset.hu/virus/conficker-aa

6. Win32/Agent trójai
Elterjedtsége az áprilisi fertőzések között: 3.11%

Működés: Ezzel a gyűjtőnévvel azokat rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: .a felhasználó maga telepíti
Bővebb információ: http://www.eset.hu/virus/agent

7. WMA/TrojanDownloader.GetCodec trójai
Elterjedtsége az áprilisi fertőzések között: 2.97%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

8. Win32/TrojanDownloader.Agent trójai
Elterjedtsége az áprilisi fertőzések között: 2.54%

Működés: A TrojanDownloader.Agent egyfajta gyűjtőneve az olyan kártevőknek, amelyek további kártékony kódok letöltésére specializálódott. A letöltött rosszindulatú szoftverek komponenseit azután igyekszik elindítani, illetve telepíteni is az adott számítógépen. Rengeteg variánsa létezik, ezek minimális eltéréssel (különböző fájlnév, különböző célmappa, különböző Registry bejegyzés) végzik ugyanazt a feladatot, és ezzel a technikával érik el a kártevő terjesztők, hogy egy már fertőzött gépen a rosszindulatú program is képes magát frissíteni. Elindítása után legtöbbször DLL állományokat hoz létre a Windows fő könyvtárában, vagy annak rendszermappájában, a letöltés közben pedig a TEMP mappában csomagolja ki, illetve készíti elő a gyanús fájlokat, amelyeket többnyire .CC végződésű, azaz Kókusz szigeteki doménekről próbál meg letölteni.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-agent

9. JS/Exploit.Agent.AFH trójai
Elterjedtsége az áprilisi fertőzések között: 2.47%

Működés: A JS/Exploit.Agent.AFH olyan weboldalak kódjába rejtett JavaScript program, amely védtelen számítógépek biztonsági hibáját használja ki, és amiatt képes letöltődni és lefutni. A kártevő terjedése érdekében a Microsoft ms99-042 jelű sérülékenységét használja ki. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Esetleges fertőzés és mentesítés után érdemes a webböngésző átmeneti tárolóját (Temporary Internet Files mappa) is kitörölni, valamint a szükséges Windows biztonsági javításokat haladéktalanul telepíteni.

A számítógépre kerülés módja: böngészés közben automatikusan letöltődik a hiányos védelmű felhasználó számítógépére
Bővebb információ: http://www.eset.hu/virus/js-exploit-agent-afh

10. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége az áprilisi fertőzések között: 1.88%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyű leütés naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására és a jelszó adatok titokban való továbbküldésére fókuszál. A távoli támadó ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthat hozzá, amelyet aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1109745

Kommentek:

MILCSI 2009.05.13. 17:43:59

Az 1-es és az általa telepített milliónyi dll fájl a haverom :-)) de én nyertem anno,igaz rendszer- és idegösszeomlás árán :-))
bekerülési mód: játékletöltés :-S

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.17. 12:36:20

Egy kis körkép a magyar viszonyokról:
itmania.hu/tart/cikk/e/0/47872/1/informatika/Sokan_veszitenek_el_adatokat_az_interneten_es_a_szamitogepen?place=srss

Ki nevet a végén?

2009.05.12. 19:37 | Csizmazia István [Rambo] | 1 komment

Címkék: budapest konferencia 2009 antivírus caro

Az idén **május 4. és 5. között Budapesten** gyűlt össze mintegy 110 profi szakember, hogy a vírusvédelem, **a kártevőkkel folytatott harc kapcsán megossza egymással gondolatait**, és valóban, az előadások között volt néhány különösen figyelemre méltó is. Mi most egy rövid képes összefoglalóval, egy-két gondolattal szeretnénk megemlékezni a Budapesten tartott CARO (Computer Antivirus Researchers Organization) 2009 konferenciáról.

Kicsit késve, de nem múló lelkesedéssel számolhatok be az eseményről.

Ami most a poszt íráskor kifejezetten vicces, hogy korábbi sajtóközlemények, és azt azt átvevő portálok szerint Jimmy Shah volt a hétfői nyitó nap első előadója.

Lévén, hogy én is ott voltam, és a saját szememnek jobban hiszek, mint a sajtó közleményeknek, továbbá beszélgettem is Jimmyvel, sőt névjegyet is váltottunk, nos nem ő volt a hétfői első előadó, hanem Righard J. Zwienenberg a Normantól. (Már jeleztem e-mailben a dolgot az illetékeseknek, ami után rövidesen kijavították a weboldalon.) Előadásában **az exploitok veszélyeiről beszélt**, ezek ugyanis egyre nagyobb szerepet játszanak a biztonsággal foglalkozó cégek életében.

Utána következett a román Marian Radu a Microsoft kutatóközpottól, és **a PDF állományokkal kapcsolatos sebezhetőségekről** volt szó, ami mondhatjuk, napjaink egyik slágere. Igen sok rés van az Adobe termékekben, és rengeteg olyan rosszindulatú weboldal van, ahol pont ilyen preparált PDF állományokat helyeznek el a gyanútlan látogatók megfertőzésére.

A McAfee szineiben Anthony Bettini következett, aki nulladik napi támadásokról tartott előadást. Többek közt arról is szó esett, hogy milyen összefüggések vannak a Patch Thuesday és a részvényárfolyamok mozgása között.

Pierre-Marc Bureau lépett a dobogóra az Esettől, és a híres-hírhedt MS08-067 sebezhetőségről beszélt a Conficker féreg kapcsán. Érdekes volt, látszott, ahogy egyre többet tettek a kártevő fejlesztői, és persze az is vicces volt, hogy **néhány résztvevő "I beat the Conficker" feliratú pólóban** mulatta az időt a nézőtéren :-)

Ebéd után aztán tényleg ;-) Jimmy Shah következett a McAfeetől, és a **mobil platformokra készült újabb kártevőkről mesélt**. Álláspontja szerint már azzal kémprogramok telepítését kockáztatja az ember, ha ismeretlen programokat lefuttatva jailbreakeli a iPhone telefonját.

A Microsofttól érkezett Bruce Dang és Cristian Craioveanu, akik **a generikus állományformátum felismerés** fontosságáról beszéltek a különböző népszerű exploitok kapcsán.

Ezután következett Cristoph Alme és Dennis Elser (McAfee). Ők a kártevő felismerésben **alkalmazott Markov modellről tartottak előadást, ahol is statisztikai módszerekkel vizsgálva az egyes utasítások gyakoriságát**, érdekes felismerésekre lehet jutni.

A Kaspersky cégtől érkezett Maksym Schipka, aki az **Office állomány típusok sérülékenységeiről beszélt**, és előadásában ugyancsak szóba kerültek statisztikai módszerek, az **entrópia alapú vizsgálatokkal szintén észlelhető, ha egy állomány nem az, aminek mondja magát**, illetve ha saját kódján kívül valamilyen kártékony futtatható kódot is magában hordoz.

A **felhő alapú védelmi megoldások kihasználható gyengeségeit ecsetelte a Symantec szakembere, Ször Péter**. Szerinte a felhő alapú szkennelés sebezhető, és néhány példával is igyekezett felhívni erre a figyelmet. Mint ismeretes, ő a szerzője a mai napig is unikumnak számító "Virus Research and Defense" című könyvnek, amely átfogó és részletes kézikönyve a vírusvédelemmel foglalkozó szakembereknek.

A második nap reggelén Andreas Marx kezdett az AV-Test.org-tól. **A kártevő ellenes programokba épített exploit megelőző technikákról** és azok teszteléséről hallhattunk néhány keresetlen szót.

Tőle ismét a McAfee, pontosabban Ivan Teblin vette át a staféta botot, és **a PE (portable Executable) állományformátum gyengeségeit, sajátosságait**, illetve a szabályos fejlécszerkezet ellenőrzésének nehézségeit járta körül alaposan.

Illés József a VirusBustertől érkezett, és az AutoIt végrehajtható, az NSIS telepítő állományokat, **valamint az SWF flash fájlokat elemezte egy új szemszögből**: bemutatta ezeket az antivírus alapprogram nézőpontjából.

Őt **Igor Muttik (McAfee) követte a Conficker féreg alapos elemzésével**, nagyon friss és érdekes téma volt.

Abhijit P. Kulkarni és Prakash D. Jagdale (Quick Heal Research and Development Center) úgy tűnik, igen sok ráérő szabadidővel rendelkezett, mert kikisérleteztek egy módszert, amivel **eredményesen kerülték meg az antivírus programok valósidejű védelmét 64**

bites rendszerek esetén.

iv Mador a Microsoft Malware Protection Centertől érkezett, és arról értekezett, hogyan lehetne még hatékonyabban beazonosítani a kártékony programok shellkódjait. Tulajdonképpen ezzel kapcsolatban keletkezett a poszt címe is, ahol a klasszikus viccben a rendőr rászól a feleségére, hogy ne dobja állandóan a szemetet az utcára. Az egyébként háztartásbeliként otthon lévő asszony azonban rendszeresen ezt teszi. Végül megfenyegeti, hogy feljelenti szemetelésért, amit végül meg is tesz. Csak ugye azt felejti el, hogy mikor megérkezik a büntetésről szóló sárga csekk, akkor azt mégiscsak neki, a keresőnek kell majd befizetnie, azaz ki kivel babrált ki? Nos kb. ez volt az érzésem itt is, szofisztikáljuk a detektálást, meg finomítjuk az eztazt, **mikor pedig az Office biztonsági frissítésekről van szó, azt ugye csak a legális juzerek tölthetik le. De hogy mindez mekkora kárt okoz, hány botnetes gép lehet a világban, és hogy ez számszerűsítve mekkora kárt okoz**, azt mintha nem is gondolnák végig. És mivel sok lopott példányt használót nem is érdekli ez az egész, valójában a bűnöző nevet a végén, aki csak szórja az Office exploitokat a weboldalakon, mint kecske a hegyoldalban :-(

A **sérülékenységekről gyűjtött adatairól beszélt a konferencia legszórakoztattóbb előadásában Roel Schouwenberg (Kaspersky)**, aki összefoglalta a lehetséges módszereket a rendszeres javítások elvégzéséhez, valamint rámutatott az elhanyagolt frissítések leggyakoribb okaira is.

Végül Nick FitzGerald (AVG Technologies) előadása következett, amelyben bemutatott néhány, **pár dollárért megvásárolható népszerű, bevetésre kész webes támadó készletet**, és azokkal szerzett tapasztalatait.

Összességében sűrű, de nagyon érdekes program volt, sok emberrel sikerül személyesen is beszélgetni - **köztük például Randy Abrams-szel is - sőt a végére még egy ereklyét is begyűjtöttem: egy dedikációt a Szőr Péter könyvembe :-)**

Ajánlott bejegyzések:

- Gyerek-barát netezés

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen

bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1109553

Kommentek:

MILCSI 2009.05.13. 17:36:20

Mindig tanul az ember lánya...sosem tudtam,mi az a Mcafee CD,amit a géphez adtak...ciki,de így jár aki analfaBéka és ráadásul macska :-)) nem tudom,más korombeli,akinek szakmailag semmi köze a számítástechnikához szintén ilyen bamba-e,de én legalább önkritikát gyakorlok időnként :-))

Akarod, nem akarod, megkapod

2009.05.13. 19:16 | Csizmazia István [Rambo] | 19 komment

Címkék: mobil spam a sms sün kéretlen szolgáltatótól

Nem emlékszem, hogy bármikor is feliratkoztam volna az "Igen, kérek tájékoztatást, a mit, hol, hogyan, miért és egyáltalán szolgáltatásra, az értesítéseket pedig az alábbi telefonszámon kérem szépen térden állva könyörgök, hogy SMS-ben küldjék ki nekem". A szomorú az, hogy még az sem kérdés, "Ki küldözgeti ezt nekem" **kéretlenül**.

Legközelebb meg majd olyanok jönnek, hogy "Cipőt a cipőboltból", vagy "mondja marha miért oly bús, olcsóbb a hal mint a hús", esetleg Skála Kópé bemegy, kijön, de milyen jól kijön, ha bemegy. **Honnan tudja a mobilszolgáltató, van-e autóm, vagy ha van is, érdekel-e, hogyan vegyek mobillal autópálya matricát**. És ha még érdekel is hogyan vegyek mobillal autópálya matricát, ott van a havi csekkes borítékjuk, benne a szokásos "legyél te is menő, tőcsd le..." logo és csengőhang letöltési reklámfüzettel ;-) - **akkor tegyék ezek közé egy szórólapon**, hogy "Ezt nem fogod elhinni, alig telt el 40 év, hogy ember a Holdon, és te máris mobillal vehetsz autópályamatricát, na mit szólsz öreg, kell vagy nem?". De **akkor sem kérek kéretlen SMS reklámot**, nem vagyok én az öreg spamolvasgató legkisebb fia. És ez az autópálya matricás legalább harmadszor jött az idén.

A másik még gázabb. Kiindulás ugyanaz. Honnan tudja a mobilszolgáltató, van-e autóm, vagy ha van is, Debrecenből vagy Nyíregyházáról miért menne valaki Budapestre a Hentes és Mészáros utcába javíttatni? **Mert hogy még az előfizetői címjegyzékkel sem egyeztették, és az összes vidéki című előfizetőnek is elküldték a kéretlen reklám SMS-üket**, az ezer százalék.

Félő, hogy **a folyamat vége a jövőben talán olyasmi lesz**, mint az HBO csatorna a kereskedelmi adókhoz képesti viszonya a reklámokkal: plusz pénzért jól nem kapjuk. **Alapból "jár" majd az ingyenes promóció minden mobilos díjcsomaghoz, de ha fizetsz havi X forintot a mobilszolgáltatódnak, akkor majd nem kapsz ilyeneket**. Az viszont egy másik jó kérdés, **mi lesz ha egy idő után az adott reklámozgatott weboldalakra majd szépen rámozdulnak a kártevő terjesztők**. És persze van még egy aspektus, **ha már kiajánlják ezt a szolgáltatást bárkinek, aki fizet érte, mi akadályozza meg azt, hogy egy bűnöző direktben rendelve szándékosan egy fertőzött weblapra** irányítsa majd a látogatókat?

Szerintem egyetlen mobilszolgáltató se csodálkozzon, **ha így az előfizetőknek sünökkel kapcsolatos gondolatai támadnak majd velük kapcsolatban**.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1118846

Kommentek:

muka 2009.05.13. 21:15:58

Maguktól, az engedélyed nélkül nem adják ki a mobilszolgáltatók a számodat, az adatkezelést nagyon komolyan veszik. Három lehetőség van, és sajnos többségében tőled indlhatott ki a számkiadás:

1. Amikor előfizettél (prepaid-et vettél) bejelölted, hogy küldhetnek neked harmadik fél üzenetet (és ez jól láthatóan ott van a lapon, amit ki kell töltened), de ilyeneknél is nagyon komolyan veszik, hogy ne akárkinek adjanak ki adatot (spam küldőnek) - az autópályánál talán ez történt, mert az a számból láthatóan az aggregátortól jött
2. A másik esetben (autószervíz) vagy Te adtad meg oda az adatodat (elvileg nekik is fel kell hívni a figyelmet az adatkezelésre), vagy megvették, mert előfizetéskor Te engedélyezted (ezt nem hinném)

Hidd el, a mobilok nagyon ügyelnek arra, hogy ha nem jelölted be, ne adják ki, ha bejelölted (mert opt-in szabályozás van), ne akárkinek adják ki.

Egyébként bármikor rendelkezhetsz arról, hogy ne adják ki, sőt kérheted is a konkrét ügyekben a kivizsgálást a T-Mobile-nál.

Lesből Támadó Szárítókötél 2009.05.13. 21:36:23

Az elsőt tényleg a mobilszolgáltató küldte, blogban való hőbörgés helyett érdemes lenne megkérdezni a mobilszolgáltatót, és ezt akkor így hogy?
A másodiknak viszont semmi köze a a szolgáltatóhoz, ez egy tipikus szpemmel SMS: jobbik esetben megadtad valahol a mobilszámod, ahol nem kellett volna, és most iszod meg a levét, rosszabbik esetben számtartományokra küldtek ki SMS-t és te pont beleestél. A második esetben érdemes lenne felhívni a számot és érdeklődn.

Before · http://azbeszt.blog.hu 2009.05.13. 21:44:24

Ezek elég durvák, engem a voda bombáz rendszeresen a faszságaival, de legalább nem 3rd-party cuccokat kínál...

Tib 2009.05.13. 21:57:27

Hát a Vodafone engem is kegyetlenül zavar. Mostanában ugyan visszafogták magukat, de könyörgöm már, ne reklámozzák már magukat N db. SMS-ben!

Illetve ha nagyon akarják reklámozni, akkor 1. kérjenek engedélyt ELŐRE ("fel akar íratkozni az Újdonságok spam-ünkre?"), 2. valami digest jelleggel, havonta-kéthavonta egyszer küldje, ha már valaki akkora birka, hogy feljelentkezik 3. inkább emailben küldje.

Én NEM adtam a Vodafone-nak engedélyt, hogy kéretlen reklámokkal bombázzon!

És a legdurvább azért az, hogy a Voda direktben csinálja, mert az ember a szolgáltatóját fontosabbnak tartja, egyéb SMS-t olvasás nélkül is kivág a fenébe, de a Voda írhatna valami fontosat is, pl. egyenleg, ált. szerződési feltételek módosulás, árak ugye változtak - na ez utóbbi kettőről ugye kussoltak kegyetlenül -, de nem, szórakoznak...

nemuccaszoc 2009.05.13. 22:35:36

ogos, egyedül, amit elviselek az a szülinapi köszöntés.

kovi1970 2009.05.13. 23:10:02

Egy valamit nem értek. Miért +100Ft (vagy mennyi) ha SMS-ben vesz valaki autópályamatricát?
Így nem is veszek ilyen módon. Úgyis meg kell állni valamelyik benzinkútnál.

ügyfélszolgálatos 2009.05.13. 23:42:15

Szokás szerint baromságot beszéltek. A T-mobile-nál szarni sem lehet anélkül, hogy ne íratnának egy szaros papírt.

atleta.hu · http://www.atleta.hu 2009.05.14. 00:35:09

Pannonnal is ikszelni kell, hogy engedelyezed-e a telszam marketing celra valo felhasznalasat. Ha nem emlekszel, hogy mit ikszeltel, akkor pl. it ellenorizheted: www.tudakozo.t-com.hu/main?xml=main&xsl=main

Itt jelzik, hogy letiltottad-e a marketing es egeyb direkt megkereses celu felhasznalast. Ha meg bakot lottek, akkor ventillalas helyett tessek jelenteni az NHH-nal.

Lajosforras 2009.05.14. 07:00:09

Angliában a vezetékes telefonnal szopatnak,ott tényleg elő kell fizetni egy szolgáltatásra,ha nem akarsz kéretlen reklámüzeneteket kapni.Hamar rákapnak majd a magyarországi szolgáltatók is...

russell 2009.05.14. 07:18:37

Komoly problémák meg kell hagyni!

Mondjuk ennyi idő alatt amíg megírtad a posztot abból az összes spam sms-t ki tudod törölni kb. 20 évre előre. Kurvára ráérhetsz ha csak ez az összes gondod.

Autópálya matrica sms vétel: az elsők között kezdtem el használni azóta sem vettem más formában. Itt legalább nem basznak át, hogy valóban érvényes-e (volt rá példa MOL kút) nem állok sorba amíg a kutas picsa kibogarássza magát, hogy "Józsi akkor most mit kell beütni?" anyádat baszod aki megszült, meg a munkáltatódat aki ilyen sötét parasztbábút alkalmaz, nincs sorban állás, hogy a tököm már megint kivan mert egy matricás megint bénázik stb. stb.

100 Ft-l többe kerül? Jah, ennyit nem is merek adni a kutas srácnak aki lemossa a szélvédőt, mert égne a pofámról a bőr.

Labasmaz 2009.05.14. 08:35:01

Altalanos iskolas kislanyom mobiljara a johiru Intrum Justicia kuldozget SMS-eket, hogy ha nem fizeti ki tartozasat, akkor be fogjak perelni. Ezeknek hova postaztassam a sunt? :-)

Mokele-Mbembe 2009.05.14. 08:50:27

Nemrégiben elém is úgy tették le az előfizetői szerződést, hogy előre be volt ikszelve a "Hogyne, persze hogy kérek spamet mindenkitől" jelölőnégyzet.

Én akkor észrevettem, de nem ez az általános. Rendszerbe van égetve a szopatás.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.14. 21:45:28

Üdv mindenkinek, köszönöm a rengeteg kommentet :-)

@Muka: a mobilszolgáltatónál BIZTOS, hogy tiltva volt ez az opció, az eset miatt külön is rákérdeztem telefonon.

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.05.14. 21:48:26

@Lesből támadó Szárítókötél:
Az autópályás dolog egy házon belüli dolog, és mint megtudtam "Tipp Info promóciós SMS szolgáltatás" a neve, ez nem is szerepelt szerződéskötési lapon, de szerencsére a telefonos ügyfélszolálaton le lehet mondani.

A második esetben szinte biztos hogy igazad van.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.14. 21:49:08

@Uccaszoc:

Szívemből szóltál, egyetértek :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.14. 21:54:03

Szia Atleta.hu!

Már jeleztem fentebb, hogy az autpályás ügyek egy a szerződéskötéskor nem rendlkezhető (mert ott csak a harmadik fél markatinget lehetett tiltani/engedélyezni) Tipp info volt, de ezt szerencsére már letiltattam.

A második (szervízes) dolog egy SMS spam, amihez a T-Mobilenak (állításuk szerint) semmi közük, így az NHH-nak sem. Amit az ügyfélszolgálat szerint tenni lehet, az a reklámszövetségnél bejelenti, náluk reklamálni. Az idén egyébként jártam autószervízben, és intézkedtem biztosítási ügyben (de vidéken) esetleg azt tudom elképzelni, talán innen kerülhetett ki telefonszám?!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.14. 22:00:43

@Russel:
Értem a logikát abban amit mondasz, de igazából egy ilyen blog pont azért íródik, hogy mások is hozzá tudjanak szólni, tájékozódjanak. Persze, hogy ki tudom törölni, de érdekel, hogy került oda, van elképzelésem, hogyan használhatja fel a jövőben ezt egy vírusterjesztő, és hasznosnak gondolom, ha ezt boncolgatjuk.

Például a bkvfigyelo.blog is simán szájbavághatná a bunkó sofőrt, az ordibáló ellenőrt, a kuka utast, és így is elintézhetné az ügyeit, vagy csak simán nyelhetné a könnyeit, de helyette blogot ír nekünk, tájékoztat, mi pedig sok esetben elgondolkozunk, okosabbak leszünk, és talán az illetékesek is időnként odatévedve nyesegetik a nagyon nem odavaló emberkék egoját vagy fizetési cetlijét ;-) Szerintem mindig akad pár ember, akinek hasznosat vagy érdekeset tud mondani, és én is ebben a hitben ringatom magam ehelyütt az én területemen :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.14. 22:02:24

@Mokele-Mbembe:
Hát igen, az apróbetűkre egyre jobban figyelni kell, de nálam nem ez volt a szitu, jó helyen volt az X.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.15. 09:03:20

Na meg van a végkifejlet is, a második esetben a T.Mobile ártatlan :-) Felhívtam a reklámban megadott ismeretlen szervízt, és kiderült, ugyanaz a tulajdonosa, mint annak a vidéki szervíznek, ahol én valóban javíttattam. És a megadott telefonszámok (ezen vártuk, hogy szóljanak, ha pár nap alatt
végre elkészül az autó) birtokában ők úgy gondolták, küldhetnek ilyet.

Én nem így gondoltam, ezért levetettem velük a listárjukról a számainkat (kettő is volt), és ezt első szóra udvariasan megtették. A tanulság ezek után az, hogy ha bárkinek névjegyet vagy telefonszámot megad az ember, jusson eszébe ez a történet.

Steve Jobs is megvolt ;-)

2009.05.15. 21:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: amazon belépés steve jobs támadó váltságdíj adathalász jelszócsere

Mire vigyázzunk, ha IT guruk vagyunk? Röviden összefoglalva: ha te akarsz a legnagyobb hal lenni a folyóban, ne engedd, hogy idő előtt kifogjanak! Minden egyéb kiderült alant...

A social engineering rejtelmei, módszerei naponta változnak, bővülnek új eszközökkel, és igénylik a **kiemelt odafigyelést a begyöpösödött pavlovi reflexek helyett**. Rendszeres jelszó csere, bizalmatlanság, tanúsítványok kiemelt vizsgálata, csak ismert és megbízható forrásból történő szoftver telepítése, és még lehetne sorolni hosszasan. Amikor Kevin Mitnick honlapját is feltörték, érezni lehetett, vibrál **egy fajta dámvadas izgalom a levegőben az ilyen különleges trófeák begyűjtésénél**, ami aztán sokszor beigazolódott, legutóbb például az antivírus cégek weboldalai elleni webes támadásoknál.

Emellett **nem lehet elhanyagolni kulcsemberek, cégvezetők, és jól ismert IT szereplők elleni próbálkozásokat** sem, főleg ha sikeres a kísérlet. Most Steve Jobs Amazon áruházas accountja került horogra, pontosabban ennek kihorgászása az elkövető Orin0co szerint már a tavalyi évben megtörtént, csak a nyilvánosságra hozatal a friss esemény. Ezek szerint emberünk időt és fáradtságot nem kímélve, létrehozott egy hamis Amazon áruházas weblapot belépéssel, és alátartotta a lavórt az érkező adatoknak. A sok hétköznapi jogosultsági adatok mellett azonban **nagy meglepetésére maga Steve Jobs is figyelmetlen volt**, és besétált a csapdába: **megadta a nevét, címét, bankkártya adatait, telefonszámát, valamint Amazonos belépési nevét és jelszavát**. A hiteles belépésről képernyőmentés is készült, és a támadó levelet is írt a "bestseller" Jobsnak, amiben azt is megemlíti, **6-7 évre viszamenőleg még plusz érdekes információ a korábbi vásárlásainak listája**. A levélben részletesen elmondja, hogyan sikerült a fenti módon bejutnia és **felajánlja, hogy egyfajta váltságdíjként vegye meg tőle ezeket az adatokat**.

Reméljük, a lista nem lesz tele szégyenszemre "Windows for Dummies..." kezdetű könyves tételekkel ;-), mindesetre az IT "celebjeinek" ha nem is naponta, de havonta mindenképpen javasolt a teljeskörű jelszócsere - és a sablonos adathalász támadásokba való be nem sétálás. **Mindenesetre én Bill Gates és Linux Torvalds helyében már válogatnám a szimpatikusabb görbületű hexakaraktereket az új jelszavaimhoz...**

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1123068

Kommentek:

Nincsenek hozzászólások.

Robotok a biztonságért

2009.05.18. 10:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mozi akció 4 terminator android nod32 eset

Összedugta a fejét **a NOD32 Androidja és a Terminátor 4 robot**, és mivel mindketten a 4-es verziónál tartanak, hát gyorsan egy **közös fellépést szerveztek** "Uralkodj a gépeken" címmel :-)

A lényeg, hogy az akció keretében meg lehet rendelni **az ESET Smart Security limitált kiadását, amelyhez ajándékképpen 2 mozijegyet is kapunk a Terminátor - Megváltás premier előtti vetítésére**.

A vetítést 2009. június 2-án, este 8 órakor tartják, a Duna Plaza mozijában. Minden további részlet és tudnivaló elolvasható itt.

Mikrobi és R2D2 esetleges részvételéről nincsenek hitelt érdemlő információink ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1128295

Kommentek:

Nincsenek hozzászólások.

Hogy ki a feladó? Hát izé, ehhez kattints rá!

2009.05.19. 09:23 | Csizmazia István [Rambo] | 1 komment

Címkék: trükk képeslap virtuális kártevő

Számos csalárd **elektronikus képeslap kering már, sokféle ünneppel kapcsolatosan**: ismerjük van mikulásos, húsvéti nyuszis, karácsonyos, vagy akár Valentin napos. És vannak a szürke hétköznapok, amiken ennek ellenére azért még jöhet "meglepetés" küldemény.

A Sophos kutatói nemrégiben figyeltek fel arra a **virtuális üzenetre, amely egy rövid levélkét és benne egy animált bébi fejet tartalmazott**. Az eredetileg portugál nyelvű levél nagyjából az alábbi szöveget tartalmazta:

"Az alábbi üzenet 5 napig érhető el.
Valaki küldött az Ön számára egy különleges titkos üzenetet:
Mondok egy titkot: Szeretlek!
Hogy láthassa, valójában ki is küldte az üzenetet, kattintson!"

Nos **ez az a pont, ahol aztán a nem kívánt mellékhatások önálló életre kelnek**, és aki bedől/elhisz/kattint, az gazdagabb lesz egy élettapasztalattal, **valamint egy banki jelszólopó trójai programmal**. És megint lesznek emberek, aki majd saját kárukon tanulnak meg ismét valamit :-(Úgy vélem, azoknak, akik például ezt a blogot is olvassák és meg is értik, **nagyobb a felőssége, mint a többi átlagembernek, aki nem tud ezekről, nem is érti**, stb. Nekünk kellene számítógépesen - persze nem Supermenként - de valahogy mégis többet, jobban segíteni a környezetünkben élő többi "non-geek"-nek. Nem volna szabad, hogy a kiszolgáltatottak, a magukat megvédeni nem tudók így járjanak :-(

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1128238

Kommentek:

gothmog 2009.05.19. 20:54:17

Épp ma jött egy mail bizonyos sgt. Cristopher Lewis amaerikai katonától, aki szeretne nekem 8 millió $-t átutalni. Aszongya Szaddam palotájában találta egy hordóban.
Szerinted? ;)
Jó, ez nem trükkös képeslap, csak egy szimpla spam a csupa nagybetűvel írott fajtából, csak gondoltam, azért elmesélem, még ez a típus sem halt ki.

Folytassa hacker...

2009.05.20. 18:21 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: bbc webkamera hacker trójai kémprogram prevx

Valaki úgy látszik azt tanácsolta a BBC stábnak, hogy "Folytassa..." **Meg is lett az eredménye, elkészült ugyanis a következő demonstrációs epizód is**, a hacker vezérelte webkamera avagy így fertőznélek meg és így lopnám el az adataidat, ha akarnám munkacímmel.

Nem kellett sokat várni a korábbi botnetes témájú BBC és Prevx koprodukció újabb filmjére, már meg is érkezett.

Lehet, hogy ezúttal is vegyes érzelmekkel teli fogadtatásban lesz részük, bár **az első epizódhoz képest annyit mindenesetre megtettek, hogy szóltak és engedélyt kértek a kísérleti nyúltól**. Szóval telepítésre került egy trójai, ami képes a képernyőképet közvetíteni a támadóknak.

De ez még nem minden, mert a webcamera képét is mutatja, így például hallhatjuk-láthatjuk, ahogy emberünk, Tony Jones éppen a noteszgépe előtt telefonál. Természetesen **a billentyű leütés naplózás is működik, így a csillagokkal begépelt jelszó** sem marad titok.

Nehéz megítélni, ettől majd megijed-e annyira az átlagfelhasználó, hogy biztonságtudatosabb legyen, operációs rendszert frissítsen, naprakész biztonsági szoftvereket futtasson, de **kíváncsiak leszünk majd az ilyen irányú statisztikákra**. Az **a kétely azonban továbbra is él, hogy aki ilyen dolgokkal akar foglalkozni, az amúgy is értelmesebb annál, semmint egy bulvár műsorból tanuljon, viszont a "Pistikéknek" lehet, hogy pontosan egy ilyen adás kelti fel a kedvét** egy kis házi vagy iskolai kémkedéshez. Bizarr módon világszerte a BBC kínálja az etikai mércét és kódexet, ami az ilyen műsorok után megosztja a szakembereket és nézőket is. A tájékozottak és a szakemberek amúgy is tudják, hogy a botnet és a trójai kémprogram létező probléma.

És még egy apró adalék: a BBC többszöri e-mailes megkeresésünkre sem reagált semmit, csak a tértivevény érkezik vissza tőlük, de **a négyszeri levélre kettő hónap alatt sem bírtak ezidáig válaszolni**. Ennyi erővel akár albán kecskepásztoroknak vagy orángutánoknak is írhattunk volna, hiszen ők sem válaszolnak e-mailekre. Bár az orángutánok **pár banán után lehet, hogy esetleg mégis csak megtennék ;-)**

Ha az olvasónak van véleménye arról, hogy **vajon hasznosak vagy inkább károsak az ilyen bemutatók, illetve hogy illegális-e ilyen adást készíteni** - akár pro, akár kontra - **örömmel várjuk a kommenteket**. (És vajon mi itt etikusak vagyunk-e, hogy bemutatjuk, azt, ahogy mások bemutatják azt, hogy... :-) Ha Henryre hallgatunk, nem igazán, mert szerinte "Hová vezetne ez?!"

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1133011

Kommentek:

Nincsenek hozzászólások.

IQ mentes MKB elleni adathalász akció

2009.05.21. 12:15 | Csizmazia István [Rambo] | 33 komment

Címkék: bank szánalmas helyesírás phishing mkb adathalász

Vannak esetek, **amikor ijedtség helyett a röhögés jön az emberre némely "szofisztikált" phishing támadás** esetén. Nos, a Magyar Külkereskedelmi Bank (MKB) elleni május 14. akció folytatása **láthatóan limitált mennyiségű agysejttel és csekélyke magyar nyelvtudással rendelkező** bűnözőtől származik - talán a válság miatti össznépi spórolás jegyében automatikus fordítással látta meg a napvilágot.

Hogy **a mélyen szánalmas levél tárgya vajha miért lett "Surgos Hirdetes"**, az korunk egyik óriási rejtélye a többi hasonló kaliberű világrengető kérdés mellett, mint például hogy a hóeke vezetők reggel hogyan jutnak el a munkahelyükre.

Az már első pillantásra látszik, hogy **ha a továbbiakban használni akarjuk a "kontunkat", akkor bizony folytatni kell a "procseszt"**, ez világos, mint a nap. Az mkb.hu helyett a link azonban a noerrpole.com/blabla oldalra küldene. **Időközben az oldalt már sikeresen bannolták**, így annak eredeti állapotához már nem volt szerencsénk.

Úgy véljük, a nyomozó szervekkel ellentétben **nekünk viszont sikerült lelepleznünk a tetteseket**. A levelek bitszintű alapos vizsgálata nem zárult ugyan teljes sikerrel, **de a helyesírás elemzés szerencsére megadta** a várva várt infomációkat, Grissom papa elbújhat melletünk: **Török Szultán és Fülig Jimmy együtt bűnszervezetben követte el ezt az MKB Bank elleni adathalász támadást!**

Hát ezúton "KÖszönjük az eggyetértést.", "hejesírás" rulez, meg hasonlók :-)

· 1 trackback

Ajánlott bejegyzések:

- A PRISM szeme mindent lát

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1134931

Trackbackek, pingbackek:

Trackback: HTML Info 2009.05.26. 15:29:54

Biztonsági figyelmezetésSzeretem, ha egy bank gondoskodik rólam. Hát még, ha biztonsági figyelmeztetést is küld egy biztonsági intézkedésről. Csak ne kérné el az adataimat… Ha nem csak magyarul nézne ki a szöveg… És ne akarna valahová a vilá…

Kommentek:

johevi 2009.05.21. 12:49:06

Már egyszer írtam, hogy az igazi adathalászok kikérik maguknak az "adathalászás" kifejezést, ez annyira gagyi... Kb olyan, mintha valaki odajönne hozzám és azt mondaná: add ide lécci lécci a slusszkulcsod, pont ilyen autót akarok venni, had' menjek vele egy kört... . Az adathalászat (szerintem) az amikor feltörnek, leolvasnak, visszakódolnak dolgokat (mondhatni energiát és tudást fektetnek bele) az ilyen "add meg lécci lécci" adatod, kulcsod, pénzed dolgot nem neveznék adathalászásnak, ez egyszerű átbaszása a hülyéknek akik esetleg odaadják, megadják.

bécsi pszicho · http://www.flickr.com/photos/haazee 2009.05.21. 12:50:38

MKB Bank Zrt vagy régi nevén Magyar Külkereskedelmi Bank!
(ki volt az a barom, aki kitalálta, hogy MKB Bank... van ott néhány nagyon agyas marketinges)

bécsi pszicho · http://www.flickr.com/photos/haazee 2009.05.21. 12:51:43

Mellesleg ezek a barmok (SZVSZ) nem rendelkeztek semmiféle nyelvtudással. Ezt valami fordító szoftverrel csinálhatták...

nemuccaszoc 2009.05.21. 12:52:12

Surgos tiszta Pákó. Ő is biztos felcsapott cyberhalásznak.

SirJohn 2009.05.21. 13:52:45

Nekem az IQ-ról a TOYOTA IQ jut az eszembe amit a TOYOTA SAKURA-nál ki is lehet próbálni. www.sakura.hu Most egy tesztvezetéssel lehet nyerni egy okostelefont is. Érted? IQ és okostelefon...

Dövan 2009.05.21. 13:54:48

Mivel az, hogy szép eszköz A Google fordító, az összes hülye emberek azt hiszik, hogy attól a pillanattól kezdve, hogy képes lesz arra, hogy írjon üzenetet bármilyen nyelven. Ezek azok az emberek, akik úgy gondolom, hogy ők is fertőzöttek egy számítógépes vírus, és az esti híradójában beszámoló elterjedt DOS támadást, a következő napon, üljön le, hogy a számítógép a védő maszkot. És most csinálnak "adat-adathalász" ...

(c) google translator :D

razzia (törölt) 2009.05.21. 14:00:29

Én is kaptam tőlük 2x is: "Fontos announcement" meg "Surgos nemtommi" tárggyal. Még jó, hogy nem vagyok ennél a banknál. :))

Kósza 2009.05.21. 14:01:05

@bécsi pszicho: miért, az O Takarékpénztár Bank mennyivel jobb? Egy jól mozaikszó legalább 3 betűs, és a tevékenységi kör megjelölése szintén nem hátrány! Hogy a vélhetően Te szakmádnál maradjak, hány ...computer számítógép nevű céggel találkozhatsz?!

Kósza 2009.05.21. 14:02:38

A kedves postoló kijavithatná, MKB=Magyar Külkereskedelmi Bank,..... De leginkább Hajrá MKB Veszprém! :)

kispista 2009.05.21. 14:06:43

"a securitate okokbol kifolyolag zártuk le az ön kontját"

A legjobb rész. A románok ellopják a lovainkat és a bankszámláinkat:)

BruceTheHoon 2009.05.21. 14:08:05

A második levél szerintem nem géppel van fordítva, hanem olyan valaki írta, akinek román az anyanyelve, és középfokú szint alatt van valahol a magyartudása, (vagy magyar ugyan, de nagyon erős román környezeti hatás alatt áll). Erdélyben teljes folytonos skála található a szép magyar beszédtől kezdve a magyar nyelvtanba ágyazott román szókincsig, ez a mail az említett kontinuum egy pontját illusztrálja.

brodaclop 2009.05.21. 14:10:22

@BruceTheHoon: Bizony. Securitate, kont, procsesz.

Mar csak a borkan es a punga hianyzik. :)

W Joe 2009.05.21. 14:14:35

Kedves ugyfel, biztonsagi okokbol nem hasznalunk ekezeteket. Kerjuk utalja at nekunk minden penzet. Nem atveres, mi tenyleg a bank vagyunk. Nem atveres. De tenyleg.

W Joe 2009.05.21. 14:15:42

"Én egy román vírus vagyok, de sajnos technikai fejletlenségem miatt nem tudok kárt okozni a számítógépedben. Kérlek, hogy törölj le egy számodra fontos fájlt és küldj tovább!"

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.21. 14:17:25

Köszi Kósza!

Javítottam. És emellettt leginkább Hajrá MKB Veszprém! :-)

Kósza 2009.05.21. 14:22:48

@Csizmazia István [Rambo]: a cimbe beleszúrhatnád, hogy elleni,... aza MKB elleni akciót minősitesz

---

most kaptam meg a jegyeket a vasárnapi bajnokavatóra :)

BruceTheHoon 2009.05.21. 14:47:49

A második levél szerintem nem géppel van fordítva, hanem olyan valaki írta, akinek román az anyanyelve, és középfokú szint alatt van valahol a magyartudása, (vagy magyar ugyan, de nagyon erős román környezeti hatás alatt áll). Erdélyben teljes folytonos skála található a szép magyar beszédtől kezdve a magyar nyelvtanba ágyazott román szókincsig, ez a mail az említett kontinuum egy pontját illusztrálja.

BruceTheHoon 2009.05.21. 14:50:17

mér' jelenik meg kétszer a posztom?

Yarner · http://androlib.blog.hu 2009.05.21. 14:56:25

kaptam belőle már 5-öt.
Szerintem is román lesz a drága, legalábbis gyakorlatilag nemlétező román nyelvtudással is az "A securitate okokbol kifolyolag zártuk le az ön kontját" még nálam is csengetett valamit :-).

ReWriter · http://miazhogy.blog.hu 2009.05.21. 15:06:13

Szerintem hétvégén és is restaurálom a kontjaimat.

Repülő Majom · http://www.kutyushop.hu 2009.05.21. 15:33:01

Nekem is volt szerencsém hozzá, kollégával derültünk jókat rajta. Kicsit az albán vírus jutott eszembe, ami felszólít, hogy töröld magad a vincseszter tartalmát, de előtte küldd el még az összes címre ami a levelező programodban van.
Viszont abba is gondoljatok bele, aki nem igazán ért a számítógéphez (pl. sokunk szülei), azok ennek is simán bedőlnek.
Úgyhogy csak óvatosan!

Sekiwake · http://ennyirefutja.blog.hu 2009.05.21. 15:56:23

Én mindig követem a küldött linket és megadok ilyenkor tuti felhasználóneveket és jelszavakat. pl:
login: suckhorsedick
pwd: fuckyourdog

Udvariasan megköszönték és az igazi MKB oldalon találtam magam

wowww 2009.05.21. 16:08:31

én egy ilyen verziót halásztam ki a spam könyvtáramból, ez akkor a 2.0-s?:

Kedves MKB ugyfel ,

Biztonsagi okokbol is felfuggesztettek a fiokjat, egy biztonsagi intezkedes, amelynek celja, hogy megvedjuk Ont es szamla.
Meg kell ujra az adatokat a folyo fizetesi merleg visszaallitja a mukodeset a fiokjat, es megerositi, hogy meg nem volt az aldozatok szamitogepes lopas.
Meg kell ujra adja meg az adatokat a kovetkezo oldalon, hogy az ellenorzesi folyamat soran:

https://www2.mkbnetbankar.hu/login.jsp?lang=HU&start=true

Koszonjuk szives egyuttmukodeset.

wowww 2009.05.21. 16:10:05

ja bocs csak a szekuritátést néztem, most látom a másikon fent is ez van

MILCSI 2009.05.21. 17:47:17

Ha Kossuth díjas színészek,tehát relatíve tanult emberek bedőlnek egy telefonnak és önként,dalolva átadják a megtakarításukat,akkor jogosan gondolják,hogy vannak "emberek",aki bedőlnek egy hivatalosnak látszó levélnek...azt pedig,hogy a helyesírás kívánnivalót hagy maga után,csak az veszi észre,aki tudja,milyen állatfajta a helyesírás :-))
Amúgy meg:

http://www.youtube.com/watch?v=JUdgn1O8dqQ

Ha a zene nem tetszik -bár igen jó :-))-, elég a feliratokat olvasni...ha beszélni nem csak madzsar :-PP

Sikamlós Jim DiGriz 2009.05.24. 07:55:17

Bocs, hogy ide írok, Rambo, csak egy gyors off kérdés: az eset.hu-n már kétszer is kitöltöttem egy volume licensz árajánlatkérőt, és még egy automatikus levél sem jött. Jó helyen kopogtatok, vagy hagyjam a francba az egészet? :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.25. 23:24:55

Szia Jim DiGriz!

Kis türelmet, utánanézek a dolognak, és rögtön jelzek.

bécsi pszicho · http://www.flickr.com/photos/haazee 2009.05.26. 05:34:09

@Kósza: a "takarékpénztár" szó nem azonos a "bank" szóval. Az MKB esetében a kis zsenik (természetesen az OTP mintájára) eltörölték a rövidítés eredeti értelmét, így lett a Magyar Külkereskedelmi Bankból MKB Bank.
Ha értelmetlen is, kimondva elviselhető az Országos Takarékpénztár Bank elnevezés, míg egy ... Kereskedelmi Bank Bank rettenetesen hülyén hangzik. :D
---
nahhh offról ennyit.

bécsi pszicho · http://www.flickr.com/photos/haazee 2009.05.26. 05:36:05

@MILCSI: tudod az úgy van, hogy az emberek öregszenek. Idős korban előfordulhatnak mindenféle mentális problémák, bármilyen nagytudású ember is volt korábban az illető... (minden gúny nélkül)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.26. 16:35:22

Szia Jim DiGriz !

Tedd meg, hogy írsz az info KUKAC sicontact PONT hu címre, és megírod benne, hogy pontosan mikor és milyen e-mailcímre kértél ajánlatkérőt. Ennek a konkrét infonak a birtokában a srácok már bele tudnak mélyedni az adatbázisba és segítenek.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.27. 11:40:05

Esetleg NoScriptes tiltás lehetett nálad az oldalon Firefoxban?

Sikamlós Jim DiGriz 2009.05.27. 13:34:05

Opera volt az istenadta, és mentek a scriptek, de máris dobom a mailt.

nyos (törölt) 2009.06.01. 03:40:21

Vegyuk peldaul a TCP/IP protokollt.
Kiirva: Transmission Control Protocol/Internet Protocol protokoll.
Meses. Ehhez kepest az MKB bank nudli.

Amikor a farok csóválja

2009.05.26. 20:45 | Csizmazia István [Rambo] | 1 komment

Címkék: spam sms általános feltételek e mail kéretlen szerződési baumaxx

Egy korábbi bejegyzésben már megvitattuk a szoftverekhez mellékelt, sok oldalas és bonyolult megfogalmazású felhasználói licencszerződések kérdését. **Aki nem ügyvéd, és eddig még sohasem vásárolta meg az Utolsó vacsora című festményt ÁFA visszaigénylés céljából**, az eleve hendikeppel indul egy ilyen apróbetűs szövegekkel végzett artistamutatványos versenyben.

Mai kitekintésünk emellett még egy kissé kapcsolódik az SMS spam témájához is, ahol az derült ki, **egy egyszerű autójavítás esetén a gyanútlan ügyfél kéretlenül bekerül a szervízes cég adatbázisába, ahol SMS-en keresztül kap kéretlen üzleti ajánlatokat**, például 100 kilométerre lévő autószervízt ajánlgatnak neki. A másik érdekesség pedig **a mobilszolgáltató saját üzleti ajánlatainak fogadása vagy elutasítása nem szerepelt a szerződésben annak megkötésekor, és a "Tipp Info promóciós SMS szolgáltatásról"** való leiratkozást egyedileg kellett a nyájas ügyfélnek intéznie.

Amit tehet még az alapos állampolgár, az az, hogy elmegy **a területileg illetékes Polgármesteri Hivatalba, és egy űrlapon kéri postai címének tiltását**, hogy senki harmadik félnek ne adják ki azt. Ha ezt megteszi a kérelmező nyilatkozattal, úgy **az egyébként alapértelmezett beleegyezés helyett életbelép a tiltás**, és az illető jó esetben nem fog többé kapni kártyás gyűjtőmappákról szóló soha vissza nem térő ajánlatakot, és a Reader's Digest **nyereményautó pléhből nyomott "slusszkulcsa"** is elkerüli majd nagy ívben a továbbiakban.

Ez eddig szép és jó, **marad a végére az emberi tényező, szépen felépített várunkat hogyan lehet a legkevesebb mozdulattal porig rombolni egy kis figyelmetlenséggel**. Általános Szerződési Feltételek nevű állatfajták nagyon sok helyen vannak, mi most egy szimpla pontgyűjtő, árkedvezményre jogosító áruházi kártyát nézünk meg, de a hasonlóság további valódi piaci szereplőkhöz természetesen nem a véletlen műve. **Ki ne szeretne egy Árfűrész nevű, és 10% kedvezményre jogosító kártyát?** Valószínűleg csak az, aki valóban el is olvassa a feltételeket. **Aki kész 2020-ig személyes adatait átnyújtani, és postai, e-mailes vagy SMS-en át érkező reklámajánlatokat szeretne kapni, az semmiképp ne habozzon tovább**. Azonban egy dolog fontos: **ezek már nem számítanak spamnek, hiszen nem kéretlenek**. Ugyanis nagy okosan (vagy figyelmetlenül, esetleg szántszándékkal) mi magunk voltunk azok, akik kérték, a kedvezményért cserébe.

"Érted? Nem! De remélted! A távcsövet a boltban te kérted."

Hát **ilyen az emberi természet: nem nagyon akaródzik elhinni, hogy ingyenebéd valójában márpedig nem létezik**. Persze van néha olyan eset is, amikor "ártatlanok" vagyunk: ha valaki a Top-Shop vagy WS Teleshopból vásárol bármit, sok kéretlen utánhívásra számíthat: nincs-e kedve merő véletlenségből még valami egyéb más terméket is rendelni, stb. Azonban mindig akadnak olyanok is, akik úgy érzik,

kedvezményekért (kuponok, kedvezményre jogosító kérdőívek, stb.) **cserébe szívesen önként és örömmel adnak alább a magánszférájukból.** Ha ők úgy gondolják, hát az már az ő bajuk, megbocsátunk nekik, mert talán nem tudják mit cselekszenek.

Aki viszont valóban vigyázni akar, az legyen nagyon óvatos, és **figyelmetlenségből lehetőleg ne rombolja le reggelre, amit a saját biztonságáért korábbi pedáns lépéseivel felépített estére**. Hiszen ettől függetlenül még így is kaphatott II. György angol király reklámlevelet a Delltől ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Utaljunk pénzt a S.O.C.A.-nak
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1144295

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.06.08. 08:09:26

Örökös szolgaság és lelkek adásvétele: miért kell elolvasni a szoftverlicencet?
www.bitport.hu/trendek/miert-kell-elolvasni-a-szoftverlicencet

Vírusellenőrzünk online, meg-megállva

2009.05.27. 12:04 | Csizmazia István [Rambo] | 4 komment

Címkék: online regisztráció anonim nélkül ellenőrzés eset scanner

Nyikorgó kosár ugyan nem lesz az ölünkben, viszont igyekszünk még serényebbek lenni. Az ESET online vírusellenőrzője már sokaknak lehet régi ismerős. **Segítségével a NOD32 letöltése, regisztrálása és telepítése nélkül is ellenőrizhetjük**, hogy az adott számítógépén található-e vírus vagy kémprogram, sőt ezt **akkor is elvégezhetjük, ha éppen nem a NOD32 antivírus rendszert használjuk, de szeretnénk próbára tenni, vagy összehasonlítani** jelenlegi vírusirtónk és a NOD32-nek teljesítményét.

Mostanra a **magyar nyelvű ESET Online Scannert még több beállítási lehetőséggel és megújult grafikus kezelőfelülettel látták el** a fejlesztők. Az alkalmazás a többszörösen díjnyertes NOD32 antivírus rendszeren alapul, a kártevők felismerésére pedig az ESET Víruslaboratóriumából kikerülő **legfrissebb vírusadatbázisokat és heurisztikus algoritmusokat használja**. Képes a rejtett fertőzések felderítésére, így **a rootkitek detektálására és eltávolítására is**.

Az Online Scanner legfrissebb újdonságai:

- Az ESET Smart Installer program telepítésével az eszköz már nem csak Internet Explorerrel, de az Opera, a Firefox és egyéb böngészőkkel is használható - ezt már nagyon vártuk :-)
- Anti-Stealth technológia, amely képes a rejtett károkozók - így a rootkitek - felismerésére és eltávolítására.
- Továbbfejlesztett ellenőrzési beállítások (a számítógép teljes vagy részleges ellenőrzése).
- Továbbfejlesztett proxy beállítások.
- 64 bites Windows rendszer támogatása.
- Megújult grafikus kezelőfelület

Aki szeretné kipróbálni, hogy mire is képes ez a technológia, az a 30 napos tesztverziókon felül **ingyenesen próbára teheti** az ESET magyarországi honlapján (www.eset.hu/viruslabor/onlinescan) elérhető online vírusirtót is, mely **néhány kattintással lehetővé teszi a számítógép teljes körű ellenőrzését és a kártevők biztonságos eltávolítását**.

Az Online Scanner **kitűnő megoldás lehet, ha valaki szeretné kipróbálni a NOD32 technológiát, vagy éppen csak meg kíván tisztítani egy fertőzött gépet**. Futtatása mindazonáltal a processzor sebességének, a merevlemez méretének és a tartalmazott állományok számának függvényében néha igen hosszúra - akár néhány órásra is nyúlhat. Mi egy kettéparticonált NTFS és EXT3 120 GB merevlemezt vizsgáltunk egy ősrégi 1400 Celeronos noteszgéppel XP alatt, rengeteg kis méretű állománnyal, és úgy kb. egymillió fájl vizsgálata után (ekkor már javában a Linuxos particiót ellenőrizgette) **megállítottuk (, de nem mentünk fel a padlásra).**

Azt is fontos kihangsúlyozni, hogy valósidőben nem véd a támadások ellen, csupán **ellenőrzi és eltávolítja a már a számítógépre került fertőzéseket, így semmiképpen nem helyettesíti a rendszeresen frissített és állandó használatra feltelepített vírusirtót**.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1146268

Kommentek:

atko 2009.05.28. 08:45:43

Üdvözlendő kezdeményezés.
Annó 2005 előtt még wines felhasználóként a Nod32-t tartottam a legjobbnak. Sajnos a Linux világában inkább csak a válalati felhasználókat célozza meg az Eset.
Könnyen telepíthető desktop verzió hiányzik a kínálatból. Így most Avast-t használok. De visszasírom a Nod32 kényelmét és gyorsaságát.

MILCSI 2009.05.28. 16:04:52

Kipróbáltam...pöpec :-))

Vargnatt 2009.06.12. 01:53:06

Kipróbáltam én is, valóban meggyőző.

Mindig ott volt bennem a kisördög, hogy nem bújkál-e valami rejtett kórokozó, ne adj isten rootkit a gépemen, és mivel a NOD-ot eléggé nívós programként ismerem, gondoltam itt az alkalom, hogy anélkül nézessem meg vele a gépem, hogy előtte a jelenlegi vírusírtómat valahogy forgalmon kívül helyezem, és felrakom a próba-NOD-ot.

Szerencsére semmi durvát nem talált, csak néhány korábban letöltött program telepítőjét találta gyanúsnak, azok meg nem aktiválódnak, amíg nem indítja el őket az ember. De aktív garázdálkodó vírust szerencsére nem talált, nem is éreztem, hogy lenne egyébként.

Ezentúl azt hiszem, inkább ezzel fogom végezni a rendszeres víruspucolást, a jó kis AVG Free meg marad rezidens védelemnek, mert azért elég jól bevált nálam, és az eredmények szerint nem nagyon engedett be eddig semmi komolyat.

Bár sejtem, hogy marketing szempontból az lenne egy ilyen online-scanner célja, hogy meggyőzze az embert a rendes program megvásárlására, és talán meg is tenném (a diákkedvezménnyel egész baráti az ár), ha nem volna az AVG Free, vagy ha most kiderült volna, hogy a látszólagos védelem mellett beengedett egy csomó mindent. De szerencsére még van ingyen AVG, és nem szerepelt le nagyon, úgyhogy egyelőre marad.

Viszont tény, hogy a NOD jelentősen gyorsabban nézte végig a teljes gépem, mint az AVG. Bár az AVG-nél is az utóbbi időkben jelentősen rágyúrtak a scannelési sebességre, de ez rájuk is fért már, mert a korábbi 7-8-9 órás scannelési idők gyakorlatilag elfogadhatatlanok voltak.

Van néhányszáz GB-nyi scannelnivalóm, és rengeteg apró kis file, meg egy rakás telepítőprogram, plusz a telepített programok mappáival is sok a szöszölés, de még így is durván lassú volt régebben az AVG, mostanában viszont átlag 1-2 órával hamarabb végez, mint korábban.

Bocsi a kisregényért, de gondoltam, hasznos egy kis user feedback ;)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.15. 11:33:05

Ez az online cucc lehet, hogy akkor jön a legjobban, ha valaki AV nélkül bekap valamit, ami miatt aztán már nem is tud telepíteni virusirto progit.

Madonna muszlim lett

2009.05.28. 19:46 | Csizmazia István [Rambo] | 5 komment

Címkék: spam us kanadai hiszékenység kínai madonna cert gyógyszerész

A sztárokkal annyi minden történik, vagy ha éppen nem is történik semmi, akkor pedig **egy rakat hülyeséget összeírkálnak róluk**, hogy a hír hallatán szempillánk sem rezdült: talán még igaz is lehetne. Mondjuk a Madonna fanok talán kattintanak, esetleg elmerengenek, hogy "No persze, majd pont a kínaiak fogják ezt nekünk bejelenteni" - nem tudhatjuk.

Lassan **akár egy komplett tankönyre való is összejön a social engineering, és az elmés e-mail küldözgetés** témaköréből, ráérő időmben majd konzultálni fogok Csernus doktorral, és lehet, hogy összehozzuk a nagy művet ;-) A fejemet mertem volna tenni már elsőre, hogy hamis a hír, az ilyenekről inkább a Blikkből, Story Magazinból és egyéb szaklapokból szokás tájékozódni, és nem Altidor B. Kristy kéretlen elektronikus leveléből.

A **linkek persze az unalomig ismert kanadai gyógyszerész oldalakra** visznek. A Super Size Me következő epizódjában (Return of the Hamburger) már valószínűleg nem csak Jézus Krisztust és az amerikai elnököt nem fogják felismerni az óvodások és a felnőttek, de még a McDonalds bohóc fotójánál is "hőő, hát ez a tag meg itten kicsoda?" félmosoly várható. **Egyedül a gyógyszerész néni és a gyógyszerész bácsi lesz 100%-os arányban felismerve , hiszen "ők azok, akik feltűnnek, bármire is kattintunk a számítógépen" :-)**

A többit már tényleg csak kiegészítésképpen mutatjuk, hiszen van itt kérem "rafiniren", **ha valaki éppen nem bukik Madonnára, van még egyéb muníció is a tarsolyban**: meleg party mészárlással, legutóbbi levelünk hibás küldésére való hivatkozás, hihetetlen pénzkereseti lehetőség (a szó szoros értelmében;-), ingyenhitel, stb. - **ki mire gerjed**. Lehetne akár "Enrico Palazzo elénekli a Himnuszt csak most, csak önöknek" is ;-)

Elsőre talán az is elég lenne, ha emberek úgy gondolkodnának, hogy **van nekem bármiféle dolgom kínai weboldalon? Hogy persze hogy nincsen? Hát akkor meg mit keresek én itt és miért kattintok?** Ne adjunk magas labdát a legújabb kártevő verzióknak, exploitoknak vagy csak a felesleges idő és erőforrás pocséklásnak. Az ősi testépítő igazságot jól kiforgatva: **"Az vagy, amire rákattintasz!"** Addig is ajánlunk egy kis olvasnivalót a témában az US CERT jóvoltából.

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1148608

Kommentek:

nemuccaszoc 2009.05.28. 21:33:36

Jó kis cikk ;)

S. Annyi 2009.05.28. 23:20:12

Zsidó már volt, most muszlim. Lesz majd buddhista is, de lehet, hogy néger?

varangyos diszkó 2009.05.29. 00:15:14

sose volt igazi zsidó, ugyanis betérése nem igazi
a reform betérő se betérő és a kurva anyját aki ennek ellent mond!

Ленина · http://szanalmas.hu 2009.05.29. 00:40:08

madonna egy ribanc.
és a gurva annyát aki ellent mond.. :)

I-brahi 2009.05.29. 07:27:21

OFF:

Az MTV meg akarja szüntetni a a Tűzvonalban című sorozatot. Ne hagyjuk. Írd alá az alábbi petíciót!

www.petitionspot.com/petitions/tuzvonalban

Firefox kiegészítő telepítés orvul

2009.06.02. 19:05 | Csizmazia István [Rambo] | 19 komment

Címkék: microsoft firefox biztonság patch extension .net mozilla

A hitviták közül mindig is kiemelkednek a jelentősebb témák, régebben a Commodore64 VS Spectrum, aztán később **a Windows kontra Linux volt ilyen elementáris erejű**, személyeskedésektől és elvakultságtól sem mentes flamewar. A kedvenc vagy éppenséggel a biztonságosnak tartott internet böngésző kliensről szóló értekezések is komoly indulati erőket, érv hegyeket képesek megmozgatni.

De hogyan értékeljük azt, amikor egy aktuális Microsoft frissítő csomag suttyomban, kérdés nélkül "öv alatti ütéssel" egy biztonságot gyengítő Firefox plugint telepít a gépünkre? Talán Sándor György szavai illenek ide leginkább: "Egyenlő pályák, egyenlő esélyek! Én biciklivel megyek."

A hírek szerint a .NET Framework (NET Framework 3.5 Service Pack 1) telepítő csomagja feltesz egy úgynevezett "Microsoft .NET Framework Assistant" extensiont, amelyről nem értesülnek a felhasználók. Maga a kiegészítés **arról gondoskodik, hogy rajta keresztül ettől kezdve könnyen és csendben (IE módi?!) lehessen programokat telepíteni a számítógépre**. Ha valaki tudatos döntése folytán választotta az Internet Explorer helyett a Firefoxot, akkor ezt könnyen a háta mögötti orvtámadásnak és **a biztonság megcsúfolásának tarthatja**.

Tovább **súlyosbítja az esetet, hogy ha az ember ezt nem szeretné így, akkor viszonylag nehéz tőle megszabadulni. A 2009 februári útmutató szerint kézi matatások szükségesek** a Rendszerleíró Adatbázisban (Registry), hogy az említett kiegészítő és annak hatása eltűnjön. Érdekes módon **néhányan még a Mozillára is neheztelnek a dolog miatt**, hogy az nem biztosít egyszerű uninstallálási lehetőséget az ehhez hasonló kiegészítők eltávolítására, hiszen az Uninstall gomb itt szürke, és nem működik. (Azóta egyébként az MS oldalán már közzétettek egy egyszerűbb eltávolítókát.)

Jó lenne persze, ha az ilyen esetekben **nem a szokásos "Használj Linuxot!", "Miért is nem használsz inkább Mac-et?" jótanácsok és kérdések repkednének a levegőben**, hanem valahogy korrektebbül zajlanának ezek a dolgok a Windows rendszereken belül. Például a tájékoztatás igen foghíjas itt, lehetne egy figyelmeztetés, ne adj' Isten kérdés jóváhagyással-választással, etc, vagy a "mellékhatások tekintetében kérdezze meg Steve Ballmerét", "Timeo Danaos et dona ferentes", miegymás. Azért, mert valaki Windowst használ, nem okvetlenül lenne kötelező pluszban még így is kibabrálni vele ;-)

Az ilyen buta manőverek, melyben tudatosan megsértik a felhasználói bizalmat, semmiképpen nem hasznos lépések a cég életében. **Az effajta kémprogram-szerű települések ellenszenvesek a nagy többség számára.**

Reméljük, Redmondban is olvasnak The Registert :-) És semmiképpen sem akarnak belekerülni abba a körbe, ahol csupa olyan alkalmazásokat fejlesztenek, amikhez a legtöbb Google találat "How to remove..."-val kezdődik ;-)

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1158398

Kommentek:

atko 2009.06.02. 22:35:28

Ez nem egy használj inkább Linux/Mac hozzászólás, de azért jó érzéssel tölt el, hogy erről én nem tudok semmit, a "registry" bejegyzéseket, meg egy mappa törléssel elintézhetem :-).
Sajnálom, hogy ilyet bármikor megtehetnek az emberekkel.

Vargnatt 2009.06.02. 22:43:23

Hmmm... eddig fel se tűnt ez a kiegészítő, de tényleg ott van. Mondjuk legalább azt be lehet állítani benne, hogy kérdezzen rá a ClickOnce programok futtatása előtt. Persze alapértelmezetten azért kérdezés nélkül végrehajta. Tisztára mint az autorun.inf...

"mellékhatások tekintetében kérdezze meg Steve Ballmerét"

Az ilyen, és ehhez hasonló beszólásokon szoktam fetrengve röhögni XD

De a cikk végén a póló felirata is nagyon tetszik, tanulságos. Vajon hol lehet ilyet kapni?

Kazi (törölt) · http://redmond.blog.hu/ 2009.06.03. 09:17:43

Nem akarok senkit megbántani, de láttatok már ClickOnce alkalmazást települni? Lehet róla mondani bármit, de azt enyhe tulzásnak érzem, hogy csendben települ. Finom voltam és udvarias. :-) Csá.

amodent 2009.06.03. 18:00:57

Én személy szerint nem neheztelek a Mozillára, de azért tényleg furcsa, hogy bizonyos addon-ok eltávolíthatatlanok. Itt van ez, de nekem egy Thinkpad ujjlenyomat-olvasós jelszókezelő addon-al is meggyűlt a bajom, miután egy böngésző-frissítés után abbahagyta a működést (gondolom érzékelte, hogy a verziószám már nem megfelelő), de eltávolítani sem engedte magát.

gothmog 2009.06.03. 18:53:42

@Kazi: Nem, hálistennek. :) De probléma nem is annyira ez, hanem a tény, hogy az ms kérdés nélkül belepiszkál az egyik legkellemetlenebb konkurense programjába. Nem mondom, hogy szándékosan rendezték így, mégis van a dolognak egy ilyen furcsa mellékíze.
"kitúrjátok a saját böngészőnket, a saját oprendszerünkből? Attól még a ti böngészőtök a mi rendszerünkön fut, így azt teszünk vele, amit akarunk." márpedig nem. na.

Kazi (törölt) · http://redmond.blog.hu/ 2009.06.03. 22:59:42

@gothmog: Bármilyen hihetetlen, ezt nem az MS találta ki, hanem user kérésre tette bele. Ugyanis a ClickOnce lényege, hogy egyszeri jóváhagyással lehet nagyon könnyen .Net-es alkalmazásokat telepíteni. Márpedig ha a ClickOnce plugin nincs telepítve Firefox alá, akkor az egész semmit sem ér.

Ha valaki pedig nem akar még ezer kattintással sem .Net alkalmazásokat telepíteni, akkor eleve fel sem kerül a gépére a kérdéses plugin. A helyzet ennyire nevetségesen egyszerű.

Nem akarom senki kenyerét elvenni, de az sem baj, ha látjuk a tényeket is. Talán egy kommentbe belefér.

Vargnatt 2009.06.04. 02:18:07

@Kazi: Pedig én nem akartam telepíteni ezt a plugint, de mivel nem kérdezett rá a .NET framework+SP1 telepítésekor, ezért csak felkerült ez is. Pedig én általában nem csak Next/Next/Finish módon telepítek, hanem többnyire meg is nézem, hogy mit és hogyan telepítek éppen. Ha szólt volna, hogy telepíteni akar egy ilyet, valószínűleg nem hagyom neki.

Kazi (törölt) · http://redmond.blog.hu/ 2009.06.04. 07:49:01

@Vargnatt: Ha nem akarsz .Net programokat futtatni, akkor miért telepítetted a .Net Framework 3.5 SP1 csomagot?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.04. 07:54:54

Vargnattal értek egyet.

Ezen az alapon a Microsoft azt is megtehetné, hogy megnézi, nincs-e Linux a gépemen, és annak a böngészőjébe is belepetézhetne kéretlenül és titokban egy Active-X vezérlők telepítését megkönnyítő kódot.

Az nem mentség, hogy "nem az MS találta ki, hanem user kérésre tette bele". És ha egy juzer majd víruskódot kér bele, akkor

azt is beletenné? (lásd Nürnbergi per, ahol mindenki mindent "csak" parancsra vagy utasításra tett.

Ha valaki titokban pénzt lop ki a pénztárcámból, van persze jelentősége, hogy 100 vagy 20000 forintót vesz el, de erkölcsi szempontból mindegy.

A Microsoft nem teheti meg, hogy azoknak, akik a "Halál vagy ungabunga" kérdésre "akkor inkább a halál"-t válaszolják, azoknak "na jó, de előbb (titokban) egy kis ungabunga" feleletet adják. Persze szigorúan szerintem... ;-)

Nem lett volna itt semmi baj, ha erről minden felhasználó értesül és választhat, akarja-e ezt vagy sem. Akkor ez a post sem született volna meg. De mikor valaki az erőfölényével visszaél, és a másik cég szoftverében alapvető módosítást hajt végre titokban, az nem úriemberhez méltó eljárás.

atko 2009.06.04. 08:52:23

@Csizmazia István [Rambo]: Hát azt a linuxra teszek valamit a közösség tudta nélkül című műveletet végignézném egy kényelmes páholyból. :-)
A nyílt forráskódnak pont ez a lényege: Nem tudsz titokban semmit csinálni, mert Tisztelt kódolvasó Barátaink elolvassák és értik is azt amit olvasnak (ellentétben velem) És azt mondják: "Eddig és ne tovább"
De ez még mindig nem oprendszer párharc. Abban ultra liberális vagyok. Egyik sem jobb, csak mások használják.

gothmog 2009.06.04. 09:57:24

@Kazi: példa: Ati Catalyst Control Centert láttál már?

Vargnatt 2009.06.04. 12:00:43

@Kazi: Szeretnék .NET-es programokat futtatni, de nem a böngészőmben.

A SP1-ben meg azért nem csak ez az a ClickOnce-os dolog volt, amiért telepíteni lehetett, de egyébként csak azért települt az is, mert épp akkor raktam föl magát a .NET 3.5-öt, és a letöltésben (www.microsoft.com/downloads/details.aspx?familyid=D0E5DEA7-AC26-4AD7-B68C-FE5076BBA986&displaylang=hu) ez így együtt volt.

Mint utólag látom, írnak itt valamit erről a ClickOnce dologról, de ebben egy szó nincs FF-kiegészítőről, még csak ActiveX-ről sem.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.04. 12:59:05

@Atko:
Hát ezt én is szívesen megnézném ;-) Technikailag ugye nem lehetetlen, Win alól pl. simán tudom írni/olvasni az ext3-at mondjuk az Ext2 Volume Managerrel.

Nem is itt koppanának fel, hanem a lelepleződéskor meg a bíróságon. Reméljük, azért idáig nem fajulnak a dolgok :-D

Az OS vitánál azért vannak különbségek: ha valakinek nincsenek különleges igényei (SAP, Macromedia Flash, AutoCAD, stb.), vagy nem szeretne a meglévő x millió kártevő 99.9 százalékával közelebbi ismeretségbe kerülni, az Win helyett Linuxozhat vagy költözhet Macre.

atko 2009.06.04. 15:37:05

@Csizmazia István [Rambo]: Olyat, hogy a jogtiszta linuxos merevlemezemen kalóz windows is legyen? ej ej..
Legfeljebb egy xplight a vboxban, onnan aztán ellenőrizhet ;-)
Az is csak a nyamvadék ie6 miatt kell, melyet persze futtathatnék wine alól, de akkor a linuxomat rondítanám el vele. így meg marad a vbox.
Az os-ről meg ugyanaz a véleményem, mint a office2007 kezelőfelületről. Aki amit tanul azt szereti. A sógonőm a laptopján mandrivát kapott, ő azt szereti. Csak kattogtatni tud, de attól még netezik szöveget szerkeszt skypol, bloggol stb. Szóval mint egy windows felhasználó, csak nem tudja mi az. :-)

Kazi (törölt) · http://redmond.blog.hu/ 2009.06.04. 19:14:50

 Vargnatt: A dolognak semmi köze az ActiveX-hez. Azt elismerem, hogy tényleg dokumentálhatták volna, hogy ez a plugin is települ, valóban, de magát a telepítést és a plug-int egyáltalán nem érzem problémásnak. Azért nem, mert szó sincs erőfölénnyel való visszaélésről, ugyanis pont az történik, hogy ne kelljen ClickOnce miatt IE-t használni, hanem FF alatt is működjön. Elmúltak azok az idők, amikor a MS az IE-t erőltette mindenáron, a plugin puszta léte is ragyogó példa erre. Üdv.

Kazi (törölt) · http://redmond.blog.hu/ 2009.06.04. 19:17:31

@Vargnatt: "Szeretnék .NET-es programokat futtatni, de nem a böngészőmben."

A ClickOnce nem .net programok böngészőben futtatására alkalmas, hanem egy a TELEPÍTÉST segítő technológia. Olyasmi, mint a Windows Installer, azzal is szoftvereket tudsz telepíteni, a ClickOnce-szal is.

MILCSI 2009.06.08. 23:27:57

Engedte magát letiltani...az nem elég? AnalfaBÉKA üzemmódú választ kérek szépen :-)))

dX 2009.06.11. 09:48:39

ugyanaz a kérdésem, mint milcsinek. a letiltás nem véd meg a káros következményektől? (persze azért szégyeld magad M$!)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.15. 11:59:33

Szerintem ha letiltunk valamit, akkor az nem müxik. Nem is amiatt írtam én, hogy bármiféle konkrét veszélyről lenne tudomásom. Hanem képzeld el a szitut, a konkurens cég belepiszkál titokban a másik programba, ami lehet hogy 100% jó, 100% szép, de akkkor jelezni kell, tájékoztatni, választást felkínálni.

Például az milyen lenne, hogy a Brawn-Mercedesz mérnökei éjjel suttyomban beszerelnek egy "igen hasznos" alkatrészt a Williams-Toyota autójába :-D

Izgatott Twitter csiripelés hallatszik

2009.06.04. 17:10 | Csizmazia István [Rambo] | 1 komment

Címkék: pdf twitter hamis script antivirus exploit

Ezúttal **a Twitter került sorra**, kártevőre mutató linkeket helyeztek el ismeretlenek az üzenetekben. Ha valaki óvatlan volt, egy hamis antivírusprogram keveredhetett a gépére.

A támadások hátterében **néhány feltört fiók, és az azokból küldött üzenetek állnak**. Ezekben **egy állítólagos videóra mutató linket helyeztek el "best video" címmel, amely egy külső hivatkozásra mutatott**. Maga a link korunk nagyszerű vívmányának köszönhetően (de természetesen szigorúan csak az animált GIF mögött :-) rövidített formában tartalmazta a kártékony URL-t.

Az oldalon azonban a várva várt videó helyett egy script fut le, emiatt pedig **egy exploit kódos PDF állomány kezd el letöltődni**, és elindulni. Legvégül a kitalált riasztásokkal operáló hamis antivírus próbál meg a fertőzött gépre feltelepülni. A Twitter szerint azóta már megszüntették a problémát, és törölték az érintett üzeneteket.

Nyilvánvaló, hogy **az ilyen módszer a jövőben egyre népszerűbb lesz**. Nekünk mindössze annyit kell az eddigi szabályainkon változtatni, hogyha Vladimir Banderas, Antonio Lenin, Iljics Ramirez, Fan van Dong, esetleg Üzmürü Tükmüty török alsómosó **vagy akárki ismeretlenül hülye linkeket küldözget**, akkor nem csak akkor nem kattintok rá, ha ez e-mailben jön, **hanem akkor sem, ha egy közösségi portálról érkezik ez üzenet formájában**. Reméljük, azért a többségnek ez nem lesz túl bonyolult feladat ;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1163238

Kommentek:

cworm (törölt) 2009.06.04. 17:13:57

Reménykedni mindig lehet és kell is, de ezrek fognak bedőlni az ilyen trükköknek is még... De akkor már inkább százezreket kéne írnom.

Vesztegzár a Grand Hotelben

2009.06.11. 22:16 | Csizmazia István [Rambo] | 3 komment

Címkék: hotel számítógép közös nod32 blaster internetszoba

Kicsit **Rejtősre vettük a címet, de ennek nincs igazi oka**. Egyik kedvenc vidéki szállodánkban időztünk, és **a vendégek számára fenntartott közös internetes szobába lépve furcsa dolgok** látszottak a monitoron.

A két darab Windows XP gépen egy igen **régi frissítésű NOD32 V2.7 vírusirtó ücsörgött, több éves adatbázissal**. Az opciókat sajnos nem sikerült megnézni, mert le volt jelszavazva az admin, de gyaníthatóan **nem volt bekapcsolva az aktív védelem, az AntiStealth, meg talán még a heurisztika sem, és emellett a Windows frissítései is ki voltak kapcsolva**. Eleinte ugyan még rettentő lassan működött az internet, aztán egyszerre csak elszabadult a pokol, **jött a már oly jól ismert és annyire utált visszaszámolós ablak**: Blaster a fedélzeten és újraindítgatja a gépet, grrrr!

Jeleztem a recepción a dolgot, és bár szabadságon vagyok, nem mellesleg azért felajánlottam a személyes segítségemet is. Hogy **pontosan mi volt a géppel, nem derült ki**. Megköszönték, hogy szóltunk, és a jelek szerint nem volt szükség a segítségre sem. Fél nap elteltével visszaérkezve ugyanis már szép **tiszta állapotban, és NOD32 4.0 programmal felvértezve**, felfrissítve találtuk a gépeket, és szépen hasították a NET habjait.

Hát ez most csak egy ilyen rövid helyzetjelentés volt, **pici szünet után** jövő héttől a blog is hasítja majd a habokat.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1179918

Kommentek:

Vargnatt 2009.06.12. 01:30:06

Kellemes kis tanmese volt így elalvás előtt :)

Amúgy valóban félelmetes, hogy ilyen közös netes helyeken mennyire elhanyagolják a vírusvédelmet, meg úgy egyáltalán a szoftverek/hardverek állapotát. Általában a minimum, amit összeszed az ember ilyen helyen, az egy-két autorun.inf terjedésű károkozó, már ha rá van kényszerülve az ember, hogy használja a pendriveját.

Abba meg, hogy hány keylogger figyeli közben a jelszavainkat, jobb nem is belegondolni...

atko 2009.06.12. 12:33:39

Nyilvános terminálon csak nyílvános dolgokat csinál az ember, vagy ha van hozzáférése beteszi a mindig kéznél lévő pendrive oprendszerét ;-) és azzl boldogul ha tud. Jómagam a POTE egyik nyilvános gépén bootoltam sikeresen pendrivről, ami azért elég súlyos biztonsági kockázat.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.15. 11:31:43

Ami még szerintem durva, hogy Skype és MSN is volt telepítve, és a vendégek használták is időnként. Nem véletlen, hogy a CARO2009-en mindenkinek ott fityegett a SIM stick a noteszgépében, pedig volt hoteles ingyen wifi :-)

Tarolnak az exploitokat kihasználó JavaScriptek

2009.06.15. 15:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

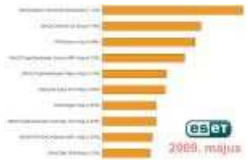
Az ESET víruslaboratóriumának szakértői szerint egyre több veszély leselkedik a fertőzött weboldalakon azokra, akik **nem futtatják le a Windows, az Office és immár az Adobe alkalmazásaik biztonsági frissítéseit**.

Bár Magyarországon továbbra is a Virtumonde végzi a legnagyobb pusztítást, egyre inkább erősödik a múlt hónapban **a vírusok magyarországi 10-es toplistájára került JS/Exploit.Agent** nevű kártevő: míg áprilisban csak a kilencedik volt, májusban már a hatodik helyet sikerült elfoglalnia.

Ha megnézzük napjaink legújabb fertőzési forrásait, egyre inkább a népszerű fájlformátumokra készült exploitok (biztonsági sérülékenységet kihasználó támadó kódok) tekinthetők „slágernek". A **Microsoft Office irodai programcsomag fájltípusai mellett ezek között rendre megtaláljuk az Adobe PDF és SWF, valamint az Apple QuickTime** kiterjesztéseket is. Így az elmúlt időszakban tömegesen jelentek meg olyan weboldalak, amelyeken preparált, a különféle sebezhetőségeket kihasználó PDF, SWF, DOC stb. dokumentumok találhatóak.

A JS/Exploit.Agent névre keresztelt károkozó a terjedéséhez egy már korábbról jól ismert Microsoft sebezhetőséget is képes kihasználni (egészen pontosan az MS99-042 nevűt, melynek leírása a http://www.microsoft.com/technet/security/bulletin/ms99-042.mspx címen található). A kártevő a támadó részére a webes látogató gépéhez hozzáférést biztosít, onnan fájlokat olvashat ki és módosíthat. Mindezek mellett a károkozót tartalmazó fertőzött weboldal arra is képes, hogy **az Internet Explorer bizonyos verzióiban egy kártékony kódot futtasson a gyanútlan látogató számítógépén**, természetesen annak beleegyezése és jóváhagyása nélkül. Reális veszély emellett az is, hogy a védtelen, és megfertőzött számítógépeken a kártevők az FTP jelszavakat ellopják, majd ennek birtokában a weboldalak kódjába szúrnak be olyan IFRAME szekciót, amelynek linkje zömében kínai weboldalakról igyekszik újabb kártevőket letölteni a látogatók gépeire. Akár kimondható, hogy egy új korszak jött el az interneten, amikor a vírusoknak köszönhetően már egy kattintás után sem lehetünk benne biztosak, hova is jutunk el a végén.

Aki saját weboldalát FTP elérésen keresztül szokta szerkeszteni, még nagyobb figyelmet kell, hogy fordítson számítógépének tisztaságára. Hiába tartja ugyanis titokban FTP jelszavát, a kártevő képes azt kiolvasni, és végigfertőzni a weboldal akár összes HTM, HTML és PHP állományát. Ilyen fertőzés esetén **a weboldal kódjának „kigyomlálása" csak az egyik lényeges teendő, a haladéktalan FTP jelszócsere, illetve lehetőség szerint áttérés titkosított FTP kapcsolatra, ugyanilyen fontos**. Ha pedig tudomásunk nélkül megfertőzték weboldalunkat, amelyet a Google kereső már feketelistára is tett „Bejelentett támadó webhely" címkével, úgy a mentesítés után a Google Webmester Tools segítségével kérhetjük, hogy vonják vissza az oldalunk blokkolását, amelyet általában néhány nap alatt teljesítenek.



Végezetül következzen a magyarországi toplista. Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2009 májusában az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek együttesen 39.26%-ot tudtak a teljes tortából kihasítani maguknak.

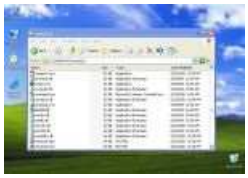
1. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a májusi fertőzések között: 7.41%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

2. Win32/Conficker.AA féreg
Elterjedtsége a májusi fertőzések között: 5.18%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: http://www.eset.hu/virus/conficker-aa

3. INF/Autorun vírus
Elterjedtsége a májusi fertőzések között: 4.89%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

4. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége a májusi fertőzések között: 4.33%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amelyek látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálják, azonban valójában maga a kártevő lapul a „csomagban”. Emellett hátsóajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-nbf

5. Win32/Wigon trójai
Elterjedtsége a májusi fertőzések között: 3.37%

Működés: A Win32/Wigon trójai kártevő család a számítógépre jutva különböző fájlokat hoz létre a Windows\System32 alkönyvtárban, ezek egyike a WinCtrl32.dll. Ezek segítségével készít el további kártékony állományokat a helyi gép TEMP mappájában, és eközben a rendszerleíró adatbázisban is módosításokat végez. A bejegyzések segítségével eléri, hogy a fertőzött DLL állomány törlése utáni rendszerindításkor az állomány ismét visszakerülhessen. Tevékenysége során elindít egy szervizfolyamatot is a fertőzött gép memóriájában.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/wigon-ck

6. JS/Exploit.Agent.AFH trójai
Elterjedtsége a májusi fertőzések között: 3.30%

Működés: A JS/Exploit.Agent.AFH fertőzött weboldalak kódjába rejtett JavaScript program, amely védtelen számítógépek biztonsági hibáját használja ki. A JS/Exploit.Agent névre keresztelt károkozó a terjedéséhez egy már korábbról jól ismert Microsoft sebezhetőséget is képes kihasználni (egészen pontosan az MS99-042 nevűt, melynek leírása a http://www.microsoft.com/technet/security/bulletin/ms99-042.mspx címen található).
A kártevő a támadó részére a webes látogató gépéhez hozzáférést biztosít, onnan fájlokat olvashat ki és módosíthat. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Esetleges fertőzés és mentesítés után érdemes a webböngésző átmeneti tárolóját (Temporary Internet Files mappa) is kitörölni, valamint a szükséges Windows biztonsági javításokat haladéktalanul telepíteni.

-

A számítógépre kerülés módja: böngészés közben automatikusan letöltődik a felhasználó hiányos védelemmel rendelkező számítógépére.
Bővebb információ: http://www.eset.hu/virus/js-exploit-agent-afh

7. Win32/Agent trójai
Elterjedtsége a májusi fertőzések között: 2.82%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

8. WMA/TrojanDownloader.GetCodec.gen trójai
Elterjedtsége a májusi fertőzések között: 2.82%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

9. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a májusi fertőzések között: 2.62%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszó adatok titokban való továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

10. Win32/Delf.NFB féreg
Elterjedtsége a májusi fertőzések között: 2.52%

Működés: A Wind32/Delf.NFB féreg egy PECompact segítségével összetömörített kártevő, amely lefutva különböző fájlokat (pl. sRpcS.dll, RpcS.exe, hma.exe) hoz létre a Windows\System32 alkönyvtárban. A fertőzés során módosít bizonyos Registry kulcsokat is, amelyek az RPCS (Remote Procedure Call System), azaz a távoli eljáráshívásokkal kapcsolatosak, és elindít egy szervizfolyamatot windows_0 vagy RpcS néven a memóriában. Tevékenysége során további kártékony kódokat igyekszik letölteni Kínában bejegyzett weboldalakról.

A számítógépre kerülés módja: fertőzött külső adattároló csatlakoztatásakor az automatikus futtatás funkció segítségével.
Bővebb információ: http://www.eset.hu/virus/trojandropper-delf-nfb-1

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1186176

Kommentek:

Nincsenek hozzászólások.

PDF: csak megnyitom, és már indulok is...

2009.06.16. 22:03 | Csizmazia István [Rambo] | 1 komment

Címkék: biztonság kód pdf virustotal kártékony

A mai exploitokkal terhes, vérzivataros időkben érdemes lehet a szimpla rákattintás helyett megvizsgálni **a kapott, e-mailben érkezett, weboldalon található PDF állományokat**, mert az ördög nem alszik.

Minden állomány fejléc- és fájlszerkezetében lehetnek olyan értékek, amik lehetőséget adnak barkácsolásra, trükközésre, exploit kód vagy kártékony JavaScript program beillesztésére. Nem kivételek ezalól a manapság annyira népszerű PDF, azaz Portable Document Format alapú fájlok sem. Pontosan emiatt **került be a VirusTotal eszközei közé a PDFiD nevű alkalmazás**, amellyel kontrollálhatjuk, van-e gyanús adatsor a megnyitni kívánt állományban. A PDFiD a PE EXE fejléc elemző segédprogramokkal szemben nem egy valódi elemző (parser), hanem **ismert, veszélyes stringrészleteket keres**, és aztán ennek alapján értékeli ki az állományt.

Nemrég olvashattunk arról, hogy egy vírusirtó programnál a PDF feldolgozó modult javítani kellett, mert csak "bambán" kereste a "%PDF" karaktersorozatot, amelynek megtalálása után kezdi a kiértékelést. **Ha esetleg egy manipulált PDF-ben nem volt ilyen**, akkor például a Kaspersky program **nem ismerte fel PDF-ként a vizsgálandó állományt**.

Egyébként nem segít mindig pusztán az alternatív PDF olvasók használata sem, bár az Adobenál jobban járunk vele a sebezhetőség és a sebesség tekintetében is, de sérülékenységek természetesen vannak a Foxit Readerhez is. Sőt, **az Adobe és a Foxit az offset értékeket figyelmen kívül hagyva vígan megnyit** piszkált fejlécű PDF állományokat is, és sajnos a bennük lévő JavaScript kódokat is lefuttatja.

Érdemes lehet megkérdezni orvosunkat-gyógyszerészünket, illetve kicsit Microsoftosan fogalmazva kizárólag megbízható (hehe) helyről származó PDF-eket **nyissunk csak meg - legalábbis nekifutásból** -, míg a kérdőjelesek járjanak el előtte egy násztáncot a VirusTotalon, és csak az eredmény ismeretében bökjünk a megnyitásra.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1188420

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.19. 20:31:34

Emelkednek a PDF támadások a statisztikák szerint:
blogs.technet.com/mmpc/archive/2009/06/17/pdf-e-ducation.aspx

Adok-veszek-cserélek bűnözőknek

2009.06.17. 12:09 | Csizmazia István [Rambo] | 8 komment

Címkék: adatok kereskedelem lopott botnet

Biztonsági kutatók nemrég egy olyan weboldalt fedeztek fel, amelyen úgy **kereskedtek a bűnözők a különféle kategóriákban lopott adatokkal, botnet kapacitással**, akár egy kereskedelmi E-bay portálon.

A hackerek közti piactéren vásárolható vagy bérelhető kártékony kódok rendszerint **igyekeznek elbújni a kereskedelemben kapható biztonsági programok elől**, így olyan eszközökkel találkozhatunk bennük például, mint a titkosítás vagy a kódösszezavarás (obfuscating).

Természetesen nem csak az oldalon kapható kódok trükkösek, **magának a weboldalnak is olyanok a tulajdonságai, hogy a szakemberek számára minél nehezebben követhető legyen**. Az oldal adminja éberen figyel a fürkészési kísérletekre, és ha biztonsági céget sejt a háttérben, azonnal letiltja, feketelistára teszi. Különféle proxyszervereket is használnak annak érdekében, hogy **a biztonsági szakembereket valamint, a bűnüldöző szerveket lehetőség szerint távoltartsák**.

A jelenségről beszámoló Yuval Ben-Itzak, a Finjan kutatója szerint **igen élénk forgalom tapasztalható a weboldalon**, vagyis van komoly érdeklődés az ilyen árucikkekre. Abban tehát **nem érdemes bízni, hogy a számítógépes bűnözők nehezen tudnának** ilyen eszközökhöz vagy erőforrásokhoz hozzájutni.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1190405

Kommentek:

tbalazs · http://www.eloszto.hu 2009.06.17. 14:49:40

Kíváncsi lennék, hogy összesen már mennyi pénznél tartunk amit a kedves adathalászok nyúlnak egy év alatt. Szerintem igen tetemes összegről beszélünk

nemuccaszoc 2009.06.17. 14:57:25

De az átlag mp3-at töltő usert még jobban meghúzogatják adott esetben, az ilyet meg el se kapják.

fireman4 2009.06.17. 15:54:30

WEB címet akarunk.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.17. 16:24:29

hehe, www.botnet_bankkartya_adok_veszek_occsoert.com ;-)

foobared 2009.06.17. 16:27:24

De ez IRC!!! :D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.17. 20:15:51

Sorry vagyok a hegyről, Icuka csak illusztráció volt. Az eredeti webhelyről sajnos egyelőre egyáltalán nem találtam screenshootot :-(

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.18. 08:37:14

Közben találtam már bővebb infot is, Golden Cash Network a neve:
news.cnet.com/8301-1009_3-10266977-83.html

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.06.24. 14:03:35

A Finjan által közzétett árlistán Magyarország is szerepel: hazánkban 1000 fertőzött számítógép 20 dollárt ér
biztonsagportal.hu/online-vasarlas-alvilagi-modra.html

URL rövidítés és átkampózás

2009.06.18. 22:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: link incidens url rövidítés cligs sablan

A minap érdekes cikket lehetett olvasni arról, hogy az egyik URL rövidítés szolgáltatót **feltörték, és az általuk közvetített linkeket lecserélték másikra**.

Az URL rövidítés lényege, hogy bármilyen kacifántosan hosszú linkből képes egy rövidke, akár a twitterhez szükséges max 160 karakterbe beférő új linket generálni. Vagyis ha eredetileg a

http://www.vitez.nagybanyai.horthy.miklos.legkedvesebb.matroza.com/kipreparalom.html

lenne, akkor az új lehet akár egy ilyen nyúlfarknyi is:

http://cli.gs/abcdEFG

Az áldozatul esett Cligs a negyedik legnépszerűbb ilyen cég, amelyet a Twitteren rövidítésre használnak. Persze emellett **a spammerek is nagyon kedvelik ;-)** A mostani tettesek egy biztonsági hibát kihasználó exploit kód segítségével hatoltak be, és változtattak meg linkeket nagy mennyiségben.

A dolog **szerencsére mintha egy Proof Of Concept akart volna lenni, nem járt jelentős károkozással**, de ha azt nézzük, hogy 2.2 millió kattintásra váró link változott meg nagy hirtelen az akció keretében, azért félelmetes. **Lehetett volna akár 2.2 millió kártevőre mutató link is** ez, nagyon valószínű, hogy az elkövető ezt szándosan nem lépte meg valamilyen rejtélyes okból (talán Márta nap volt, és az illető olvasta Az elátkozott part című Rejtő könyvet). A Márta napnak hála **így viszont 2.2 millió link Kevin Sablan blogger oldalára mutatott** a freedomblogging.com weblapján. A Cligs egy nyilatkozatban tájékoztatta a felhasználókat az esetről, és a linktartalmakat korábbi mentésből voltak kénytelenek helyreállítani. Ez kissé döcögősre sikeredett, mert állítólag nem rendelkeztek rendszeres napi mentésekkel.

Nagy figyelmeztetésnek értékelhetjük az esetet, és van új a nap alatt. Amiből akár arra is gondolhatunk, hogy **az ilyesfajta akciók skalpként és eredményességben is vonzó cél lehet a jövőben** a rossz fiúknak. Graham Cluley szerint a jövőre nézve esetleg jó megoldás lehetne egy olyan böngésző plugin, amely képes a rövidített link mögé pillantva kérésre megmutatni annak eredeti tartalmát.

· 1 trackback

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1193294

Trackbackek, pingbackek:

Trackback: HTML Info **2009.06.18. 17:30:59**

Rövid URL - jó nekünk?Egyre inkább divatossá válik a rövid URL-ek használata. Van, aki “előzékenységből”, más “kényszerből” használja. Az URL rövidítő webes szolgáltatások mindenesetre élnek, virulnak, köszönik, jól vannak. A We...

Kommentek:

Nincsenek hozzászólások.

Nindzsák és szamurájok

2009.06.19. 20:12 | Csizmazia István [Rambo] | 4 komment

Címkék: spam kanadai levél kínai szamuráj nindzsa kéretlen gyógyszerész

Obi-Wan Kenobi szerint "**Harcolni sokféleképp lehet**". Nincs ez másként a kéretlen e-mail üzenetek küldőinek világában sem, akik vágynak arra, hogy levelük érdeklődést és rákattintást váltson ki.

Egy régi Hofi viccben a katona élményekről volt szó, mikor is az őrmester furmányos kérdéseket tett fel az újoncoknak: "Emberek, kinek van itt gépjárművezetői jogosítványa?", "Emberek, ki szeret olvasni?" vagy "Emberek, ki tud itt rajzolni?". Azonban a jelentkezők rendre hopponmaradtak, mert a beugrató kérdés után a szabvány válasz mindig ez volt: "Oké, akkor indulás, takarítsa ki a vécét". Egyszer új őrmester érkezett, aki felsorakoztatta az újoncokat és megkérdezte azokat: "Emberek, ki akarja kitakarítani a WC-t?" Mindenki meglepődött, és úgy érezte, eljött az ő ideje, akkor ehelyett biztos valami kellemes feladat várható. A jelentkezőnek azonban végül ezt mondták: "Nagyszerű, örülök hogy önként jelentkezett, akkor lehet is indulni takarítani, ott a vödör és a rongy!".

Sokszor és sokat foglalkoztunk már spamekkel, kanadai gyógyszerész oldalakkal, és azt a végkövetkeztetést vontuk le akkor, **nekünk igazából semmi szükségünk kínai (.CN) oldalakra való kattintásra**, lehetőség szerint érdemes ettől tartózkodni. Állítólag az ember attól ember, hogy ugyanazt a dolgot más nézőpontból is tudja látni, ennek függvényében újra tudja értékelni, **új tartalmakat és összefüggéseket képes az egyszer már megismert jelenségek mögé látni**. Einstein például szeretett hegedülni, és önéletrajzi könyvében azt írja, aki besavanyodik és csak a saját szakterületére szorul be, az sosem tud olyan jó gondolatokra jutni, mint aki nyitott és befogadó az élet minden területére. Ekkora babérokra mi nem törünk, csak egy aprócska levélkére nézünk rá. **Ezúttal a kanadai gyógyszerész oldalakra mutató levelek két archetípusát mutatjuk be, ami a post címét is ihlette.**

Az első **trükkös ninja versenyző kőkeményen becsap minket**, azt állítja, ott vannak az interneten a fényképeik valahol, és hogy állítólag fel is iratkoztunk valamilyen Riqpi nevű szolgáltatásra. Csellel arra csábít, kíváncsiságunknak engedve kattintsunk. Ám **mindegy mit szeretnénk, a megerősítés és a nem működő leiratkozás egyaránt a gyógyszerész oldalra visz**. Nem mellesleg látszólag saját e-mail címünkről érkezett a küldemény.

A másik levél sem mentes ugyan egy kis cseltől, de itt **szemtől szembe őszinte szamuráj mentalitással megkapjuk az arcunkba már a levél tárgyában: "Medication refills"**. És a feladó címe látszólag is és valójában is megegyező: Barbicana ő, nincs itt kérem semmi titkolódzás. Bár az igazi link el van ugyan rejtve egy audiomarket.com-os cím közbeiktatásával, de ennyi belefér, valóban azt kapjuk, ami a subject: megintcsak Kínában, a szokásos pasztillák társaságában kötünk ki. **Jó lenne látni egyszer egy statisztikát arról, vajon melyik harcmodor az eredményesebb**. És **állítólag tényleg élnek a Földön olyan élő hús-vér Homo Sapiensek, akik valóban vásárolnak** ezekből :-O Persze amikor valaki rakétából akar kerítést hegeszteni magának - és életbenmaradásával egyúttal kizárja magát a Darwin díjból - már semmin sem csodálkozhatunk.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1194837

Kommentek:

Pomme 2009.06.20. 00:09:03

Lécci ne használjátok már ezt a "gyógyszerész" jelzőt, a hamis gyógyszert áruló spammerek és csatolt bűnbandáik hol gyógyszerészek már?

bécsi pszicho · http://www.flickr.com/photos/haazee 2009.06.20. 07:03:50

"És állítólag tényleg élnek a Földön olyan élő hús-vér Homo Sapiensek, akik valóban vásárolnak ezekből :-O"

Mit gondolosz, miből táplálkozna a Darwin-díj legendája, ha nem lennének ilyenek? :D

DownQ · http://letoltes.freebase.hu 2009.06.20. 10:04:49

Sok hülye van, ez tény!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.23. 17:49:03

Szia Pomme!

Köszi a hozzászólást. Nem akartuk megbántani az igazi gyógyszerészeket. de ez a szóhasználat terjedt el a szakmában. Javasolhatnál esetleg helyette valamit, addig is idézőjeles formában fogom használni.

Opera nyitány a botnetek felé?

2009.06.22. 20:38 | Csizmazia István [Rambo] | 3 komment

Címkék: opera biztonság fájlmegosztás kockázat unite

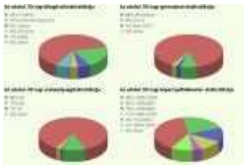
Sokak kedvence és méltán népszerű a multiplatformos (Win, Linux, Mac) Opera alternatív böngészője, amely ha nem is mondhat magáénak akkor tábort, mint a Firefox, de mindenképpen jelentős szereplő. Most az új tizes verzióval olyan **újdonságokat készülnek bevezetni** köztük az Opera Unite-tal, ami túlmutathat a készítők eredeti szándékain.

Jónéhány évvel ezelőtt Németországban a biztosítók az akkoriban még újdonságnak számító légzsákkal rendelkező autók biztosítási díját eleinte egy ideig magasabb összegben jelölték meg, mint a többi járművét. **A furcsa döntés oka az volt**, hogy zömmel fiatalokból álló bandák ráálltak a légzsákos autók rendszeres lopására, és azokkal pedig szándékosan falnak vagy fának hajtottak, és **így gyűjtötték a "skalpokat"**: ki hányszor kockáztatott, ütközött és úszta meg ép bőrrel. A TV-ben később - bár az autógyáraknak ez nem volt különösebben jó reklám - **pontosan emiatt bemutattak** egy olyan balesetet, ahol nem nyílt ki a légzsák, és a sofőr meghalt. Ezzel is figyelmeztetni próbálták a felelőletlen autótolvajokat. Itt volt tehát egy eredetileg jó ötlet: baleset esetén a légzsák megmenti az életet, **de volt egy ezzel ellentétes ötlet és másmilyen használat**: szándékos adrenalin emelés, virtuskodás, a kis százaléknyi meghibásodást is beszámítva még akár az életük kockáztatásával is.

Megvan ez a fajta leleményesség a számítástechnikában is. Ha még emlékszünk **a kártevők sokszor használnak ki olyan ritka, rejtett tulajdonságokat, funkciókat, amelyeket tervezőik eredetileg más célra szántak vagy nem is gondoltak rá**. Említhetjük például a companion vírusokat, ahol a CEB szabály alapján az azonos nevű állomány akármi.bat, akármi.com és akármi.exe közül mindig a COM, majd az EXE és utána az BAT kiterjesztésű állomány próbál meg elindulni.

De amint azt a Vista esetében láthattuk, még egy egyszerű animált kurzor fájl is lehet a fertőzés forrása. Bármilyen zseniális újdonság is jelenik meg ugyanis manapság, a fejlesztőknek **muszáj (lenne?) számot vetniük a "mire lehet ezt még (ki)használni" kérdéssel is**, mielőtt még valakik előttük és helyettük teszik meg ugyanezt.

Olvashatjuk, hogy az új Opera hibrid p2p Unite funkciója képes webszerver futtatási lehetőséggel felruházni a böngészőt, ám ezzel nem csak nagyszerű lehetőségek nyílnak meg, **mint például fotómegosztés, médialejátszó, chatszerver**. Már az is jó kérdés, hogy a Windowshoz hasonlóan nem lesznek-e majd olyanok, akik tudtukon és akaratukon kívül megosztják majd a gépüket másokkal. De a legfontosabb talán mégis az, hogy a proxyn keresztül folyamatos fájlmegosztással bármilyen szándékú felhasználók is terjeszthetik a saját tartalmait, és ez akár kockázatos is lehet.



A még alfa fázisban lévő alkalmazás fejlesztői remélhetőleg méltányolják majd a biztonsági cégek ezirányú figyelmeztetéseit, addig is kíváncsian várjuk a végleges megjelenést, és hogy valóban beváltja-e a hozzáfűzött reményeket.

Aztán **hogy valóban lesznek-e majd ilyen irányú próbálkozások, visszaélések** a kártevőterjesztők részéről, nem tudjuk, de sejtjük, ezért addig is megtesszük a fogadásainkat tétre, helyre, befutóra.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1200574

Kommentek:

Közöd?? (törölt) 2009.07.04. 08:43:40

remélem lesz az operából unite nélküli változat, ha nem akkor számomra az opera halott

Nameless® · http://dirtywindows.hu/ 2009.07.04. 15:21:53

úristen... a unite kivan kapcsolva nem fog bekapcsolni... Megint egy hozzáértő megírta ezt a barom cikket.. A unite nem működik ha nincs opera accountod. Be kell jelentkezni hogy veszélynek tedd ki magad .. nem hinném hogy pont az operaát fogják tamádani.. Nem értem hogy minek kell egyártalán számításba venni a tudatlanokat... azok nemhogy operát még a firefoxot se ismerik.. maradnak az ie6 nál

atomgoa 2009.07.04. 16:15:16

Nameless_nls@ soha nem lehet tudni...egy "tudatlan" számítógépén sok minden megtörténhet, akarata ellenére. én is várom a fejleményeket, opera használó vagyok, bár unite egyelőre nem mozgatta meg a fantáziámat.

Állásügyben jöttél? Akkor kérjük a jelszavaid!

2009.06.23. 16:35 | Csizmazia István [Rambo] | 3 komment

Címkék: adatvédelem állás magánélet közösségi oldalak jelszavak adathalász bozeman

Hihetetlen történetek rovatunkban most egy olyan sztori következik, amit első olvasás el sem akartunk hinni. **Sajnos mégis igaz, következzen a szomorú valóság a "demokrácia őshazájából"**.

Az állásra jelentkezőktől Bozeman városában (USA, Montana) rendszeresen elkérték a jelentkezők weblapokhoz, közösségi oldalakhoz tartozó belépési adataikat - úgynevezett "háttér ellenőrzés" céljából - vagyis **nem csak a neveket, hanem hozzá a jelszakat is**. (A kutya oltási bizonyítványának számát azonban nem is kérték ;-) A törvénysértő gyakorlat egy jelentés nyilvánosságra hozatala után váltott ki heves felzúdulást a városban. A tiltakozók között felemelte szavát az Electronic Frontier Foundation (EFF) is. A **botrány kirobbanása után az érintettek közleményt adtak ki**, melyben az eddigi gyakorlat megváltoztatását is bejelentették.

Most készülnek arra, hogy a Homárdíjas és példátlan eset kapcsán megpróbálják orvosolni a helyzetet, **és jelezzék az érintett álláskeresőknek, haladéktalanul változtassák meg kiadott jelszavaikat**. (Magunk közt szólva, ha valaki a munkahelyén csak egyszer is belép a privát postájába vagy egy közösségi oldalra, már bebukta, mert a proxyból bármikor elővehető az account, de akár ugyanez lehet a helyzet akkor is, ha technikailag a munkahely biztosítja az otthoni internet elérést.)

Belegondolni is rossz, mennyi **visszaélésre adhat lehetőséget az ilyen kiszolgáltatott adat**, sőt egy rosszindulatú alkalmazott machinációja vagy az adatok elvesztése esetén **igazi katasztrófával is szembesülhetnek a szerencsétlen munkakeresők**.

Ha csak messziről, szigorúan technikai szemmel nézzük, akkor bátran megállapíthatjuk, hogy **ezzel a jogellenes kéréssel az érintettek igazi adathalászként viselkedtek**. Okulásul kéne nekik egy horog, esetleg pont egy bal, vélhetően valamelyik Klicskó fivér be is vállalná a szabadidejében ;-) Most viszont talán a nyilvánosságtól kapnak eleget, reméljük, tanulnak belőle, innen kívánunk sok sünt nekik.
Hamarosan meg amúgyis jönnek az olyan munkahelyek, ahol már nemcsak a jelszavainkat kell majd előre megadni, hanem csak és kizárólag DNS mintával lehet majd pályázni az állásra ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1203114

Kommentek:

atko 2009.06.23. 17:37:42

Régebben azt gondoltam, hogy a Gattaca csak egy fikció. Mára már másként gondolkodom erről. Sajnos ma már ünnepelünk, amikor egy kutyát 6 példányban ajándékoznak önmagának. És új lenyomat kell ahhoz is, hogy legyen egy útlevelem. A telefonom tudja hol van a legközelebbi automata, vagyis tudja, hogy én hol vagyok. És ez még csak a kezdet.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.23. 17:50:41

És hogy mennyire nem fikció ez az egész, a demokráciák éppen megtiltják, nálunk meg éppen bevezetik:
index.hu/tudomany/genadat802/

atko 2009.06.24. 09:07:57

Ezen én akkor sem csodálkoztam, mert nálunk a parlamentben nem vitáznak csak szavaznak, azt amit a frakció előtte ilyen-olyan érdek mellett elfogad.
Az én személyes génjeimet biztos helyen tartom, az utódomban.
:-) remélhetőleg ő is továbbadja és akkor örökké élek majd és csak röhögök a sok birkán :-)

Siralmas eredmények a közösségi oldalakon

2009.06.25. 18:21 | Csizmazia István [Rambo] | 14 komment

Címkék: biztonság felmérés lustaság közösségi oldalak webroot

A Webroot egy átfogó, mintegy **ezeregyszáz Facebook, MySpace, Twitter, Linkedlin oldal felhasználóját kérdezte ki** egy felmérés keretében. Az eredmények alapján elmondhatjuk, **az óvatósság sajnos nem igazán jellemző**, sokan adnak fel itt magas labdát.

Mint a mogyorós csokik csomagolásán található szófordulattal élve, itt is hasonló arányokat látunk a biztonságtudatosságra: "nyomokban előfordul", de sajnos abszolút **nem ez a többségre jellemző**. A most megjelent értékelés az alábbiakat tapasztalta:

- a válaszadók **kétharmada egyáltalán nem korlátozza a személyes profiljában olvasható részleteket**, amik így akár egy Google keresővel is láthatóak
- több, mint **a fele (59%) nem tudja biztosan, kiknek is engedélyezte** pontosan profilja megtekintését
- körülbelül **egyharmaduk (32%) adott meg legalább három személyes** azonosításra alkalmas információt
- **egyharmaduk (36%) ugyanazt a közösségi portálon használt jelszavát máshol is használja**
- **egynegyedük (28%) fogad el barátkérőt idegentől**

Más mutatók sem festenek szebb képet. Az igaz, hogy **78% aggódik személyes adatai miatt, de ugyanakkor 30% nem rendelkezik vírus- és kémprogram védelemmel**.

A korosztályok közt **a fiatalok számítanak a legveszélyeztettebbnek**, az átlagos 28% értékkel szemben náluk 40% fogad el barátkérőt idegentől, és náluk **sokkal jellemzőbb az összes személyes adat, elérhetőség megadása is**.

Jól látható, hogy **a közösségi oldalak egyre jobban a kártevőterjesztők célkeresztjébe kerülnek**. Kártevők, csalások, hamis linkek, átveresék ugyanúgy kifizetődnek itt is, mint az átlagembereknek küldött adathalász levelek: elegendő csak 5%, aki lépremegy, és a tetteseknek már bőségesen megéri. És a legalább 5% sajnos pontosan ezt teszi. Mi mást is javasolhatnának végül, mint **a személyes adatok ésszerű korlátozását, gyanakvást az idegenekkel szemben, rendszeres frissítéseket, biztonsági szoftverek használatát, valamint egyedi jelszavak alkalmazását mindenhol**.

Persze igaz, **ezek az erőfeszítések, jelszócserék, minden helyen más jelszó használata munka, teendő, odafigyelést igényelnek**. De akárcsak a mentések készítésénél, **megtérül a befektetés, ha legyőzzük a lustaságunkat**. Amit pedig érdemes legyőzni, ha nem akarjuk veszélynek kitenni magunkat. Végezetül ha már a lustaság szóbakerült, egy idevágó idézettel zárunk:

"A nyár az az évszak, amikor túl meleg van ahhoz, hogy elvégezzük azt, amihez télen túl hideg volt."

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1207298

Kommentek:

Flashzee · http://www.flashzene.com 2009.06.25. 19:09:22

Csak olyat szabad feltenni, amit úgy érzünk, nyilvános!

lifelike 2009.06.25. 19:10:25

1db kep, semmi mas nem kell
aki felrak minden szart az se 100as

nemuccaszoc 2009.06.25. 19:49:32

Idősebb korosztály még normális, de a fiatalok nem ismernek határokat.

szilvacska 2009.06.25. 20:37:28

iwiwen 80-90 kép profilon, 30 db ugyanakkor készült, sorozatképek, csak más szögből. szánalmas

másik: fürdőszobában fotózza magát meztelenül, persze érdekes részeket takarja, dehát meglátja ezt tanárbácsé,néni.. jaj, fiatalok

algi 2009.06.25. 23:00:24

Nálam az az első, hogy a kényesebb ismeretségeknek utánajárok. Derült már így ki pszichológusról, hogy vállalkozó az erotikus iparban.

PicÚr 2009.06.25. 23:58:08

be kell állítani, hogy tényleg csak a barátaid láthassanak mindent és az meg már mindenkinek a saját hülyesége ha elfogad olyan embert aki nem is a barátja, akkor minek használja az oldalt... -.-'

grigorij (törölt) 2009.06.26. 08:00:37

Önmagában ostobaság az ilyen oldalakon megjelenni!
Ez nem más, mint magamutogatás egy fajtája!
Ez a nem védem dolog, meg pont olyan, mint amikor egy jó bszaás közben felveszük az aktust, majd meglepődünk, ha a szakítás után azok felkerülnek a netre...
Ohhh...

algi 2009.06.26. 08:20:27

@grigorij: És a blogokon kommentelés az mi a lópikula?

Andie 2009.06.26. 08:53:25

Kicsit szenzációhajhász az indexes ajánló cím :)
Amúgy Rambó, irtam neked mailt kb fél éve. Ilyen ritkán nézed a mailjeidet, vagy csak simán elfelejtettél válaszolni? :)

hatR 2009.06.26. 09:11:01

nem lehet hogy a 30%, aki nem hasznal virusirtot, az mind osx-el nyomul? :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.26. 11:26:14

@Andie: Szia!

Az Indexes ajánló címet nem én szoktam írni, beleszólásom sincs, az már az ó reszortjuk.

A levéllel kapcsolatban meg mélységes elnézést, kínosan ügyelni szoktam, hogy mindenkinek válaszoljak. Gyorsan keresgéltem, de nem találtam meg az üzeneted. Megteszed, hogy elküldöd újra, memgírem VIP figyelemmel fogok rá ügyelni :-) Mégyszer nagyon sajnálom.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.06.26. 11:29:21

@hatR: Szia!

Én nagyon örülnék ennek, ha Mac és a Linux ekkora tortaszeleten osztoznának, de szerintem ez sajnos kisebb. Mindenesetre a Windozosoknak van a legtöbb félnivalója, ez nagyon is igaz.

A személyes adatoknál pedig indiferrens az OS, akár SUN Sparcról is beírhatja valaki a személyi számát, és a TB kártyája azonosítóját.

Andie 2009.06.26. 11:53:20

@Csizmazia István [Rambo]: Tudom, hogy nem te irtad a cimlapos mottót, csak megjegyeztem, hogy szokás szerint elég figyelemfelkeltő lett :) (ami nem baj a blognak!)
A levelet már nem találom, de meg is oldódott a kérdés, valami számomra ismeretlen virusos dolog volt (IE a háttérben elindult, és hangokat, reklámokat játszott le)
Azért megnyugtattál, hogy olvasod a leveleket, igy legközelebb is veszem a bátorságot, és irok neked, ha nyügöm van.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.06.26. 11:58:56

@Andie: Örülök, hogy ilyenkor sokkal többen olvassák a blogot :-D Én sem panaszkodom addig, amíg a "Vírusos noteszgépek a Tescoban"-t nem "Döbbenet: Kiszely Tünde a trolibuszon villantott"-ra konvertálják ;-)

Jelezz bátran ha lesz valami, megpróbálok segíteni.

Kell egy barát

2009.06.29. 14:25 | Csizmazia István [Rambo] | 1 komment

Címkék: microsoft windows frissítés biztonság inspector secunia

A **Windows biztonsági frissítések és egyéb használt alkalmazások javításainak dzsungelében jól jön egy kis automatizált segítség**. Az ember feje nem káptalan, képtelenség ennyi mindent naprakészen kezelni. Szerencsére vannak ebben segítő programok, az egyik legkedveltebb a Secunia Personal Software Inspector (PSI), melyből nemrég érkezett meg a legújabb változat, amely **már magyarul beszél** és sírva vígad.

Röviden összefoglalva **a program képes feltérképezni az operációs rendszerünket, valamint az alkalmazásainkat**. Ha ezekből frissebb verzió vagy javító folt érhető el, erre figyelmeztet, sőt kattintható link formájában azonnal le is tölthetjük és telepíthetjük.

Németh Balázsnak hála - ezúton is köszönjük neki a munkáját -, ezentúl már magyar nyelven is használhatjuk a programot, amely emellett számos újdonságot is tartalmaz. Mostantól **a 64 bites rendszereket is támogatja**, bekerült egy úgynevezett PSI Worldmap, amellyel országok, kontinensek és földrajzi régiók **frissítésekkel kapcsolatos állapotát** kísérhetjük figyelemmel. Javítottak a lokalizált Windowsok működésén is, ezzel korábban voltak kisebb problémák az ázsiai, afrikai és dél-amerikai rendszerek esetén. Akit részletesen is érdekel, a teljes changelog lista ezen a helyen érhető el.

A technikai javításokon és újításokon felül **kisebb memóriahasználatot és a kedvezőbb sebességet is ígérnek** az új változat használóinak, amely magánfelhasználók részére **továbbra is ingyenesen tölthető le és használható**. Remélhetőleg sokan fedezik fel és kapnak rá az ízére a vírusirtó mellé. Jó étvágyat hozzá!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1210495

Kommentek:

cworm (törölt) 2009.06.29. 15:10:46

a screenshot-ok alapján végezhetett volna jobb munkát is a fordító.:P a csapata szóból hiányzik egy a betű, meg azt sem értem, hogy mi az a "Javítva Fenyegetettség"...

Buszsáv bírság ellen Conficker féreg

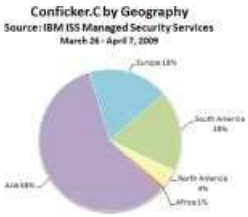
2009.07.01. 19:25 | Csizmazia István [Rambo] | 3 komment

Címkék: költségek birság féreg közlekedési mentesítés conficker

Kicsit a "sárkány ellen sárkányfű" analógiára rímel a főcím, de inkább az domborodik ki az egészből, hogy a **kártevő támadás esetén néha milyen egyéb járulékos anyagi kockázatokkal vagy a másik oldalról szerencsével** lehet még számolni.

Vírustámadás után a **mentesítés, esetleges újratelepítés, külsős szakértők alkalmazása és a folyamatos ügymenetben elszenvedett kényszerszünet** költségeinek bekalkulálása ugyebár eddig is evidencia volt. **Most viszont itt a be nem szedett bírság miatti veszteség keserű pirulája a hivatalnak**, és ezzel párhuzamosan a megkönnyebbült sóhaj a közlekedési kihágók részéről.

A **Conficker féreg támadása miatt a Manchester városban szabálytalanul közlekedők** - ebben szerepel a címadó buszsáv illetéktelen igénybevétele is - nem kapták meg a törvényben előírt 28 napos határidőre a bírságról szóló értesítést, így **a hivatal elesik mintegy 43 ezer angol fontnyi (körülbelül 13.7 millió HUF) bevételtől**.



Azért, **hogy ne legyen minden ennyire szép** (ugye a kedvenc mondása Lincoln elnöknek, hogy "Ingyen ebédet még senki nem evett"), kiderült, hogy a mentesítésre, tanácsadásra nem elhanyagolható mennyiségű adófizetői pénzt fordítottak. Ilyen tételek olvashatók benne, mint 1.2 millió GBP (382 millió HUF) IT kiadás, benne 600 ezer GBP ((191 millió HUF)) tanácsadói díj, beleértve például a Microsoft szakértőinek részvételi költségét is. Ezt a nem kicsiny összeget olvasva esetleg kicsit a magyar tender, pályázati, offshore és egyéb viszonyok ugorhatnak be, de rossz, aki rosszra gondol ;-)

Az is érdekes, hogy az eset előtt két héttel elveszítettek két titkosítás nélküli laptopot, rajta 1754 helyi dolgozó személyes adataival. Lehet, hogy a BSA, VPOP, stb. mintájára kellene egy adatvédelmi kommandót is létrehozni, és ha a hivatalok nagy ívben tesznek a kötelező titkosításra, nem tartják be a rendelkezéseket, akkor lecsapna az adatvédelmi akármi hivatal valami gigászi bírsággal (a földgolyó több évi búzatermése például). Mondjuk Angliában ez akár tuti üzlet lehetne, **hiszen minden héten ellopnak, elhagynak valamilyen titkosítatlan kormányzati adathordozót vagy noteszgépet**.

Mindenesetre a közlekedési kihágási **bírság elmaradása miatt mintegy ezerhatszáz vezető könnyebbülhet** most meg, és talán ha lenne szobra a Conficker féreg írójának, mostanában egy csokor friss virágot meg némi aprót is elhelyeznének rajta, random mécsesgyújtással kiegészítve :-)

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1219805

Kommentek:

Vidi Rita · http://www.hosnok.hu 2009.07.02. 15:45:26

:)))
már úgyis bennevagyok a kommandózásban, betársulsz István? :)

Nekem hónapok óta az az érzésem - válság óta -, hogy nemcsak, hogy nem tud számolni az emberiség, de nem is akar!

Való igaz, amíg ezekértnem kaphatnak büntetést, addig majd valaki kicsengeti a lóvét..

A megelőzés meg a legeladhatatlanabb szolgáltatások egyike.. Kár..

Vidi Rita · http://www.hosnok.hu 2009.07.02. 15:46:07

Egyébként szavaztam a blogra goldenblogon. Nem mondom meg, hányast adtam ;)))

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.02. 16:43:23

Szia!

Köszi, rendi vagy, de tisztában vagyok a reális esélyeimmel... Azért még színes tintákról néha álmodom :-)

Michael Jackson holtában sem pihen

2009.07.02. 19:12 | Csizmazia István [Rambo] | 1 komment

Címkék: spam michael jackson kártevő halálhír

Nem, most nem arra gondolunk, amikor állítólag felül a helikopterben, és amikor állítólag mégsem halt meg, és állítólag a Grönlandra készült. Ezúttal **a szerencsétlen ember halálát kihasználó kártevő terjesztők írják az újabb fejezeteket**.

A maga nemében páratlanul tehetséges zenész extrém szokásaival, titkaival és egész magánéletével olyan viharokat kavart, ahol a bulvár média nyugodt lélekkel rendezkedhett be ezek hosszútávú szellőztetésére vagy puszta kitalálására - nem tudhatjuk. Most, hogy már nincs az élők sorában, nincs ám vége a műsornak, hamis boncolási jegyzőkönyvek jelennek meg, és a **kéretlen levelek indulnak hosszú sorokban, sőt kártevőt terjesztő új weblapok is elkezdik áldatlan működésüket**.

A Sophos cég arról számolt be, hogy sarah@michaeljackson.com oldalról olyan hamis e-mail üzenetek indultak el, **amelyek kártevőt terjesztenek** (esetleg Sarah Connor írja a jövőből?!). Angolul tudók már a "Rememebring"-nél felnyeríthetnek, akárcsak a "doors opening" helyetti Doors koncert esetében ;-) Az mindenesetre igen jellemző, hogy **a hamisított levelek számos helyesírási hibával látnak napvilágot**, ez is lehet egyfajta mankó a felismerésben. Aki rajongóként a michaeljacksonsongandpictures.doc.exe levélmelléklet állománnyal találkozik, az azért **legyen felkészülve egy alapos csalódásra**.

Emellett a Sunbelt blog is tudott újat mutatni, ők pedig egy Ki ölte meg Michael Jacksont tárgyú levélre hívták fel a figyelmet, ahol a linkelt weboldal exploit kódot tartalmaz. Az F-Secure pedig egy képmegosztó oldalakon feltűnt olyan hamis képet fülelt le, amely valójában egy rosszindulatú EXE állomány, és **számos helyre feltöltötték a gyanútlan áldozatok megtévesztésére**, például Facebookra, MSN-re, Orkut-ra.

Van egy fogadásunk arra is - és ez persze már nem vírushír, hanem csupán lehetséges üzleti és ügyeskedési trükk - hogy **az ilyen állítólagos ismeretlen és eddig kiadatlan dalok majd valóban és "váratlanul" elő fognak kerülni különböző emberek "fiókjaiból"**, hiszen ezek akár élethosszig tartó lottó ötösként onthatják a pénzt a jogdíj gépezeten keresztül.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?

- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1222105

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.20. 09:28:09

Hol pénz vala, ott hamisítás is vala:
autogram.blog.hu/2009/07/19/hamis_jackson_autogramok_a_magyar_aukcios_portalokon_is

Ismét a Conficker vezet a vírustoplistán

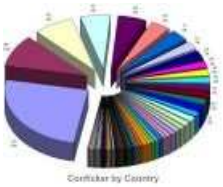
2009.07.03. 10:59 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET víruslaboratóriumának szakértői szerint **a magyar vírustoplistát ezúttal is a biztonsági frissítések nélküli gépek és a felhasználók által futtatott trójaiak** alakították ki.

Bár Magyarországon hosszú ideig a Virtumonde végezte a legnagyobb pusztítást, a múlt hónapban a második helyre esett vissza. Az élre a 2008. november vége felé felbukkant **Conficker féreg került, amelynek erősödéséről azóta is** folyamatosan olvashattunk.

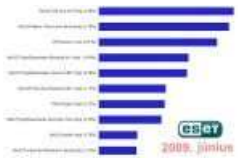
Mint ismeretes, a Win32/Conflicker.AA egy olyan hálózati féreg, amely a Microsoft Windows biztonsági hibáját kihasználó exploit kóddal terjed, és a gyenge admin jelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül szaporodik. Bár az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőséghez **már tavaly októberben kiadták az MS08-67 jelű Microsoft biztonsági javítócsomagot**, sajnos sok felhasználó nem fordít elég figyelmet az operációs rendszer frissítésére.



Ha figyelembe vesszük, hogy a júniusi toplista második helyére visszaszoruló Virtumonde úgy terjed, hogy ingyenes .mp3 fájlok és más tartalmak ígéretével ráveszi a felhasználókat a telepítésre, látható, hogy a kártevők elleni védekezésben **továbbra is az ember a leggyengébb láncszem**.

Tovább haladva a toplistán: az Autorunnal kapcsolatos fertőzések e hónapban is a harmadik helyen találhatóak, míg a negyedik helyre **egy vadonatúj versenyző, a Win32/TrojanDownloader.Bredolab.AA** köszönt be. Ez egy olyan trójai, amely megkísérel távoli oldalakról további kódokat letölteni és végrehajtani. Futása közben a Windows, illetve a Windows/System32 mappákban igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás **felel eredetileg a felhasználó hitelesítő adatainak továbbításáért** az ügyfélszámítógépről a célkiszolgálóra.

Összességében elmondhatjuk, a biztonság megteremtése érdekében alapvetően fontos az operációs rendszer naprakészen tartára. Épp ezért az új, 4.0 verziójú ESET NOD32 Antivirus és ESET Smart Security már képesek arra, hogy a hiányzó biztonsági frissítésekre figyelmeztessék a felhasználókat.

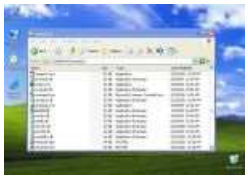


Végezetül következzen a magyarországi toplista. Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2009 júniusában az alábbi 10 károkozó terjedt a legnagyobb számban**. Ezek együttesen 33.78%-ot tudtak a teljes tortából kihasítani maguknak.

1. Win32/Conficker.AA féreg
Elterjedtsége a júniusi fertőzések között: 5.48%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal

számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: **http://www.eset.hu/virus/conficker-aa**

2. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a júniusi fertőzések között: 5.29%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/adware-virtumonde**

3. INF/Autorun vírus
Elterjedtsége a júniusi fertőzések között: 4.81%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: **http://www.eset.hu/virus/autorun**

4. Win32/TrojanDownloader.Bredolab.AA trójai
Elterjedtsége a júniusi fertőzések között: 3.64%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, melynek segítségével a távoli oldalakról letöltődnek és végrehajtódnak ezek a kódok. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/trojandownloader-bredolab-aa**

5. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége a júniusi fertőzések között: 3.58%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amelyek látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálják, valójában azonban maga a kártevő lapul a „csomagban". Emellett hátsó ajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/trojandownloader-swizzor-nbf**

6. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a júniusi fertőzések között: 2.71%

Működés: Ez a kártevőcsalád olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: **http://www.eset.hu/virus/psw-onlinegames-nmy**

7. Win32/Agent trójai
Elterjedtsége a júniusi fertőzések között: 2.67%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevőcsalád mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: **http://www.eset.hu/virus/agent**

8. WMA/TrojanDownloader.GetCodec.gen trójai
Elterjedtsége a júniusi fertőzések között: 2.53%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: **http://www.eset.hu/virus/trojandownloader-getcodec-gen**

9. Win32/Kryptik.GT trójai
Elterjedtsége a júniusi fertőzések között: 1.55%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.
Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/kryptik-gt**

10. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a márciusi fertőzések között: 1.52%

Működés: Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: **http://www.eset.hu/virus/toolbar-mywebsearch**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1223785

Kommentek:

Nincsenek hozzászólások.

Jimmy visszatért

2009.07.06. 19:51 | Csizmazia István [Rambo] | 7 komment

Címkék: spam bank csalás nigéria dél korea 419

Ha a barátunktól kapunk levelet, az felettébb örvendetes. Ha viszont valaki **ismeretlenül ír nekünk "KEDVES BARATOM" tárgysorú üzenetben, akinek nem mellesleg kéretlenül jövedelmező üzleti ajánlata is van**, legszívesebben még a mostaninál is melegebb éghajlatra küldenénk egy bájos süncsalád társaságában.

Ezúttal a 419-es nigériai csalás új metemórfózisban jelentkezik, gazdasági válság esetén talán nagyobb is a csodavárási hajlam, mindenesetre **az fájdalmasan sántít egy baráti levélben, hogy a jó pajtás, a kedves cimbora oltári slamposan "Undisclosed recipients" módon mindenkinek** csak úgy odaadja ezt a remek baráti ajánlatot, és nem csak egyedül bennünket tisztel meg a határtalan bizalmával. Mondjuk magunk közt szólva vagy egy gigantikus lúzer **az a dél-koreai bankigazgató, akinek csak egy hongkongi yahoos e-mail címre futja**, vagy az is lehet, hogy egyben remek James Bond, és ezzel csak a kiemelkedő konspirációs skilljeit alkalmazta, hogy ezzel is levegyen bennünket a lábunkról.

Friss, meleg, mai termés, és **bár maga a levél magyarul beszél, közben mi vígadunk sírva** és csapkodjuk a térdünket. Az automatikus fordítás eredményeképpen **Tuskó Hopkins, Csülök, Török Szultán és Fülig Jimmy nyári szabadságvesztésükről mind visszatértek**, és biztosítottak arról, hogy *"Megvan a hivatkozást a keresési valaki, aki megfelel az én javasolt üzleti kapcsolatot bele oda neki."* Ettől a szerfelett kedvező hírtől most már sokkal nyugodtabbak lettünk, kevésbé zihál a lélegzetünk, és **bátran reméljük a dél-koreai bankigazgató valóban értesít majd, már alig várjuk**.

Ott vagyunk már? Ott vagyunk már? Ott vagyunk már?

Egyelőre még nem reagáltak, pedig eddig már eltelt vagy 10 mp, és még mindig semmi ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1230006

Kommentek:

Eladó lakás Pécs legszebb helyén · http://elado-lakas.internode.hu/ 2009.07.06. 22:00:14

Én is megkaptam! Nagyonjó, főleg az első mondat... :D

Fedup Sári 2009.07.06. 23:16:23

De most komolyan, mit csinál, ha magyarul visszaírok neki?

nemuccaszoc 2009.07.07. 07:19:24

Kedves BARATOM, JOSHI BARATOM.

szivárvány és szarhalom 2009.07.07. 08:01:31

@Fedup Sári: ráereszti a fordítót és csodálkozik, hogy milyen olvashatatlan lett...

misterx 2009.07.07. 08:29:12

Sztrovacsekek!
Kedves barátunk, "Peter Lee" nem hülye, sőt. Ezt a levelet alighanem minden kelet-európai nyelvre le gépi fordította és a országdomain szerint szétválogatva szétküldte a valahonnan vásárolt címeire.
Ha a sok ezerből vagy tízezerből akár csak egy hülye is akad (márpedig a nagy számok törvénye szerint akad, hiszen hallottunk már ilyen magyar rémtörténeteket is) akkor már jó üzletet csinált, pár hétig nem kell dolgozni mennie...

Andie 2009.07.07. 09:36:59

Javaslom ezt az oldalt: www.419eater.com/
Én fetrengtem néhány sztoritól. (pl amikor a mókus kirágta a faszobrot mire odaért a postán :)))

Sam. Joe · http://www.matchboxmemories.hu 2009.07.07. 19:10:08

Totál megrémültem, hogy Zámbó Jimmy tért vissza!!! Rambo, a frászt hoztad rám! 8-]

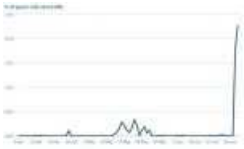
Kiborul a Bit.ly

2009.07.08. 20:31 | Csizmazia István [Rambo] | 12 komment

Címkék: spam firefox plugin url rövidítés bit.ly

Egészen pontosan az történik, hogy a **spam és kártevő terjesztők hihetetlen mértékben rákaptak az URL rövidítési technikákra**. Mit tehetünk ez ellen, hogyan, miért és egyáltalán?

A MessageLabs jelentése szerint nem pusztán üres szavak a "rákaptak", ha **a mellékelt grafikonra pillantunk**, minden valószínűség szerint "aha" élményünk lesz. Természetesen értelmes okkal is használják ezt a rövidítést például a Twitterezéshez, de mindent lehet jó és rossz célra is használni: az atom lehet bomba, de táplálhat erőműveket is. Egyszer már rugóztunk ezen a témán, akkor a **cli.gs rövidítés szolgáltató feltörése** adta ehhez az apropót.



Az ottani végszóban Graham Cluley azon óhajának adott hangot, miszerint minő kellemetes dolog lenne, **ha megjelennének pluginek a böngészőkhöz**, amelyen mondjuk hovernél (az egeret a terület felé visszük) kibontaná még a kattintás előtt és **maszk nélkül megmutatná a teljes hosszú hivatkozást**.

Hát így legyen ötösünk a lottón, már ami a Bit.ly-t illeti Firefox alatt, erre egyáltalán nem kell tovább várni, **elég csak megtalálni azt, hiszen már jó ideje szerepel a kiegészítők között** a Bit.ly Preview, a legutóbbi frissítése például áprilisban történt.

Ez pontosan ezt csinálja, amiről fentebb szóltunk. És bár a jótanács úgy szól, **idegentől sose fogadjunk el (tudatmódosító) cukorkát vagy kéretlen linket**, időnként mégis csak egy használható jó kis eszköz lehet ez a fegyvertárunkban.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1233740

Kommentek:

is 2009.07.08. 21:45:48

ez jó. tetszik.

Before · http://azbeszt.blog.hu 2009.07.08. 22:14:22

Jó bizony, bár én már jó ideje nagyon óvatos vagyok a tiny url-ekkel...

Mirko 2009.07.08. 22:34:30

Tessék a jui.cc-t (jui.cc) használni, már régebb óta van benne preview mód.

dX 2009.07.08. 23:54:52

sajnos egyik sem 100%-os tapasztalataim szerint

longurl.org/

LongURL Mobile Expander 2.0.0
addons.mozilla.org/hu/firefox/addon/8636
Preview Link 0.3.4
addons.mozilla.org/hu/firefox/addon/6916
bit.ly preview 1.262
addons.mozilla.org/hu/firefox/addon/10297

iNick 2009.07.09. 00:17:10

Szerintem meg egyszerűbb lenne megoldani a hosszú linkek problémáját. Akkor nem kellene mindenféle plug-izékkel bajlódni.

atleta.hu · http://www.atleta.hu 2009.07.09. 02:09:13

Ilyen mar volt tinyurl-hez is. Igazabol egy greasemonkey script eleg hozza, azt meg pillanatok alatt osszedobjak a juzerek (pl. userscripts.org/scripts/search?q=url+expander&x=0&y=0).

A bosszanto nem is a spam levelekben a rovidites, hiszen maga a rovidites szolgaltatas szerepeltetese egybol kuldheti a kukaba a levelet, hanem az, hogy egyes balfek felhasznalok akkor is hasznaljak ezeket, amikor nem kene. A twittert meg megertem, ott van egy ertelmetlen meretkorlatozast, amit igy probalnak kikerulni a felhasznalok, de egesz sokan forum postokba meg e-mailekbe is ilyet dobalnak, ami egyreszt bosszanto, mert jo lenne latni, hogyhova mutat az az URL, akkor is ha megbizunk az uzenet irojaban, masreszt segiti a trukkozoket, mert igy aztan tenyleg nehez kivalogatni a nemkivanatos linkeket.

@iNick: > Szerintem meg egyszerűbb lenne megoldani a hosszú
> linkek problémáját.

Konkretan mire gondolsz? Nincs problema, ezenkivul ha van is, nem lehet megoldani. Minden site letrehozoja maga talalja ki az URL strukturajat, erre nem lehet kozpontositott egyedi megoldast adni. Egyes site-ok egyes oldalainal elkerulhetetlen, hogy parameterek is legyenek az URL-ben. Lasd pl. a fenti userscripts-es linket. Erre nincs megoldas, mert ez nem problema. Az URL-nek nem rovidnek, hanem konnyen ertelmezhetonek, jol olvashatonak kell lennie (tobbek kozt).

> Akkor nem kellene mindenféle plug-izékkel bajlódni.

Plugin izekkel mindig kell bajlodni, ha kenyelmesen akarod hasznalni a webet. Azert, mert kicsi az eselye annak, hogy a bongeszo keszitoi pont telibe talaljak a funkciokkal a te izlesedet. Vagy ha te ilyen szerencses vagy, akkor a maradek 99.999% nem lesz az, es ezzel sincs mit tenni :)

bean 2009.07.09. 02:28:18

tessek tinyarro.ws -t hasznalni.

DownQ · http://letoltes.freebase.hu 2009.07.09. 06:24:48

Én nem véletlen nem kattintok sose ilyen rövidített URL linkre!

ZöPö_ · http://route66.blog.hu/ 2009.07.09. 07:25:28

@DownQ:

Teljesen igazad van, én sem teszem soha (és nyugodtan alszom).

◄ViZion 2009.07.09. 07:56:26

Ahogyan az öregek mondják: "ne csak azt figyeld mit mondanak, hanem azt is, hogy ki mondja..."

Azaz ha sandra bullock, vagy Jacko (RIP) a feladó, akkor mind1 hogy milyen url van a levélben.
Ha ismerős a feladó, de láthatóan "továbbküldős-megnyerős", vagy "véraadóssegítős-átkozós" a tartalma, akkor az delete.

Baromméter 2009.07.09. 08:37:20

konkrétan mi az a rövidített url? Mikor az url be van ágyazva egy text sztringbe?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.09. 09:06:02

@Baromméter:
Mondjuk a twitterre írnál egy bejegyzést, ami maximum 140 karakter lehet.

A szöveg alá (pl. Győzike és ET közös gyereket akarnak) be szeretnéd tenni az alábbi linket:
www.hosszulink.hu/vitez/nagybanyai/horthy/miklos/legkedvesebb/matroza/matraverebelyre/utazott/vonattal/klepetusban.html
linket, ami nem ferne be.

Ekkor elmesz egy URL (link, Universal Resource Locator) rövítési oldalra, például bit.ly/, és ott begépeled a fenti hosszú linket. A Bitly vissza ad egy rövid, hat karakteres azonosítóval rendelkező másik linket (pl. bit.ly/123456) ami UGYANODA elvisz ha rákattintasz, de kisebb helyet foglal. Nagyjából ennyi a lényeg.

Nyertünk a lottón

2009.07.09. 20:54 | Csizmazia István [Rambo] | 12 komment

Címkék: microsoft spam lottó

Ha valakinek **deja vu érzése lenne a mai posttal** kapcsolatban, az korántsem a véletlen műve. Mint ahogy örülni is korai egy ilyen típusú "nyereménynek".

Levelet hozott a posta, **maga a fenséges Microsoft értesít bennünket, micsoda fényességes szerencse** ragadott el bennünket és a sors a tenyén hordoz. Vagy mégsem? A **Microsoft Email Lottó azt közli velünk egy elektronikus üzenet útján, hogy nyertünk**, mindössze a mellékelt LOTMS.DOC állományt kell ehhez megnyitni.

Paranoid Android ilyenkor **szépen felhelyezi az ilyesmit a VirusTotal-ba, és megnézi az eredményeket**. Ez most 0 találat a 41 motorból, ami vagy azt jelenti, hogy **vagy nincs kártevő**, és csak sima szélhámosság, vagy pedig egy nulladik napi sebezhetőség is lehet benne még - **emiatt érdemes lehet pár nap múlva ismét bedobni egy vizsgálatba**.

Mi most **nagy furmányosan Linux alatti OpenOffice programmal nyitjuk meg**, abból nagy baj nem lehet, és máris olvassuk a cirkalmas iratot.

Angol zászló, címer, árulkodó gmailes elérhetőség, "hiteles" referencia szám, biztonsági (LOL) kód, parasztvakítás, korábbi "nyertesek" fényképei: egyszóval **van itt kábítás nem középiskolás fokon**. Nagyjából az a vicc ugrik be róla, hogy *gazdagéknál csörög a telefon. Anyjuk kérdezi: na mi az apus? Áh semmi, csak most szóltak, hogy megint nyertünk egymilliót, borzasztó, hogy az embert már enni sem hagyják nyugodtan*. Azért ha ennek ellenére **valaki mégis vett magának már néhány tucat jachtot vagy pár seychelles szigeteki kalyibát a Microsoftos email lottónyereményből**, legyen már oly jó, és **írjon nekünk ide egy kommentet ;-)**

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1236657

Kommentek:

jdavidpeter (törölt) 2009.07.09. 22:54:47

VirusTotal, Linux, Open office...
Nem bíztad a véletlenre, az is biztos...

I'll be Beck! 2009.07.10. 00:14:19

Nem, ez tényleg nem éri el a középiskolás fokot. De hát egyszer tíz éves az ember. Annál van baj aki abban a korban nem küldözget ilyet. Meg azzal aki úgy tizennégy után még mindig. Meg annál - életkortól függetlenül - aki felül neki. Meg azzal a kibaszott köcsöggel aki szemben lakik, és egész éjjel - most is - kibaszott call of dutyt játszik anyabaszó 300 wattos mélynyomóval.

cuebler 2009.07.10. 06:14:35

@Môžeš mi pomôcť?: m'ér' nem játszol vele major league baseball 2009-et 80 cm-es keményfa "testápolóval"? én már rég megtettem volna...

én hetente nyerek valami holland vagy belga lottón 10-50m "ajrót", győzzük lapátolni a sarokba a pénzt azóta is :-D

érthetetlen, hogyha nem vírusfertőzött az állomány, mi hasznuk van az egészből? nem lehetséges, hogy a szolgáltató már megszűrte a levelet és így egy "vírustalanított" üzenet jutott el hozzád?

FAQlyás Menyét 2009.07.10. 07:35:25

Az nem angol zászló, hanem brit. Az angol zászló sok helyen kint van Angliában magánházakon, kocsikban is, népszerű. Ezt meg csak hivatalos helyen vagy turisták által látogatott üzletben láttam.

BKV reszelő · http://praxisfree.blog.hu 2009.07.10. 07:53:01

@Môžeš mi pomôcť?: Gyere át játszani és ne anyázz, mert seggberúglak !

FPéter 2009.07.10. 09:09:21

Bemásoltad a titkos kódot, ez nagy hiba volt: így bárki felveheti a nyereményt! Én már írtam nekik, holnap küldik a pénzt egy aktatáskában, gyorspostával! Úgyhogy ti már ne írjatok nekik! Csak a postaköltséget kérték előre!!

Nekem a 7 kontinens 8 országa jött be legjobban... 3000 név kontinensenként, összesen 21000, de 8 van felsorolva, igaz Kanada, az Egyesült Államok meg a Közel-Kelet is beleszámít... Hát, földrajzot még egy kicsit gyakorolni kell :))

@cuebler: hallottál már a Nigériai levél szisztémáról?

LegMEGMÉRETETTebb · http://megmerettetes.blog.hu 2009.07.10. 09:12:43

Ugyan már... :) Végre valahol lehet megint nyerni. Ez tök jó! :D:D

Amúgy, ahogy drága gazd.matek tanárom mondta volt: a lottón egyetlen matematikailag is megindokolható módon lehet BIZOSAN NYERNI: ha nem is játszol! :))

Aki meg ilyeneknek bedől, annak kéne egy kis kirándulást tennie a való világban.

Shitting Bull 2009.07.10. 09:13:34

@FPéter: nigériai kapcsán az emberi hülyeség és kapzsiság végtelenségére gondolsz? ;)

Malefictus 2009.07.10. 09:22:02

Nyehe, én tegnap kaptam 419 -es arcoktol, s komolyan gondolkozom, hogy jomagam is azt csinalom mint ez az urge:

www.419baiter.com/games.html

Masik dolog, hogy érdemes valaki szerint utánamenni az IP nek?

Gyűjtő 2009.07.10. 09:22:09

Még több totó-lottós kártyanaptár:

www.kartyanaptarak.hu/thumbnails.php?album=37

tárhejj · http://atarhely.hu 2009.07.10. 10:50:20

Így kell csinálni :)

Csokiropitictac 2009.08.06. 11:59:18

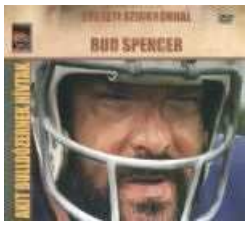
Sziasztok!
cuebler kérdezte,hogy mi hasznuk ebből az egészből ha nem vírus! Én kb 3 naponta nyerek...:DXD És úgy a 6. után visszaírtam az üzenetre,hogy nah ez tök jó,mikor kapom meg a nyereményt?:DKaptam egy nyomtatványt,hogy töltsem ki,semmi nagy szám (cím,név a szám amivel nyertem).Gondotam ennyi még belefér!:D Aztán persze kibújt az a szög.... Nemzetközi közjegyzőnek kell hitelesíteni a nyereményemet... :D Úgyhogy utaljak át nekiik 850Eurot xy számlájára és utánna megkapom a pénzt!XDXD Utalom én apukám csak győzd kivárni!:D:D Nem lepne meg ha valaki át is utalná ezt a pénzt... és már meg is van a haszon!:D

Akit Bulldózernek hívtak...

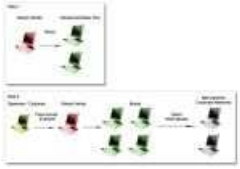
2009.07.13. 21:12 | Csizmazia István [Rambo] | 1 komment

Címkék: usa korea botnet fájl törlés mbr

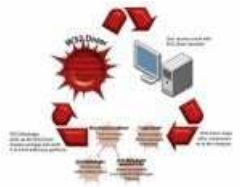
A Bud Spencer rajongók most esetleg csalódnak, nem a nevető szemű Terence Hill mackós partnere, hanem a Win32/Dozer néven is emlegetett kártevő következik, amelyről biztonsági szakemberek azt jelentették, hogy a botnetes támadás során nem pusztán csak DoS támadást hajtottak végre az USA kormányzati hivatalai és dél-koreai számítógépek ellen, hanem a kórokozó **adatpusztítással is megpróbálkozik**.



Mintha csak egy retró partin lennénk, **előkerülnek a múltból a klasszikus 5-10 éves barbár payloadok: állományok titkosítása, törlése, a merevlemez Master Boot Recordjának (MBR) felülírása, a Windows újraindításának megakadályozása**. Rombolás, pusztítás fullosan.



Az eredeti **botnetes koncepciónak ez ugye némileg ellentmond**, hiszen a botnetek üzemeltetőinek pontosan az a jó, ha hosszan és észrevétlenül irányíthatják az áldozatok fertőzött gépeit. Ezzel egyrészt lehet távoli támadásokat indítani, de a gépeken lévő személyes adatok is rendes pénzt érnek a fekete piacon. Ha valaki viszont **kitekeri az aranytojást tojó tyúk nyakát**, az biztosan nem véletlen (esetleg hadgyakorlat). Igaz, ezzel a bizonyítékokat is igyekszik eltüntetni maga ellen, de a rendszeres pénzt hozó, bérbe adható zombihálózat ezzel megsemmisül.



Zárójelesen magunk közt szólva az Egyesült Államok elleni támadás még teljesen világos (csillió számú Windows hemzseg az ottani gépeken), de mivel Dél-Koreaiaknak már évek óta van saját nemzeti Linuxa, itt már kevésbé világos a támadás vonala?!

Reméljük, egyszer talán megtudunk minden részletet, **ki és milyen - esetleg politikai - céllal szervezte ezt a támadás sorozatot**. Addig is akik úgy gondolják, azok használjanak vírus- és kémirtót. Akik pedig másként vagy akárhogy is gondolják ;-), nos ők pedig mentsék rendszeresen külső adathordozóra munkájukat a kellemetlen meglepetések elkerülésére.

A Win32/Dozert pedig együtt utáljuk, de Bud Spencert azért továbbra is szeretjük, hiszen ő maximum olykor képen töröl valakit, de semmiképpen nem törli le vagy semmisíti meg a Windowsos gépeket.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1243240

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.07.13. 22:40:22

Egy kis szinvonalas háttér info:
www.shadowserver.org/wiki/pmwiki.php/Calendar/20090710

MKB Bank reloaded

2009.07.14. 07:11 | Csizmazia István [Rambo] | 1 komment

Címkék: bank phishing mkb adathalászat

Nincs karácsony Corvin nélkül - emlékezhetnek az idősebbek és katonaviseltek. Mostanában pedig **nincs MKB Bank phishing kísérlet nélkül**.

Még két hónap sem telt el az előző kísérlet óta, amelynek inkább az volt a jellegzetessége, hogy egy vélhetően delirium tremensben szenvedő orángután három üveg sör után a magyar szótárt lapozgatva segített az elkövetőknek az online fordító programokban történő magasszínvonalú elmélyedésben. Mostani embereink már jobban igyekeztek, és **a weblap másolatát elég jól sikerült felidézniük**, de a feltűnően izraeli URL bántóan gyenge próbálkozás.

Aki nem vesz észre hogy nem a bank oldalán jár, annak alapvető ismeretei hiányoznak

Mint a Fülesben, vegye észre a két kép közötti 19 különbséget ;-)

Figyeljük meg a belépést. A csaló oldalnál nincs semmilyen tanusítvány, illetve SSL.

Amikor valamilyen próba adatot begépeltünk, akkor pedig **jöttek a PHP warningok hosszú tömött sorban**. Tanulság, egy bűnöző is tesztelje ki "becsületesen" a weboldalát, ha komolyan akar tőlünk valamit ;- A belépési oldalon az English és Deutch linkek **a valódi oldallal ellentétben** nem azonnal nyelvet váltanak, hanem a fő oldalra dobnak vissza.

Ettől függetlenül **magára vethet, aki ide begépeli az azonosítóját**, bár valószínűsíthető, hogy az oldalt órákon belül lezúzzák, a NetCraft, a Firefox és az Opera például **már be is listázta, mint adathalász kártékony helyszínt**.

Na nem mintha sajnálnánk őket, de szerintünk a csalóknak **ideje lenne feladni az automatikus fordításba vetett léha reményeket** (Arkagyij Rajkin-szerű figura ma ottan már nem igazán lenni menő bele oda neki ;-), és az egy betűs elgépeléssel lefoglalt domain név mellett valamilyen munkanélküli nyelvtanár vagy tolmács segítségét volna érdemes igénybevenni, **különben így végképp nem keresik meg még a hidegvízre valót sem ;-)**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1244583

Kommentek:

atko 2009.07.15. 20:59:15

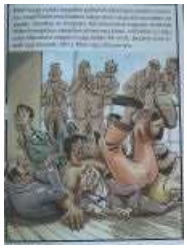
Csak az igazoló sms-t is használó oldalakban bízok. Akkor a telefonszámomat is ismerniük kéne.

Nézzünk a forrásba!

2009.07.15. 19:21 | Csizmazia István [Rambo] | 3 komment

Címkék: google javascript futás automatikus view source chrome

Ezen a különleges kánikulai napon **a ventilátorok egyhangú búgása mellett egy hűs, erdei forrásra néznénk a legszívesebben**. Egyelőre marad a Google Chrome böngészője, amelynek segítségével meglátogatunk egy weboldalt, **beletekintünk a View Source segítségével a weboldal forráskódjába**, és Fülig Jimmyvel szólva: "Lesz nagy meglepetés!"



A jelentés szerint ha a Google Chrome böngészővel a forrás megtekintés / view source használatával **meglátogatunk egy weboldalt, annak gazdája képes lehet egy olyan JavaScript programot beilleszteni a kódba, amely ebben az esetben rögtön le is fut**. Hétköznapi felhasználók általában kevesebbszer kíváncsiak valaminek a forrására, webes vagy **biztonsági szakemberek számára azonban ez mindennapos**.

Ha valaki **ki szeretné próbálni élőben - mi megtettük, és működött** - elég ellátogatnia erre a linkre a Chrome böngésző segítségével:

view-source:http://ha.ckers.org/weird/chrome-redirection.cgi

Ha felpattan az alert ablak a **"Ha ezt látod, használj másik böngészőt... komolyan",** akkor sikerült a kísérlet, és még örülhetünk is, hogy a kísérleti kódban nem a Document.Write(virus.exe) szerepel, hanem **csak egy ártalmatlan Alert() függvény**. De már várjuk az olyan alert ablakot is, amelyik az "Ember, miért használsz Windowst, térj át gyorsan Macre vagy Linuxra" feliratot jeleníti majd meg ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1247226

Kommentek:

atko 2009.07.15. 21:18:56

:-) és nem árt az sem ha a fegyvertárban ott figyel a noscript és azt tisztességgel használja is az ember gyermeke. Kicsit több figyelmet igényel, de már a 11 éves kislányom is elboldogul mellette. (a könyvjelzők természetesen engedve vannak) Ja igen és ez firefox. A chromot csak virtualboxban próbáltam xp alatt, de nekem pl mindig kiírja flash figyelmeztetést pedig a figyelmeztetés felett játsza a weboldalam videóját.

Algernon 2009.07.17. 20:52:06

Szia István!

Hm, én krómozom már egy ideje, semmi gond nem volt vele eddig. Gyors, könnyű,nem fagy...
Ha belefutnék egy ilyen módon nekem címzett "virus.exe"-be, akkor kérne tőlem rábólintást, hogy telepítsem vagy teljesen automatikusan, feltelepítené magát a háttérben?
Mert ha a belegyezésemért folyamodik, akkor talán nincs olyan nagy baj...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.17. 21:58:23

Szia Algernon!

Én úgy látom, itt pontosan az a probléma ebben, hogy NEM kérdez, hanem magától azonnal lefut.

Graffiti party Moszkvában

2009.07.16. 15:42 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: graffiti security moszkva smart android eset

Van egy hely Moszkvában, ahol **legálisan és szabályszerűen lehet a falakra pingálni**. Egy **minimális összegért kapunk egy területet, és ott aztán** szabadjára lehet engedni a fantáziát.

Kedden egy olyan baráti társaság gyűlt itt össze, akikben az a közös, hogy **valamennyien az ESET vírusvédelmi programjának értékesítésével foglalkoznak**. És mi más lehetett volna a kiválasztott téma, mint az ESET Smart Security Androidja. A csapatból **ketten igazi profik voltak, a többiek életükben először csináltak ilyesmit**.

Következzen hát a lépésről lépésre megörített munkamenet, a festmény elkészítése **nagyjából kettő és fél óráig tartott**. Köszönjük Andrejnek a képeket, és ezúton gratulálunk az alkotóknak!

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1248850

Kommentek:

Nincsenek hozzászólások.

Itt az első mobil botnet

2009.07.17. 10:55 | Csizmazia István [Rambo] | 12 komment

Címkék: spam s60 symbian sms botnet féreg trendmicro

Ha valaki eddig teljesen feleslegesnek tartotta a mobileszközön futó vírusirtót, mostantól **könnyen lehet, hogy megváltozik a véleménye**.

A TrendMicro kutatói figyeltek fel a egy olyan Symbian S60 platformon terjedő féregre, amely képes volt arra, hogy a telefon internetes kapcsolata esetén egy távoli szerverről adatokat letöltve **SMS üzeneteket küldözgessen például a telefonból kiolvasott címjegyzékre**. Ugyanakkor az is újszerű, hogy **képes a telefonból kiolvasni előfizetői és egyéb adatokat, amiket pedig erre a szerverre küld el**. A kártevő egy korábbról már ismert, de most extra tulajdonságokkal felruházott új variáns. A kutatók legrosszabb forgatókönyve szerint elképzelhető egy ilyen **fertőzéssel növekvő, spam terjesztést végző botnet kialakulása**.

Ha valaki emlékszik még a mobil kártevők múltjára, csak **néhány és inkább bosszantó, mint óriási kárt okozó egyedek szerepeltek a listán, és elterjedtségük is csekély volt**. A veszélyeknek pedig látszólag **befellegzett, amikor kiadták az S60 R3 jelű**, illetve a Symbian 9.0 verziókat, hiszen ezek számos jelentős, a biztonság szempontjából kulcsfontosságú változtatást tartalmaztak. A legfontosabb talán az a változás volt, hogy ettől kezdve már csak a Symbian és a hozzá tartozó szoftverházak partnerei által **digitálisan aláírt csomagokat lehetett telepíteni**. Emiatt is **érthetetlen, hogyan mehetett át a szűrőn** ez a mostani fertőzött alkalmazás. Most persze lehet, hogy jól jönne nekik is egy olyan nagy testvéres, iPhones lehetőség, mint a megadott alkalmazás távoli központi törlése és visszahívása az összes telefonról.

Napjaink okostelefonjai **egyre több hálózati képességgel rendelkeznek**, és kiváló célpontjai lehetnek a jövőben a kéretlen SMS küldésnek éppúgy, mint a telefonban őrzött bizalmas adatok ellopásának.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1250831

Kommentek:

FK 2009.07.17. 14:06:57

Mekkora a botnet? Hány telefont fertőztek meg? Mire használják? Mert ha a legrosszabb forgatókönyv szerint elképzelhető hogy talán kialakulhat egy esetleg veszélyes hasonló... legalább 5 éve erről hallunk, és még sosem alakult ki. Akkor most tényleg itt van, vagy inkább csak szenzációhajhászunk és reklámot csinálunk a mobil vírusirtónak?

FK 2009.07.17. 14:07:49

Ja, hogy hozzá se lehet szólni... az más. Rögtön érthetőbb így :)

FK 2009.07.17. 14:09:31

Ekszkúzmi, hozzá lehet. Lassúinda...

Joindulat SC 2009.07.17. 14:13:13

Na ezért nincs olyan telefonom amin netezni lehet. (de lehet,hogy azért ,mert csóró vagyok) Elég ha a pc-ből lesz zombi gép... De azért ezt jó tudni.
"Napjaink okostelefonjai egyre több hálózati képességgel rendelkeznek" - a juzerek meg még mindig nem értenek hozzá.

holex · http://fred-basset.blogspot.com 2009.07.17. 15:03:49

ezért nincs nokiám. :)

D9 2009.07.17. 15:23:29

Elso korben ez nem virus, es nem fereg, mert nem tud terjedni, ez egy egyszeru malware, nemletezo fertozesi vectorral. Ilyet kb. fel ora alatt ossze lehet dobni a vilag akarmelyik hw/os platformjara, csak semmi ertelme.

Masodik korben, eljen a szakerto internetes ujsagiras, amely felfujja a semmit, es szenzaciot probal belolle gyartani. Az eredeti oldalon (blog.trendmicro.com/signed-malware-coming-to-a-phone-near-you/) nagyon korekten leirtak hogy ez egy "signed malware", es kb. a cikk lajan vagy egy (hibasan) elejtett megyjezes hogy "it appears to be a botnet" Aztan a geek-com-on rogton felfujtak hogy "itt az elso mobil botnet", amit aztan a "szakerto" szo szerint at is vett mindenfele ellenorzes nelkul.

Innen mar csak remenykedni lehet hogy ez egyszeru figyelmetlenseg, es nem az idezett AV gyarto forgalom-novelo huzasa.

(es mindezektol fuggetlenul, az egyedul erdekes kerdes az egesz temaban az, hogy 1. hogy is van ez digitalisan alairva, 2. miert

nem lehet az S60-ban alairasokat visszavonni, de vegul is ezek szakmai kerdesek, amik nem erdekelnek senkit)

jtrencsenyi · http://artexgames.tumblr.com 2009.07.17. 16:07:40

"miert nem lehet az S60-ban alairasokat visszavonni, de vegul is ezek szakmai kerdesek, amik nem erdekelnek senkit"

Mert a Symbian egy rakás kaka! Azért.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.17. 21:45:52

Idézek a posztból:

"Emiatt is érthetetlen, hogyan mehetett át a szűrőn ez a mostani fertőzött alkalmazás. Most persze lehet, hogy jól jönne nekik is egy olyan nagy testvéres, iPhones lehetőség, mint a megadott alkalmazás távoli központi törlése és visszahívása az összes telefonról."

Vagyis szerintem volt szó az aláírással kapcsolatos érdekes kérdésről.

Dancho papa is nézegette már a mintát:
ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.18. 15:27:59

Itt egy példa a központi visszavonásra, nem biztos, hogy mindenki boldog ilyenkor:
www.mobilport.hu/laptop_hirek/20090718/botrany_az_amazonnal_-_lecsapott_a_nagy_testver_lecsapott/

prof. Perselus Piton 2009.07.20. 08:03:03

Sziasztok!

Nem ebbe a témába tartozik, de nem tudtam, hová írjam.

Mit jelent az a Nod víruskeresési naplójában, hogy "hiba- ismeretlen tömörítési eljárás" ?

Egészen pontosan a System Volume Information különböző összetevőinél jelenik meg.

A válaszokat előre is köszönöm!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.21. 12:51:50

Szia!

Elképzelhető, hogy esetleg valamiféle egészen új tömörítő, de pontosat akkor lehetne mondani, ha az adott állományt és a képernyőképet elküldöd a support KUKAC sicontact PONT hu címre.

prof. Perselus Piton 2009.07.22. 18:28:02

Az állományt nem lehet megnyitni és így elküldeni sem tudom. Azt írja, lépjek kapcsolatba az alkalmazás forgalmazójával és ellenőriztessem, hogy a csomag érvényes Windows telepítőcsomag-e.
És itt beüt a pánik :-(

Harry Kókler és a félvér kodek

2009.07.20. 18:52 | Csizmazia István [Rambo] | 8 komment

Címkék: potter video letöltés stream online csalás harry kártevő kodek

Sokan **szeretnék bennünk az öreg kodekletöltegető legkisebb fiát látni**, no de hát mit tegyünk, ha mégsem vagyunk azok?

A kártevő terjesztők **ismét bevetették a már szakállas trükkjüket**. Ha valaki mihamarabb kíváncsi a Harry Potter és a félvér herceg című opuszra, hát begépeli a torrenten. Vagy **újabban inkább a Google-ban keresni kezd a "watch online Harry Potter and the Half-Blood Prince" nevű tételre**. Minő meglepetés, **érdekes módon a filmet sohasem lehet azonnal megtekinteni**, annak feltétele mindig ~~egy kis ungabunga~~ egy új kodek letöltése.

És ezzel már helyben is vagyunk, amikor **pont a felhasználó segít megfertőzni saját rendszerét**, tisztára mintha a rendőr segítene kicipelni a házból a betörőnek a színes TV-t.

A letöltendő kodek neve esetünkben a xFlash.Plugin.exe vagy DivX.FLCodek.exe letöltése és futtatása lett volna, amitől nem is a későn megszólaló lelkiismeret vagy az Artisjus miatt célszerű lemondani, hanem sokkal inkább számítógépünk tisztasága okán.

Minden kodek szintén biztos **csupán merő véletlenségből arról a paxxtiger.com oldalról tölthető le**, amit alig egy hónapja jegyeztek csak be, és július 13-án frissítették a DomainTools tanusága szerint.

A Harry Potter film esetünkben mindössze csak egy aktuális apropó, a jövő héten már a Michael Jackson sosem látott felvétele jön, vagy bármi szerepelhet, fontos hogy gyermekded énünk az Al Bundys felén felülemelkedve **kételkedjen már néha egy kicsit, különben örök elszenvedői leszünk az effajta trükköknek**. Sajnos úgy tűnik, ismét a gyanútlananabb és képzetlenebb felhasználók, és a kíváncsi gyerekek lesznek a csalás fő áldozatai.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1256123

Kommentek:

nemethv · http://backtotheukblog.wordpress.com 2009.07.20. 20:06:13

isohunton fent van kodek nelkul is :)
bar eleg silany minosegben.
de tudom nem ez a lenyeg...mindenesetre ez ugyan olyan mint a mostani twitteres balhe amikor feltortek vkinek az accountjat, mert password volt a jelszava...az emberi hulyeseg ellen nem lehet szoftverrel vedekezni....

bryan 2009.07.20. 20:46:19

Egy-két víruson mindenkinek túl kell esnie, gyerekbetegség. Aztán megtanulja. Aztán, ha már eléggé idegesíti,hogy vírusírtókkal kell szaroznia, áttér linuxra, onnantól máson idegeskedhet. :)

bbocs2 2009.07.20. 21:01:31

kodek??? az minek???
mióta VLC lejátszót használok (ingyenes, nyílt forrású, multiplatform), azóta nulla darab kodeket kell telepítenem...

nemethv · http://backtotheukblog.wordpress.com 2009.07.20. 21:08:14

@bbocs2: persze, csak a dolog lenyege hogy a "video" amihez kell a kodek nem igazi video, valszeg nincs benne anyag, viszont a flash-alapu player amin keresztul meg tudnad nezni (tehat nem vlc) "keri" a kodeket...aztan a juzer meg szepen leszedi.

mbazs 2009.07.20. 21:32:23

Úristen, mekkora lúzerek vagytok!

Nekem Linuxom van, és sosem kapok be vírust, mert Linuxra nincs vírus, mert olyan fasza biztonságos!

XD

(szal kurva jó ám, csak a wifivel szopok kb 1.5 éve, meg a compiz is szétfosta, meg 10-edikre bútol, meg az adept néha beszarik, meg a flash is 100% cpu-n pörög, meg ha vmit telepíteni akarok, akkor nyolcvanöt fórumot kell átnézni, meg... áááááá)

mondjon már végre valaki egy normális oprencert!

A_Denever 2009.07.20. 21:52:56

Ez meg rendben is van, de az mar milyen hogy a lalikiraly-ra is pampog a google? Egyik nepszeru radios musor oldalat szandekosan injektalja valaki szorakozasbol?
A tuzroka meg nem is jelez ra semmit...

google.com/safebrowsing/diagnostic?tpl=safari&site=lalikiraly.mifene.hu&hl=en

kovi1970 2009.07.20. 22:20:40

@mbazs: Ubuntu? Az neked jó lesz. Arról meg, hogy Linux disztribúció nem kell tudnod. :)

mrgeez · http://elhasznaltauto.blog.hu 2009.07.21. 08:22:16

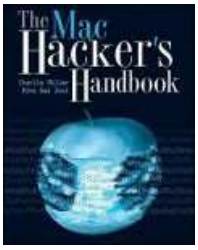
Én az előbb reflexből töröltem egy MMS-t, mert kaptam egy olyan üzenetet, amihez csatolmány tartozott, és azt írta a WM, hogy "click to open attachment". Még szerencse, hogy hülyebiztos a rendszer, és van recycle bin...

Hamarosan eljöhet a Mac gépek "ideje"

2009.07.21. 11:13 | Csizmazia István [Rambo] | Szólj hozzá!

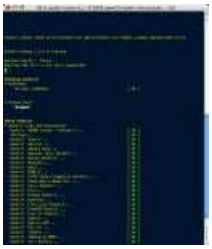
Címkék: mac os x black rootkit hat dai zovi

A stabil hardveren futó stabil operációs rendszer, UNIX alapokon - **ez sokáig megadta azt a fajta biztonságot**, amit például egy vírusokkal, kémprogramokkal, exploitokkal fenyegetett Windows kevésbbé adhat meg a felhasználóknak.



Most viszont úgy tűnik, egyre inkább szükséges lehet majd, hogy az etikus hackerek képesek legyenek egy átfogó penetrációs teszt keretében megvizsgálni, **mennyire biztonságos is egy adott OS X alatti gép**.

Ehhez természetesen az "ismerd meg az ellenséget" jegyében el kell mélyedni a részletekben, és ehhez jó adalék lehet Dino Dai Zovi a következő Las Vegasi Black Hat konferencián tartandó **előadása a rootkites fenyegetésről**. Állítása szerint bár maga az operációs rendszer valóban erős, ezen a platformon is kivitelezhető, és **ki tudhatná ezt jobban, mint maga a Mac Hacker's Handbook társszerzője**.



Emellett szó esett még arról is, hogy **Zovi szerint érdemes lenne ilyen jellegű információkkal is kiegészíteni a Metasploit Frameworkot, hogy a jövőben esetleg ezzel is bővülhessen a penetrációs tesztek** lehetősége.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1258153

Kommentek:

Nincsenek hozzászólások.

Az Erin Andrews menet

2009.07.22. 20:50 | Csizmazia István [Rambo] | 2 komment

Címkék: mac windows pc kártevő kodek sophos andrews erin

Alig két napja foglalkoztunk a Harry Potter film kapcsán csábító videókat hirdető, de **helyette kodeknek álcázott kártevőket terjesztő oldalakkal**, de máris itt a folytatás.

Most egy amerikai újságírónőről állítólag megjelent kukucskálós videó okoz hasonló kavalkádot. Egyrész **az állítólagos Erin Andrews felvétel megintcsak iskolapéldája** a "miért ne kattintsunk ilyen tartalmakra" című tanmesének. De az eset azért még ennél is több tanulsággal szolgál. **Érdemes a Sophos labor munkatársainak videóját megnézni**, hogyan operálnak a kártevő terjesztők, **micsoda szervezettséggel tartják a Google, és az érdeklődés középpontjában, ontják a linkjeiket**.

Az biztos, hogy ez egy igazi megtervezett és alaposan végiggondolt kampány, előre felkészültek rá, több különböző országban is regisztráltak a hamis kodekeknek domént. Nézelődésünk során mi főleg ukrán (.UA) és Beliz szigeteki (.BZ) oldalakat találtunk.

Ami a további megtévesztést szolgálta, **mintha valóban egy összhangolt hadművelet zajlana vagy egy multicég osztályai dolgoznának olajozottan össze**, a különféle weboldalakon, fórumokon, blogokon **rendre jelennek meg az új és új bejegyzések, hogy "de igen, létezik ez, íme a link", és jönnek egyre az újabb, ugyancsak kártékony tartalmakat terjesztő linkek**.

Tehát nem csak szimplán szélnek eresztették az akciót, hanem **folyamatosan adagolják az utánpótlást**, a dezinfomációt, a még újabb hamis linkeket - **igazi utógondozás folyik**. Akkor most már tényleg jöjjön a Sophos munkatársainak videója, ami itt található, és ráadásul még létezik is :-) http://vimeo.com/5662308

Az állítólagos fájl letöltést egyébként nem csak weblapokról, de torrentről, valamint rapidshare megosztókról is megkíséreltük, ahol azonban a várva várt **kártevő helyett mindig rendre hibás, nem létező linkekbe vagy nulla hosszúságú RAR archívumokba** futottunk bele.

Na és majdnem kimaradt a másik érdekesség, az új projekt már nem csak és kizárólag Windows gépeket céloz meg, **hanem a Mac felhasználóknak készült hamis kodek csomag**, hadd örüljenek, így ők is megfertőződhetnek, ha kattintanak. Az összeesküvéselméletek kedvelőinek pedig maradt még egy lehetséges forgatókönyv: Erin állása a gazdasági válság miatt bizonytalanná vált a televíziónál, ezért maga kérte meg ukrán maffiózó férjét/barátját/sógorát/unokaöccsét, hogy kerül amibe kerül, de javítson a népszerűségi indexén, ezzel pedig szilárdítsák meg a munkahelyi pozícióját ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1261044

Kommentek:

Andie 2009.07.23. 09:07:18

Szia Rambó!
Irtam mailt, remélem ezt megkapod :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.23. 09:49:45

@Andie:
Szia, igen, megjött :-)

Rendőrségi wardriving

2009.07.23. 10:03 | Csizmazia István [Rambo] | 16 komment

Címkék: wifi ausztrália rendőrség védelem wardriving

"Amit mi is leutánozhatnánk" című rovatunk keretében ezúttal Ausztráliába látogatunk, ahol **a rend derék őrei a tartalék izzó készlet bemutatására való felszólítás helyett** újabban **a lakossági WiFi kapcsolatok felett őrködnek** éberen.

Jó dolog lehet valamiben első lenni, ennek tudatában alakult meg egy kis önkéntes, a rendőrség kötelékében álló csapat, amely a polgárokat a csalásoktól, számítógépes betörésektől kívánja megóvni. Rendszeres járőrözésük alkalmával az észlelt védelem nélküli (még WEP-es sem, pedig az is két perc) **WiFi routerek tulajdonosait figyelmeztetik, hogy védjék jelszóval a netes kapcsolatukat**, nehogy illetéktelenek lehallgassák azt, vagy pedig titokban rákapcsolódva megcsapolják a sávszélességüket. A laptoppal vagy kéziszámítógéppel végzett barangolások során **sok ilyen védtelen, jelszó nélküli kapcsolattal rendelkező készüléket találnak, amelyekről a tulajdonos sokszor nem is sejti, hogy mekkora problémát okozhat**. Csak leveszik az üzletek polcairól, bedugják otthon és örülnek, hogy működik, és a kereskedők sem mindig figyelmeztetik a vásárlókat a szakszerű beállítások fontosságára.

Brian Hay detektív elmondása szerint **korábban rendszeresek voltak a visszaélések, az illetéktelen internet használaton keresztül egészen a személyiség lopásig előfordultak bűncselekmények**. Az akciótól ezek számának drasztikus csökkenését, valamint a lakossági internethasználók óvatosabb, és biztonságtudatosabb viselkedését remélik. Persze bírálat is éri őket, miért nem a kábítószer kereskedőket és gyilkosokat üldözik, de a rendőri vezetők szerint ez is egy fontos terület. Ha **ezzel a lépéssel szüleink, nagyszüleink egész életük során félretett megtakarításait, bankszámlájukat, személyes adataikat megvédjük** a csalásoktól, ezzel szintén hasznos dolgot cselekszünk - nyilatkozta Bruce van der Graaf, a rendőrség számítógépes egységének vezetője.

Google képtalálat: Kabuli wardriving ;-)

Innen is gratulálunk a Queenslandi rendőrségnek, és **várjuk az esetleges hasonló hazai kezdeményezéseket :-)**

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1262381

Kommentek:

Almaspite 2009.07.23. 10:55:00

De basszus, ha elmegy a rendőrautó a Havanna lakótelep mellett wardriving-olva és talál egy WPA nélküli routert, akkor honnan a rákból tudja, hogy melyik lakásba kell becsöngetni a nyolcezerből, hogy figyelmeztethesse a tulajt?!?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.23. 11:03:38

Lehet, hogy ez tényleg könnyebb Ausztráliában: kicsi a népsűrűség, csak 50 kilométerenkén lakik egy Krodil Dundee a lakókocsijával, el sem lehet téveszteni ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.23. 11:41:41

Mindazonáltal nem csak lakótelepek vannak a világon, és nem is csak Budapest létezik, tehát azért tenni mégis lehetne így is.

De ha már Pest, a PCW stáb elment egyszer este egy ilyen autózásra, és egy csomó helyen somán látszott, kihez tartozik a net: Pistike Kft, Sárga Főmajom Eszpressó, stb ilyen beszédes nevű helyeket találtak, és mellesleg ha van GPS támogatás, akkor pontosabban be lehet lőni a kordinátákat.

peetmaster · http://nemdohanyzom.blog.hu 2009.07.23. 11:49:14

és aki jófejségből, szándékosan hagyja nyitva?

Stupidella 2009.07.23. 11:58:54

Nem volna jó, ha nem tudnék úton-útfélen felcsatlakozni a jelszó nélküli wifikre. :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.23. 12:11:34

@peetmaster:

Maximum kap egy jelzést, hogy nyitva van a slicce, és annyi. Mindig akad olyan, aki direkt, tudatosan hagyja nyitva, nem

kötelező levédeni.

A figyelmeztetés azonban mégis hasznos a többieknek, akik nem vették észre vagy nem voltak képben, vélhetően örülnek neki.

Dude 2009.07.23. 12:11:48

a kedvencem a DLINK SSID, minden utcában van belőle.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.23. 12:12:35

@peetmaster:

Maximum kap egy jelzést, hogy nyitva van a slicce, és annyi. Mindig akad olyan, aki direkt, tudatosan hagyja nyitva, nem kötelező levédeni.

A figyelmeztetés azonban mégis hasznos a többieknek, akik nem vették észre vagy nem voltak képben, vélhetően örülnek neki.

dex.ion 2009.07.23. 12:17:08

@Stupidella: sztem is kurva szar lenne:))

Jegkoko 2009.07.23. 12:26:44

Hát nem tudom, de szerintem tök hülyeség, hogy mostanába már mindenki levédi a wifi hálózatát.Igaz én levédtem, de kötve hiszem, hogy a környéken bárki is felcsatlakozna rá.Viszont ha nem vagyok itthon roppant mód bosszantó, hogy majdnem minden háló zárt, igy még az indexet se tudom megnézni.Nem akarom én megtudni mi a jelszava a nyaldaszörösseggem.hu oldalon, mert ez engem teljesen hidegen hagy

Stupidella 2009.07.23. 12:43:04

@dex.ion: ugye :) mit kell itt álszenteskedni :)

dex.ion 2009.07.23. 12:54:12

@Stupidella: persze:) most se tudnék írni, ha mindenki ilyen gondos lenne:)

peetmaster · http://nemdohanyzom.blog.hu 2009.07.23. 14:34:55

@Csizmazia István [Rambo]: félek, kötelező lesz. Sarkozy hülye HADOPI-törvényében eredetileg felelős lettél volna a te hálódon letorrentezett zenéért is, ha jól emlékszem. (Vagy ez már csak a hecc volt?)
De akkor is, nem kell mindent betiltani, ami ingyenes.

gothmog 2009.07.23. 21:10:52

@Csizmazia István [Rambo]: De úgy meg elég könnyű kiszúrni, ha valaki lopja a netet.

prof. Perselus Piton 2009.07.24. 12:28:29

Nem találom a helyet, ahol jól nyakon lehet dícsérni a Sicontact-ot, ezért megteszem itt:

KÖSZÖNÖM SZÉPEN A SEGÍTSÉGET! Nagyon szép munka volt :-))

Külön köszönet a roppant türelmes fiatalembernek, aki megküzdött a gépemmel :-))
Ha minden magyar cég ilyen hozzáállással dolgozna, nem lenne semmi baj ezzel az országgal...

.A.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.24. 21:30:48

prof. Perselus Piton:

Köszönjük szépen, tolmácsoltam a technikai támogató csapatnak :-)

AVG vakriadó az iTunes programra

2009.07.27. 11:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: apple itunes avg vakriadó

Kellemetlen élményben volt részük az elmúlt hét péntekén azoknak, akiknek AVG védi a gépét és elindították az iTunest. Az antivírus **riasztott az Apple alkalmazására, megijesztve ezzel a felhasználókat.**

Az Apple blogjában is rendre feltűntek ezzel kapcsolatos megjegyzések, miszerint **az iTunes részeit képező iTunes.dll és iTunesRegistry.dll állományok állítólag fertőzöttek egy "Trojan horse Small.BOG" nevezetű kártevővel**. Ilyenkor az ember lehet, hogy gyanakszik ugyan vakriadóra, de azért száz százalékra sosem lehet biztos benne, hiszen annyi mindent láttunk már: fertőzött Maxtor merevlemezzel szállított noteszgépet, vírusos navigációs eszközt a boltok polcain, gyárilag fertőzött Asus EEE PC-ket, fertőzött banner hirdetéseket, fertőzött iPhone firmware frissítést, kártvőkre mutató linkeket a blogokban és a hozzászólásokban, stb.

A mostani eset elég **kellemetlen mellékhatásokat tudott produkálni**, hiszen akiknek a gépén törölte a tévesen gyanúsnak tartott, de egyébként tiszta fájlokat, azok **nem tudták többé elindítani vagy újratelepíteni az iTunes programot**.

Átmeneti megoldásként az AVG programot használóknak úgy lehetett megúszni a problémát, hogy "C:\Program Files\iTunes\" illetve "C:\Program Files\iPod\" mappákat fel kellett venni a keresésből kizárt kivételek közé. Ezzel ugyebár **ideiglenesen egy másféle kockázatba hajtja az ember a fejét**, de amíg ki nem jön a javított vírusismereti szignatúra frissítés, megteszi, mint **átmeneti workaround és legalább addig is fut az iTunes**. De voltak olyanok is, akik emiatt visszatértek régebbi, például 8.0-s verziójú iTunes programra, amit nem érintett ez a jelenség.

Az AVG végül észlelte a vakriadó tényét, és **a fórumos hozzászólók elmondása szerint elismerte a téves riasztást**, a poszt írásakor mindenesetre ezzel kapcsolatos **hivatalos közleményt még nem találtunk** a weblapjukon.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1270421

Kommentek:

Nincsenek hozzászólások.

Váltságdíj a böngészőben

2009.07.28. 14:40 | Csizmazia István [Rambo] | 1 komment

Címkék: csalás kártevő váltságdíj webböngésző

Van új a nap alatt! Egy **érdekes új vonalról számolt be a TheRegister.** A kártevő **Windows számítógép webböngészőit fertőzi meg**, és csak a mellékelt számra küldött emeldíjas **SMS küldésével tüntethetjük el a kéretlenül megjelenített reklámjait**.

Úgy tűnik, nincs nyári szünet bűnözőéknél. A korábbi hamis vírusirtók mellé sikerült egy újabb üzleti modellt megalkotni a kártevőterjesztőknek. Ezúttal az **orosz szövegű, és erotikus tartalmú kéretlen reklámok** az Internet Explorer, a Firefox és az Opera böngészőben képesek megjelenni. A fertőzés után minden meglátogatott weboldal elé betolakodva mutatja ezeket a felbukkanó zavaró ablakokat, és azt ígéri, hogy egy megadott számra küldött - **ki tudja pontosan mennyibe kerülő** - szöveges üzenettel lehet megszabadulni tőle.

A kártevőre a Symantec kutatói figyeltek fel, akik a böngésző beállító állományaiban és a rendszerleíró adatbázisban (Registry) végzett **kéretlen bejegyzéseket is részletesen közlik**. A TheRegister cikke szerint bár mindhárom böngésző veszélyeztetett, **a legújabb FireFox változat azonban állítólag már nem fertőződik meg** a váltságdíjszedő trójaitól.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1273353

Kommentek:

atko 2009.07.28. 14:58:09

Mindenki magától szenved a legtöbbet és aki hülye haljon meg.
Szerintem ezzel máris biztonságosabbá tehető az élet minden területe. A böngészés is.
A számítógép olyan mint a vezetés. Tanulás nélkül is lehet csinálni, de akkor veszélyes.

Amikor mi szépen hasítunk, és mások baltázzák el

2009.07.29. 20:40 | Csizmazia István [Rambo] | 3 komment

Címkék: hiba személyes incidens adatok identity theft mcafee illetéktelen

Hogy a **személyes adatainkat óvni kell, lassan mindenki megtanulja** és leszokik az "én csak egy hétköznapi egyszerű ember vagyok, semmi különös nincs a gépemben" álmentségről. De a hiba **nemcsak a "mi készülékünkben" lehet**!

Ha mi **szükszavúak vagyunk a közösségi** portálokon, **gyanakvóan állunk** az ismeretlen dolgokhoz, **gyakran váltott, mindenhol különböző és erős jelszavakat** használunk, **nem kattintunk** gyanús linkekre, használjuk a **naprakész biztonsági programokat**, és **frissítjük az operációs rendszerünket** - akkor ezzel mi **minden tőlünk telhetőt megtettünk**. Ez a tiszta, száraz érzés azonban egy pillanat alatt elszállhat, ha valahol máshol homokszem kerül a gépezetbe.

Nos éppen ez történt azzal az 1408 emberrel, akik egy McAfee által szervezett **Sydneyben rendezett konferencián vettek részt**, és egy **olyan kör e-mailt kaptak, amelyben VALEMENNYIÜK személyes adata szerepelt**: név, cím, vállalkozás, munkahely címe, telefonszám, e-mailcím. Ha volt köztük a biztonsági szakember is, akkor ezek most nem csak teljes mélységében átérezték az incidens súlyát, de valószínűleg roppant csalódottak is voltak, hogy pont velük ilyesmi megtörténhetett, és **csak remélhetik, hogy a nevükkel és beosztásukkal nem élnek vissza csalók a jövőben**.

A kicsit "a hóhért akasztják" esetnél **nem tudták megmondani, pontosan hány helyre juthattak el** végül így a személyes adatok 1 MB-os XLS táblázata. Mentegetőzésként leszögezték, hogy a tábla csak a konferencia résztvevők regisztrációs adatait érintette, és semmilyen pénzügyi adatokat nem tartalmazott. Mindenesetre **jó figyelmeztetés lehet ez mindenkinek**, hogy az e-mail kicsit olyan, mint a kimondott szó: érdemes előtte alaposan meggondolni, ha pedig már kimondtuk, az később már nem vonható vissza.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1275326

Kommentek:

atko 2009.07.31. 08:14:13

Ezt most nem értem, akkor a szervezők küldték a O-emilt, vagy valaki megszerezte és csak figyelmeztetésképp küldte el azt.
Egyébként meg folyton hangsúlyozom minden ismerősömnek, hogy az excel az már a számítógép sötét oldala! Mindig azt mondják az csak egy kockás füzetlap.. aztán kiderül, hogy számol és mindenféle trükkökre képes ;)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.31. 09:04:20

Hát pontosan ez a probléma, hogy pont egy AV cég tett ilyet: "McAfee sends out personal details in email":
www.itnews.com.au/News/151485,mcafee-sends-out-customer-details-in-email.aspx

atko 2009.07.31. 11:15:32

Így már világos és értem. "Az embernél nincs hülyébb állat a világon!" Hogy ki mondta nem tudom, de mindig tetszett, mert sajnos igaz.
Ez olyan mintha a twitteres hack felkijáltójelét írta volna le valaki büntetésből százszor.
Sajnos hülyékből mindig van utánpótlás. És ez igaz magamra és mindenkire egyaránt.

Ami a csövön kifér

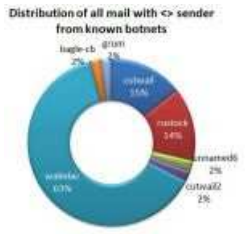
2009.07.31. 16:10 | Csizmazia István [Rambo] | 1 komment

Címkék: spam teszt zombi botnet storm sebesség eset waledac

Az **ESET kutatói eljátszottak a botnetes Waledac kártevővel**, és a forgalom elemzésével méregették a botnet spam kibocsátási képességeit.

A Latin-Amerikában végzett tesztelés szerint már egyetlen bot fertőzte számítógép is másodpercenként két spam levelet, illetve egy teljes nap alatt pedig mintegy 150 ezer kéretlen reklám levelet képes kibocsátani. A **szándékosan megfertőzött laboratóriumi PC a Valentin napi kártevővel állt be a botnetek sorába**, majd ennek kapcsán nyílt alkalom **a hálózati forgalom alaposabb vizsgálatára** is. A Waledac számos tekintetben felülmúlja a korábbi Storm képességeit, és annak reinkarnációjának tartják.

Sebastian Bortnik egy blogbejegyzésében a Waledac botnet méretét 20 ezer gépre becsüli, és ennek teljesítőképességét pedig **napi 3 milliárd kiküldhető spam** levél jellemzi. Természetesen ezek a becslésekkel készült botnetes elméleti teljesítmények **valójában tényleg csak elméletiek, hiszen a botnetet általában sosem használják ki** teljes üzemidőben és teljes kapacitással.



Az elemzés kimutatta, hogy a Waledac valóban a Storm utódjának tekinthető, és **fejlesztésénél figyelembe vették az elől csiszolandó képességeit**, például míg a Storm csak 64 bites RSA kódolási algoritmust használt, a Waledac már ebben is előrelépett, és minden tekintetben folyamatosan továbbfejlődött az év eleji Valentin naptól egészen a július 4. Függetlenség Napja ünnepekig.

Mindenesetre ha valakinek nagyon lelassult a gépe, és tudtán kívül egy botnet zombihadsereg katonája, **ezekből az adatokból megértheti, hogy például hová is tűnik, mire fordítódik az elhappolt sebesség és teljesítmény**.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat

- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1279038

Kommentek:

prof. Perselus Piton 2009.07.31. 16:17:17

Ezek rosszabb számok,mint a valódi vírusok szaporodási mutatói. Egymásnak kellene engedni az új influenza vírusát és a fertőzött gépeket :-S :-))

Rossz-e, aki rosszra gondol?

2009.08.03. 21:11 | Csizmazia István [Rambo] | 3 komment

Címkék: weboldal pdf who unlock knows

Mert ugyebár az is lehet, hogy ez a munkája. Aki (számítógépes) biztonsággal foglalkozik, annak agyában folyamatosan a legrosszabb forgatókönyv elemeinek kell pörögnie, mindenre gyanakodnia kell, akkor dolgozik jól. Illetve **aki nem ezt teszi, az nem képes reálisan felmérni a lehetőségeket, és kezelni a kockázatokat**.

Látókörünkbe került egy weboldal ;-), és a nagy meleg ellenére igyekeztünk vadászkutya bőrbe bújni. Körbeszaglásztunk, reménykedtünk, és elfilozofálgattunk picit. **Kavarja ez vagy nem kavarja** - tettük fel magunknak a Rejtői kérdést, és sokszor éreztük úgy magunkat, **mintha már éppen rajtakapnánk Piszkos Fredet valami rafinált furmányos trükkön, de aztán mégsem** így lett. A végkifejlet végül nyitott maradt, de erről majd később. A weboldalt alig pár napja, 2009. július 31-én jegyezték be, múltjáról és a tapasztalatokról ezért nem sokat beszélhetünk. A hamis vírusirtók piacán tapasztaltuk rendre azt a jelenséget, hogy a hangzatos nevű, 2010 Antivirus és hasonló programok weboldala szintén mindössze pár napos bejegyzésűek. **Emiatt a bizalmi index nálunk rögtön alacsony buxban kezdett**, de lehet, hogy valóban anonim grállovagok szamaritánusi ingyenmunkájáról van csak szó, ami éppen most indult világhódító útjára.

Kissé ugyan hihetetlen, mert Krisztus koporsóját sem őrizték ingyen, miközben valakik ingyen segítenek nekünk a mai anyagias világban a PDF-eket "locktalanítani", de legyünk megengedőek, adhatunk ennek is egy esélyt. Igaz, **a Linux, meg az Open Source keretében tényleg vannak sokan, akik a saját magukat érdeklő témák megoldásait mások számára is ingyen hozzáférhetővé teszik**, jobbára saját névvel és forráskóddal - de ezek a szimptómák valamint **az erre utaló licencek azonban most itt nincsenek jelen**. A gyanakvóaknak különben is sokkal szimpatikusabb a "letöltöm a progit, és én használom, én végzem el a saját gépemen", mint a "megosztom és odaadom az állományaimat, és reméljük, úgysem akarnak nekem rosszat a bácsik és a nénik" metódus. A weboldal **előre jelzi, hogy csak a PDF állományokban lévő korlátozások eltávolítását ígéri**, de leszögezi, a megtekintés ellen jelszavazott állományt és a DRM-mel elátott fájlokat nem nyitja, ezeket nem távolítja el.

Na uccu neki, letöltöttünk **egy Nikon D300 nem nyomtatható angol nyelvű műszaki leírást, és mi magunk is generáltunk neki egy kopi-paszta és print funkciók tiltását tartalmazó egysorost**, és megnéztük, mit lép rá. Mielőtt esetleges fanyalgó kommentek arról kezdenek szólni, hogy a majom nem ly, máris jelezzük, hogy ez szándékos és ennyi szórakozás nekünk is kijár a 36 fokos melegben. Magunk közt szólva **ezek az ósdi funkció korlátozások csak a Windows juzereket érintik**, náluk lehet hogy nem tudnak nyomtatni, kijelölni, de egy Linux alatti **foolabs féle Xpdf nagy ívben tesz ezekre, és mind a korlátozott, mind a nyitott állományt egyformán és simán** képes kedvünk szerint és mindenféle limitálásoktól mentesen kezelni.

A **Nikon doksi felkoppant a próbán a maga nem túl jelentős 15 MB méretével**, ezért maradtak a saját állományaink. Na szóval a Windowsos Adobe és Foxit Reader szépen teljesített, hűséges pulikutyaként valóban csak akkor engedte a nyomtatást, amikor mondták neki, hogy szabad, szóval a szolgáltatás korrektül működött ;-)

De ekkor már kezdett emelkedni az adrenalin, és az állítólagos Alexey Tolstokozhev gaz spammert fejbelövős média hack rémlett fel. Igazából **arra számoltunk, hogy a korlátozásoktól mentesített PDF állományokban egy jó kis exploitot fogunk feldezni, ez szinvonalas trükk lett volna**, de ilyesminek nem leltük nyomát. Vagy nulladik napi exploitot tesznek bele ;-), vagy nem is tesznek bele semmit, vagy **esetleg majd csak később a beetető időszak után**, mikor már mindenki mindenkinek pavlovi reflexekkel ajánlgatja. Ha mégsem, akkor lehet még ipari kém, aki például a kíváncsi munkavállalókra apellál, és neki aztán minden feltött dokumentum ott lesz egy kupacban. Lehet, hogy egy ismeretlen ország nemzetbiztonsági hivatalának munkatársa, vagy **egy magánnyomozó a munkaadók képviseletében**, aki aztán bizonyítékokat gyűjt, ki mikor milyen IP címről milyen vállalati dokumentumokat töltött fel, amikhez elvileg legálisan nem is juthatott volna hozzá. **A lehetőségek tárháza végtelen.** "Csak az nem fél, akinek nincs fantáziája" - mondja Rejtő Jenő.

Könnyen **lehet, hogy nem túl egészséges, ha valaki ennyire gyanakvóan gondolkodik**. Nekünk azonban legvégül még a fentieken felül az "Andreiground" effektus is eszünkbe jutott az ingyenes NOKIA telefonfüggetlenítő weboldalával. Persze ez a PDF-es story is lehet még bármi, majd az idő eldönti. Lehet, hogy tényleg **"csak a málnaszőrt kavarják"**, de az is lehet, hogy aztán öt év múlva ebből lesz a Hacktivity-n egy jól sikerült előadás **"És a sok lúzer mind betöltötte..." címmel :-D**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1285160

Kommentek:

Su Larsen (törölt) · http://sularsen.com 2009.08.04. 00:25:13

"ezek az ósdi funkció korlátozások csak a Windows juzereket érintik, náluk lehet hogy nem tudnak nyomtatni, kijelölni"

wow és még a linuxra mondják, hogy nem jó. :D

Droli · http://nivo.blog.hu 2009.08.05. 12:51:33

Némi off, de nem akkora: megírtam az antivirus blog paródiáját is a blogparódián.

blogparodia.blog.hu/2009/08/05/antivirus_top_5_kartevo

Nekem, mint laikusnak nagyon tetszik amúgy az antivirus blog, csak így tovább! :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.08.05. 13:29:48

Hello Droli!

Megtiszteltetés, hogy ilyen előkelő helyen sorrakerülhettem a teritéken :-) Sokszor gondolkodtam már, hogy egy laikusnak egy ilyen toplista, de akár az egész számítástechnikai szleng, vírusveszély, stb. mit mondhat, és te sikeresen megmutattad ezt ;-)

Neked is sok sikert a blogodhoz, szerintem remek és hiánypotló gondolat volt ezt kitalálni.

Még kémprogramra sincs szükség...

2009.08.05. 19:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: usa fájlmegosztás korlátozás fájlcsere kémkedés adatszivárgás

...ahhoz, hogy egynémely esetben bizalmas adatok, információk kerüljenek ki a kormány- és egyéb hivatalokból. Persze ne legyenek illúzióink, azokat is alkalmazzák, a kiemelt célpontok ellen akár egyedi fejlesztésűeket is bevetnek. Egy mostani jelentés szerint **bizalmas névjegyzékek, adóbevallások, és más hasonló titkos állományok megtalálhatók különféle fájlcserélő oldalakon is**.

Az információ szivárgások miatt ezért az Egyesült Államokban rendelettel tervezik szigorítani a fájlcserélő, fájlmegosztó alkalmazások telepítését kormányhivatalokban, titkosszolgálatoknál, és hasonló érzékeny adatokkal dolgozó helyeken. A felmérés nem utal egyértelműen szándékosságra, a feltételezések szerint **az incidensek egy része keletkezhet akár úgy is, hogy véletlen fájlmegosztás történik**. Mindenesetre **elérkezettnek látják az időt, hogy lépéseket tegyenek az információk védelmében**.

Emlékezetes, hogy a kínai támadók már piszkálgattak ezt-azt a Pentagonban, emellett pedig a feltételehetően észak-koreai támadók folyamatos és erős támadásokat intéznek az USA ellen is, és igyekeznek minél több bizalmas adatot megszerezni illegálisan **elektronikus úton**. Képzelhetjük, **mekkora sikerrel járhat egy többezer főből álló kiberhadtest**, ha egyetlen találékony fickó mindössze egy kitalálható hotmail jelszóval így lealázta a Twittert.

Látni kell azt is, hogy **hiába alkalmaznak erős titkosítást, titkosított fájlrendszert az ilyen gépeken, ha azon pillanatnyi nyitott állapotukban mappákat, fájlokat osztanak meg** másokkal, sokszor nem is szándékosan. **A fájlmegosztók telepítésének korlátozása lehet az egyik lépés** ez ellen, ami nélkül viszont garantáltan nem lehet előrelépés, az pedig **ennek szigorú és következetes betartatása**. Katonai alakulatoknál szokás, hogy **minden reggel vizitszerűen sorakozni kell a noteszgépükkel átvizsgálásra**, és a rutinellenőrzés percek alatt kimutatja, hogy csak az engedélyezetten telepített programok szerepelnek-e, vagy esetleg más is.

Persze **ha ezt nem egészíti ki az internetes forgalom hatékony ellenőrzése, akkor ez sem óv meg egy délután telepített fájlcserélőtől** másnap reggelig ;-) **És ami egyszer már felkerült a netre, az a tapasztalatok szerint ott is marad...**

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben

- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1289946

Kommentek:

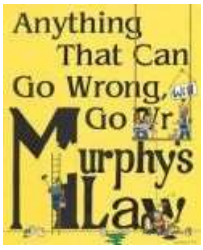
Nincsenek hozzászólások.

Mindörökké Murphy

2009.08.06. 16:28 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: letöltés link ppt eset kártevő slideshare.net

Ami elromolhat, az el is romlik - mondja az ősi igazság. Ennek analógiájára gondolhatjuk úgy, hogy **ami megtörténhet, az meg is történik - előbb-utóbb**. Most éppen egy prezentációkat megosztó oldalon bukkant fel olyan slide, amelyben hamisított, a SourceForge.Net linkjének látszó, de valójában kártevőket terjesztő oldalra mutat.



Sokan **túlságosan is megbíznak a PPT állományokban**, azonban úgy tűnik, sosem lehet az ember elég gyanakvó. Az ESET kutatói figyeltek fel rá, hogy egy ilyen megosztott állományban szerepelt egy olyan oldal, **amely a NOD32 antivírus program feltört változatának letöltési linkjét ajánlotta fel**. A PPT előadás ezen lapján egy SourceForge.Net logó is szerepelt - bár magunk közt szólva aki kicsit is ért hozzá, annak **semmilyen logó nem legalizálhat egy feltört programot**. Meg hát hamisított plecsnikről is értekeztünk már egy doktori disszertáció keretében korábban. De hát a nagy számok törvénye, a kevésbé hozzáértők, és a figyelmetlenebbek közül mindig akad, aki az ilyen "Látja? Nem látja? Na látja" trükköket beveszik, **miattuk érdemes űzni ezt a kártevőterjesztő ipart**.

Ha ugyanis rákattintanak a linkre, akkor egy **SourceForge.Net oldanak "látszó tárgy" tűnik fel a böngészőben, amely azonban kínai oldalakról a Win32/Kryptik.YT kártevőt** vagy a hamis vírusirtót telepítő Win32/TrojanDownloader.FakeAlert.ADB állományt tartalmazza.

A dolog különleges **érdekessége abban áll, hogy egy eredetileg tiszta, ellenőrzött (PPT) állományban is lehet beágyazva olyan link, amelyre kattintva viszont már on the fly érkezik is a menetrendszerű kártvő**. A figyelmeztetés után a SliideShare.net szerencsére **megtette a szükséges lépéseket, és eltávolította** az inkriminált fájlt.

Jól látható, hogy **a támadók folyamatosan keresik az új utakat**, az új helyszíneket, emellett sok igazi letöltő oldal sincs a topon a saját ajánlott programjaik ellenőrzése frontján. Végül **a kártevő terjesztőknek nem nagy kunszt egy hamis oldal összerakása**, hiszen a feladat annyira triviális, hogy "a hülye is tud letöltési oldalt készíteni". Ezért hát oly **jó lenne, ha mi viszont mégsem lennénk annyira hülyék, hogy ezeknek be is dőljünk**. Kezeket a paplan fölé, ne használjunk feltört warez programokat, és nem mellesleg éljen a blogparodia.blog, ahol tegnap mi is jól megkaptuk a beosztásunkat:-D

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás

- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori
- 25-ször több a mobilos kártevő

bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1292307

Kommentek:

Nincsenek hozzászólások.

Elszabadulnak a vírusok a Szigeten

2009.08.10. 19:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: játék a sziget kórház lemez nyeremény 2009 eset szélén

Több szervezet figyelmeztetést adott ki, melyek szerint idén a Szigeten különösen óvakodni kell a vírusoktól. Az ESET magyarországi képviselete most arra hívja fel a figyelmet, hogy **a helyzet még súlyosabb lehet, mint gondoltuk ;-)**

Az ESET magyarországi képviseletét ellátó Sicontact Kft. figyelmeztetése szerint idén a Szigeten nem csupán az egészségügyi szempontból **veszélyes kártevőkkel kell számolnunk**, hanem a leggyakoribb, illetve leghírhedtebb számítógépes vírusok előfordulásával is.

A fenyegetés **szerencsére ezúttal nem komoly, pusztán a NOD32 antivírust forgalmazó cég játékáról van szó**. A **Sziget Fesztivál első két napján, szerdán és csütörtökön 15 „vírus" fog elvegyülni a látogatók között**, a vírusvadászoknak őket kell elfogniuk. Aki **megtalálja a kártevők neveit pólójukon viselő beépített személyeket**, és bemondja a játékhoz tartozó jelszót, az **értékes ajándékot kap**.

Pár példa az elszabadult vírusokra:

3. Win32/Virtumonde

A mosolygós külső erősen megtévesztő.

A hátteret érdemes szemügyre venni, mely többet elárul a kártevő habitusáról.

Veszélyesség foka: 8/10
Elkövetett cselekmények: Egyike azoknak a vírusoknak, amik a legtöbb problémát okozzák Magyarországon. Fenyegetéssel, ijesztgetéssel megfélemlíti áldozatait, majd védelmi pénzt követel tőlük. Eddig több ezer esetről és áldozatról tudunk.
Szigeten várható előfordulási helye: Ütemes Ting Tings zenére aktiválódik.
Mit kell tenned, ha találkozol vele: **Súgd a fülébe, hogy "Kórház a lemez szélén"**, és vigyázz. Ne tévesszen meg, hogy kezdetben nagyon barátságosnak mutatja magát.

5. Win32/Agent

Kacér pillantásokkal próbálja meg tömegben felhívni magára a figyelmet.

Gyanútlan áldozatát nem ritkán kannibalizálja.

Veszélyesség foka: 7/10
Elkövetett cselekmények: Nem gondolnád róla, de igazi bajkeverő. Az áldozatainak személyes adatait és jelszavait igyekszik megszerezni, majd ezeket értékesíti a nemzetközi feketepiacon. Magyarországi áldozatainak száma több ezerre tehető.
Szigeten várható előfordulási helye: Lily Allen rajongó. Várhatóan a Ska-P-n is ott lesz, belső információink szerint ezen a koncerten nagyobb feltűnést fog kelteni.
Mit kell tenned, ha találkozol vele: **Súgd a fülébe, hogy "Kórház a lemez szélén"**, és légy vele barátságos. Nem szabad elfelejtened, hogy fokozottan veszélyes, de egy sörrel vagy Irsai Olivérrel könnyen lekenyerezhető.

A **részletes játékleírás** a www.eset.hu/virusvadaszat oldalon található. **Sok sikert mindenkinek a játékhoz!**

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1300474

Kommentek:

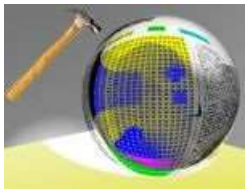
Nincsenek hozzászólások.

Toplistán a particiós táblát törlő vírus

2009.08.11. 15:51 | Csizmazia István [Rambo] | 4 komment

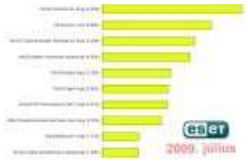
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az **ESET szakértői szerint** a vírusfertőzések többségét a múlt hónapban is meg lehetett volna előzni, ha a felhasználók frissítik az operációs rendszerüket és fontos alkalmazásaikat. A tét ráadásul most megnőtt, **a magyar vírustoplista 9. helyére került Mebroot.K ugyanis törölheti a merevlemez partíciós tábláját**.



A **múlt hónapban listavezető pozíciót elért Conficker** 2008 novemberében bukkant fel, és azóta rendszeresen szerepel a magyarországi vírustoplistákon. A kártevő egy olyan hálózati féreg, amely a Microsoft Windows egy biztonsági hibáját kihasználó kóddal terjed. Bár a Microsoft már tavaly októberben kiadta a megfelelő javítócsomagot, sok felhasználó nem fordít figyelmet az operációs rendszer frissítésére. A Conficker így hazánk mellett több országban – például Brazíliában, Ukrajnában és az Egyesült Államokban – is listavezető.

A júliusi toplista **második helyére az Autorun/Inf fertőzés került**, mely gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. Az ESET szakértői szerint már nem csupán az USB kulcsok, de az USB portba csatlakoztatható MP3 lejátszók is hordozhatják a fertőzést, mely ellen **a legegyszerűbben az automatikus futtatási funkció letiltásával védekezhetnének** a felhasználók.

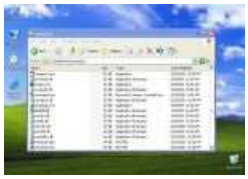


Végül a legérdekesebb a lista új szereplője, a Win32/Mebroot.K trójai. Bár **a kártevő már közel egy éves ismert**, most mégis felkerült a toplista 9. helyére. A trójai amellett, hogy további kártékony kódokat igyekszik letölteni a megfertőzött számítógépre, tönkreteheti a merevlemez partíciós tábláját is, **ami azzal jár, hogy nem tudunk hozzáférni az adatainkhoz**.

Végezetül következzen a magyarországi toplista. Az **ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2009 júliusában** az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek együttesen 35.20%-ot tudtak a teljes tortából kihasítani maguknak.

1. Win32/Conficker.AA féreg
Elterjedtsége a júliusi fertőzések között: 6.45%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: http://www.eset.hu/virus/conficker-aa

2. INF/Autorun vírus
Elterjedtsége a júliusi fertőzések között: 5.04%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3 lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

3. Win32/TrojanDownloader.Bredolab.AA trójai
Elterjedtsége a júliusi fertőzések között: 4.29%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, mely távoli oldalakról további kártékony kódokat tölt le és hajt végre. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is a bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-bredolab-aa

4. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a júliusi fertőzések között: 4.05%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

5. Win32/Kryptik trójai
Elterjedtsége a júliusi fertőzések között: 3.18%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm, illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.
Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/kryptik-gt

6. Win32/Agent trójai
Elterjedtsége a júliusi fertőzések között: 3.04%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .dat illetve .exe kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

7. Win32/PSW.OnLineGames.NMY trójai
Elterjedtsége a júliusi fertőzések között: 3.01%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon értékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nmy

8. WMA/TrojanDownloader.GetCodec.gen trójai
Elterjedtsége a júliusi fertőzések között: 2.74%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

9. Win32/Mebroot.K trójai
Elterjedtsége a júliusi fertőzések között: 1.71%

Működés: A Win32/Mebroot.K trójai elsődleges célja, hogy további számítógépeket fertőzzön meg. Ehhez az ideiglenes (Temporary) mappában létrehoz egy <szám>.tmp nevű fájlt, valamint a rendszerleíró adatbázisba számos bejegyzést hoz létre, illetve módosítja azokat, ha már léteznek. Ezenkívül megkísérel a google.com webcímre is csatlakozni. Működése során tönkreteszi a merevlemez partíciós tábláját.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/mebroot-k

10. Win32/Toolbar.MyWebSearch alkalmazás
Elterjedtsége a márciusi fertőzések között: 1.69%

Működés: Internet Explorer és Firefox alatt működő keresőszolgáltatás, amely kéretlenül reklámprogramokat helyez el a PC-n. Telepítésekor számtalan kulcsot módosít a rendszerleíró adatbázisban, és kéretlen reklámokat jelenít meg az adott számítógépen. Az alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó maga tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/toolbar-mywebsearch

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1302780

Kommentek:

Vargnatt 2009.08.11. 18:19:21

Most akkor ez a Mebroot mindenképpen kinyírja a PT-t, vagy csak működhet olyan bénán, hogy mellékhatásként azt is

tönkreteszi? És főleg: hogyan terjed, hogyan lehet megelőzni a fertőzést? Van valami specifikus rés, amit kihasznál?

Vargnatt 2009.08.11. 18:22:05

Ja, és még valami: két merevlemez esetén mindkettőn tönkreteszi a PT-t?

roli · http://nivo.blog.hu 2009.08.13. 21:05:09

A Conficker vírus első helye számomra hihetetlen... tavaly hatalmas figyelem övezte, mindenből ez folyt, azt hinném, hogy ettől az emberek jobban figyelnek a frissítésekre és a vírusirtók fontosságára - s lásd, az a dög ott van az első helyen. Azért ez valahol szomorú, mert még pénzbe sem kerül kivédeni, hiszen a biztonsági frissítések letöltése nem kerül semmibe, s van ingyenes vírusírtó-tűzfal-kémporgrameltávolító is... szóval gáz.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.08.23. 14:57:52

Szia Vargnatt!

Amit az ESET Mebroot.K-nak nevez, abból több is van, így nehéz általánosan válaszolni a kérdésekre.

> Most akkor ez a Mebroot.k mindenképpen kinyírja a particois tablat,
> vagy valamilyen feltetel teljesules eseten?
Nem kinyírja, hanem megfertőzi, azaz a saját kódját beleírja az MBR kódjába.

> hogyan terjed, hogyan lehet megelőzni a fertőzést? Van valami
> specifikus rés, amit kihasznál?
Fileból indítva megfertőzi az MBR-t, utána onnan IS tud indulni. Nem mindig fertőzi az MBRt azonnal, esetenként várni kell rá, általában 10-15 perc elég.

> Ha ket merevlemez van a gepben, akkor mindkettot, vagy csak a
> bootosat?
Mind a kettőt meg tudja fertőzni.

Rövid szélcsend

2009.08.17. 10:05 | Csizmazia István [Rambo] | Szólj hozzá!

Nem, nem siklott ki az antivirus.blog.hu vonata. Mindössze **néhány napra elcsendesül a blog némi nemű szabadság** és családdal eltöltendő idő ürügyén, hogy aztán a 20-i ünnepek után újult erővel jöjjünk vissza.

Addig is hébe-hóba a Twitteres mikroblogon jelzünk ezt-azt, ha lesz valami érdekesség.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1314482

Kommentek:

Nincsenek hozzászólások.

DDoS-oljuk meg együtt Obamát!

2009.08.24. 14:41 | Csizmazia István [Rambo] | 4 komment

Címkék: spam malware obama kártevő becsapás ddos

A pályaválasztási tanácsadókban **a kreatív gyerekeknek akár a spammer szakmát is ajánlgathatnák;-)** Mert nem igazán jellemző rájuk, hogy bármikor is kifogynának a trükkökből, ötletekből. Most éppen a **"Nem kedveli Obamát? Akkor itt az alkalom, töltse le a mellékelt linkről ezt a szoftvert, és terheljük túl együtt az utált politikus weboldalát (Fehér Ház)!"** című kéretlen e-mail jelent meg a repertoárjukban.

És mindig van, aki belemegy a játékba, **letölti a mellékelt linkről a szoftvert**. Sajna nem lehet minden link mellé egy külön rendőrt állítani. Amikor pedig kap egy értesítést, hogy **antivírus programja lehetséges, hogy kártevőként fogja felismerni, azt tanácsolják neki, ne is törödjön vele, ez normális, kapcsolja le nyugodtan a védelmet**. (Ezt a Barba trükköt már láthattuk korábban néhány warez szériaszám generátornak látszó programnál is.)

Szóval egyszerre két dolog kell hozzá, hogy az ember komplett hülyét csinálhasson magából. Robin Hood-i lelkesedéssel belevetni magunkat **az állítólag közutált csúnya politikus DDoS-os móresre tanításába** (ami nem mellesleg büntetendő), de emellett annyira naívnak is kell lenni, hogy **közben mi magunk legyünk azok, akik kézzel lekapcsolják a vírusvédelmet, és kitárjuk az ajtót a kártevőknek**. Egyik sem látszik követendő metódusnak.

Emellett reméljük, a módszerből nem kap tippet a magyar számítógépes alvilág. Mert hogy **nem kedvelt vagy közutálatnak örvendő magyar politikusból nem csak hogy nem szenvedünk hiányt, hanem jelentékeny túlkínálat is van napjainkban** ;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1334455

Kommentek:

atko 2009.08.24. 18:25:16

A vicc jó! Sajna szerintem csak annyian értik, mint a Chuck sorozatban a Tron poszter emlegetését. :-D
Mindig mondom, jogosítvány kell a géphez!

El Argentino 2009.08.24. 18:49:13

:) mókás

rodimus_prime 2009.08.25. 21:34:52

off
Helló Rambo

Privát ment, előre is hálás köszönet

off/

rodimus_prime 2009.08.25. 21:35:31

Akarom mondani, indára :)

Még nem is létezik, de mi már letölthetjük

2009.08.26. 19:25 | Csizmazia István [Rambo] | 1 komment

Címkék: os macintosh reader x pdf trójai kártevő foxit

Korábban sokan úgy tekintettek a PDF állományra, mint abszolút megbízható és biztonságos formátumra - nos ez a helyzet mára gyökeresen megváltozott. Az Adobe Readertől sokan **nem csak az olvasó lomhasága, nagy mérete, hanem ritka biztonsági frissítései miatt is elpártoltak**, és választottak helyette alternatív olvasókat a Sumatra vagy éppen a FoxIt Reader személyében. De minden csapástól ez sem óv meg.

Természetesen jó választások ezek a kisebb, gyorsabb és biztonságosabb dokumentum olvasók, de persze **arról szó sincs, hogy ezekben - ahogy bármi másban sem** - ne lehetne kihasználható hibát keresni és találni. A mostani akció keretében **kedves fele- és egész barátaink a Foxit Reader for Mac verziót ajánlgatják a nyájas érdeklődőknek**, és ebben az a tény sem zavarja őket a legcsekélyebb mértékben sem, hogy **a nevezett szoftver csak és kizárólag Windows, Windows Mobile illetve U3 / Desktop Linux alá van kifejlesztve**. A nem lézető Mac változatra mutató link - tegye fel a kezét, aki meglepődött, igen-igen, ott a második sorban :-) - hogy hogynem kártevőre bír mutatni. És igen, egy korábbi OS X alatt futó trójai programot rejt, **ami néhány hónappal korábban még kodekletöltési trükkel próbálta meg a gyanútlan felhasználók** gépét megfertőzni.

Az ilyen kodek letöltési megtévesztés és egyéb hamisított telepítési csomagok jelentik az egyetlen esélyt az OS X-en a kártevő terjesztőknek, **a Windows-zal szemben ugyanis itt semmi nem fut le automatikusan**, kénytelenek tehát a felhasználót valamilyen furmánnyal rávenni, ugyan legyen oly bátyánk, és telepítse már fel az általunk oly hőn kínált trójait.

Korábban már mi is beszámoltunk, hogy egy létező kémprogram-irtó nevét bitorolva egy másik ugyanúgy Spyware Terminátor nevű csalárd alkalmazás is feltűnt a színen kártevőket terjesztve, de az AVG vírusvédelmi cég programját is hamisították már, akárcsak a Flash Playert. Sajnos úgy tűnik, semmi nem szent, ha eredményt kell elérni, mindent megpróbálnak hamisítani. Ezért **már most lehetne gondolkodni** a majdan bevezetendő "hamisítás felismerési alapismeretek az általános iskola 3. osztályos tanulóinak" című tantárgy gerincén és szofisztikált törzsanyagán ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1339080

Kommentek:

atko 2009.08.26. 11:40:21

Okulásul okular kde alatt más nem is kell.
A gép tévedhetetlen, az ember aki tervezi és használja nem.

Mit tegyünk, ha zavarják drága time?

2009.08.27. 16:32 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam drága time kínai magyarul webáruház nyersfordítás

Sprechen Sie Deutsch? Do You Speak English? Govoritye po Russzkij? Csupa-csupa felesleges mondat ez, hiszen szemlátomást átvette ezen ódivatú módszerek helyét az instant kínai-magyar nyelvjárás, ami ha nem is olyan világrengető hír, mint az afrikai magyar törzs, de azért valamilyen szinten határokat döntöget és közelebb hozza népeinket.

A kínai levélírók szemlátomást világuralomra törnek: **a földrajzi és nyelvi korlátok bilincseit egyaránt feszegetik**. Mivel pár héten belül **már a harmadik ilyen esik a postaládánkba**, megmutatjuk őket: **hogyan szpemmeljünk bármilyen nyelvről bármilyen nyelvre** translate.google.com-mal, és itt közben mindenki gondoljon egy olyan barátjára-ismerősére, aki két sör után már bármilyen nyelven képes kommunikálni.

Nagyjából a magyar bankok elleni adathalász levelek nyelvi cizelláltságát és helyesírási szimptómáit hordozza magán **az a pár levél, amit kínai barátaink orvul lenyomtak a Google automata fordítójának torkán**. Persze értjük mi, nem könnyű a magyar, erre ékes bizonyíték, hogy rajtunk kívül nem is beszéli senki ;-) A helyi Tusko Ching Hopkins és Fülig Chang Lee Jimmy mindent megtett, hogy a kötött magyar nyelvtani szabályrendszer nüanszai dacára nemzetközi üzleti kapcsolatuk kapuját minél szélesebbre tárja.

Következzenek hát az emlegetett gyöngyszemek "Halló, egyen zabot!" stílusban, a színpad ezúttal a Tai Pitypang műveké ;-)

Levél #1.

Levél #2.

Levél #3.

Vegyük észre, hogy a második üzenet ráadásul van olyan pofátlan, hogy "Re: Helllo" subjecttel közelítsen felénk nagy kéretlenül. A levelek **a magyar nyelv elleni merényletet leszámítva látszólag sima spamek** voltak, a weboldalakon elsőkörben nem találtunk semmilyen kártevőt, de **a jövőben persze ez a forgatókönyv sem zárható ki**, ezért hasonlóan a gyógyszeres reklámokhoz, érdemes kellő kétkedéssel és távolságtartással fogadni ezeket.

Ha netalántán **van olyan olvasónk, aki már sikeresen vásárolt be** bármilyen műszaki cikket a "Tai Pitypang" dohány, tabak és gyarmatárú nagykereskedésből, **kérjük ossza meg velünk** értékes tapasztalatát egy komment erejéig ;-) Addig is, **amíg telik a "drága time"**, éljen soká és virágozzék a leleményes internacionalista nyelvi igényesség!

Ajánlott bejegyzések:

- □ártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1341255

Kommentek:

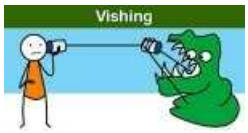
Nincsenek hozzászólások.

Népszerű a telefonos adathalászat

2009.08.31. 19:15 | Csizmazia István [Rambo] | 3 komment

Címkék: kína telefon csalás vishing adathalászat

Folyamatosan **nő a trükkös elkövetők által üzött vishing**, vagyis telefonos adathalászat. Nem egyszerűen csak telefonálgatnak, hanem **iparszerűen hamis call centereket üzemeltetnek** a bűnözők.



Koreai áldozatok bejelentése alapján indítottak nyomozást Kínában, melynek során olyan **elkövetőket kerestek, aki érzékeny információkat kíséreltek meg gyanútlan áldozatoktól megszerezni**. Az akció keretében ezúttal 22 embert tartóztattak le, nyolc tajvani és 14 kínai-koreai állampolgárt. **A csalók tisztviselőknek, banki alkalmazottaknak, rendőröknek adták ki magukat**, és napi tíz órában véletlenszerű tárcsázással hívogattak koreai állampolgárokat, akiktől személyes adatokat, jelszavakat, banki accountokat próbáltak állítólagos ellenőrzés céljából bediktáltatni, illetve a begépeltetni.

A leleplezés sikeréhez nagyban hozzájárult, hogy **egy kínai□koreai titkosügynök beépült az adathalász maffiába, és a belülről megszerzett információk segítségével** sikerült végül a társaság letartóztatása. A nyomozás kiderítette, jól szervezett bűnbandával volt dolguk. A profi bűnözők Dél-Kínában **nem csak egyszerűen üzemeltettek egy ál callcentert, hanem magas fokon konspiráltak, lakásokat béreltek, amiket rendszeres időközönként cseréltek**, hogy nehezítsék a felderítést. **A munkát felosztották részlegeik között**, így voltak, akik a telefonos hálózatért voltak felelősök, egy másik csapat a szükséges beszélgetési sémákat fejlesztette, míg **egy harmadik brigád végezte e forgatókönyvek alapján a telemarketinges munkát a véletlenszerű számok tárcsázásával**.

A csoport tagjai "munkájuk" után **nem csak alapfizetést kaptak, de teljesítmény ösztönző bérezésben** is részesültek. A tavaly külön e célra alakított koreai nyomozó csoport **eddig már 129 elkövetőt tartóztatott le** összesen 13 különböző vishing bűncselekmény gyanújával.

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1351271

Kommentek:

magocska 2009.09.15. 17:20:50

Csak akkor tudják megszerezni ezeket az adatokat, ha kiadjuk őket. Emberek! Gondolkozni!

neofin 2009.09.17. 00:21:46

Nálunk is vannak hasonló dolgok ...

Saját tapasztalat :
- Bank felhív [Nem jelzi ki a számot] , hogy speciális információt akar velem közölni, de elősször szeretne azonosítani ...
Első kérdése : anyja neve ?
Aztán kiderült, [miután visszahívtam, hogy csak egy egyszerű ajánlat :( ]

- Utazási szokásaimról érdeklődnek ...
[mi a garancia, hogy nem az APEH vagyonosodási vizsgálattól hívnak? :)]
A múltkor meg is kérdeztem a telefonos hölgytől, honnan tudjam, hogy őn nem Az APEH-től hív fel?

---

pepita ceruza • http://80037134749768090 73.slide.com/ public pr true 2009.09.17. 14:29:19

én, már a(z új) telefonszámomat se adom meg szívesen senkinek az ismerősökön kívül, szóval, eleve kiküszöbölöm a hívásokat.
A bank közölje velem az óhajait írásban.

Hamarosan Hacktivity

2009.09.02. 08:10 | Csizmazia István [Rambo] | 2 komment

2009. szeptember 19-én és 20-án kerül sor a **Hacktivity 2009 konferenciára, új, tágasabb helyszínen** a Trefort Kertben lévő Gólyavár Rendezvényközpontban. A sorban **immár hatodik Hacktivity** a legrégebbi hazai független IT biztonsági konferencia, ahol hagyományosan az információbiztonsági szakma legrangosabb **hivatalos és „nemnyakkendős" képviselői jönnek össze** a téma iránt élénken érdeklődőkkel.

Bár az eseményre jellemző az oldott, kötetlen stílus, a tartalom ennek ellenére – vagy pont ezért? – rendkívül nívós, sok új ismeretet nyújtó, mélyen technikai. Bár hazánkban még nem tudunk róla, a külföldi társrendezvényeken már évről-évre résztvevő a titkosszolgálat is.

Amerikában és Európa egyre több országában is évek óta gyakorlat már az olyan IT biztonsági konferenciák sora, ahol az öltönyös cégvezetők mellett megjelennek a formaságokra cseppet sem adó informatikai guruk, sőt a felsőoktatásban informatikai képzésben részesülő diákok is. Tény, hogy **egy-egy ilyen rendezvény olyan fórumot kínál a felhasználók által érzékelt információbiztonsági, jogi, szociológiai problémák ismertetésére, amelyet más konferenciák nem igazán tudnak megoldani**, éppen ezért ezek a rendezvények mindenhol egyedinek számítanak a szokványos konferenciák között.

A Hacktivity-re nagyon jellemző az interaktivitás melyet az idén három új program elemmel is támogatnak a szervezők!

A „Hack the Vendor" verseny keretében a résztvevőknek lehetőségük lesz a saját területén piacvezető (és bátor) **McAfee cég két információbiztonsági termékét tesztelni, vagyis legális keretek között feltörni azt a helyszínen**. Ennek a versenynek a célja, hogy nem megszokott módon hívja fel a szakértők figyelmét a gyártó valamely termékére, pláne a szerencsés hacker tehetségére. A feladat egy átlagosan elkészített - és ezért néhány helyen hibás - web alkalmazás feltörése, miközben a rendszert a McAfee betörés megelőző termékei (IPS) védik.

A BYOL (hozd magaddal a saját laptopod) workshop – A második nap vélhetően egyik legérdekesebb programjának a francia Joffrey Czarny workshopja ígérkezik, melynek keretében **minden résztevő a saját laptopján az előadóval együtt végezheti el egy hibásan konfigurált CITRIX © rendszer hackelését**.

A **megújult Wargame játékban a szervezők rögtön 3 különböző nehézségű pálya** sorozattal is kedveskednek a nagyérdemű hackelő közönségnek. Tanulva az előző évek tapasztalataiból összesen több mint 20 pálya várja a megmérettetésre vágyókat. **A feladatok az elmúlt évek, biztonsági auditjai során tapasztalt hibákból állnak össze**. Míg az első akadály pályában a csetlő botló „guglizó" kezdők lelhetik örömüket a harmadik szintre programozói és alapos hackelési tapasztalat nélkül senki nem fog merészkedni.

Na de ha használjuk a hacker és hackelés szót, talán elkél hazánkban még ennek a kifejezésnek a magyarázata is. **Hackerek alatt olyan számítástechnikai szakembereket értünk, akik az informatikai rendszerek működését a legmagasabb szinten ismerik**. Közülük is a „jók" a white hat hackerek, tehát a fehér kalaposok, akik a tudásukat arra használják, hogy a biztonsági hibákat felfedezzék és kijavítsák, s ezzel megakadályozzák a „rosszak", a feketekalaposok támadásait, akik ezeken a biztonsági réseken át igyekeznek bejutni és kárt okozni a rendszerekben, adatokban.

Az a szakember, aki a Hactivity-n akar előadni, annak nem csak a legjobbak között kell lennie, de pályáznia is kell, itt megszólalni ugyanis a szakma egyik legrangosabb elismerésének számít. Az elmúlt évek bizonysága szerint **több komoly állásajánlatot kapott az, aki sikeresen megállta a helyét a pódiumon**. Az egész konferenciát átlengi a szakma iránt elkötelezett fanatikusok vitája, itt egy folyosói beszélgetésen többet tudást lehet elcsípni, mint egy vaskos szakkönyvből. **A hangulat ugyanakkor sajátosan laza, szinte elvárás sörrel beülni az előadásokra**, ugyanakkor önszántukból aktívkodnak a résztvevők a workshopokon, és persze fergeteges az esti buli is.

A hazai nívós előadókon túl, **idén 2 külföldi meghívott vendégelőadó is lesz a konferencián**. A nyitóelőadást az az Alexander Kornbr tartja aki az elmúlt 6 évben több mint 200 biztonsági hibát talált különböző Oracle termékekben és alapítója, ügyvezető igazgatója a Red Database Security-nek, amely Oracle biztonsági szolgáltatásokra specializálódott. Az eseményen az IT biztonsági szakvizsgákkal (CISA, CISM, CISSP) rendelkező szakemberek úgynevezett CPE pontokat gyűjthetnek, amelyek a minősítésükhöz szükségesek. **A szervezők az elmúlt évek tapasztalatai alapján 400-500 érdeklődőre számítanak.**

A Hacktivity gyémánt fokozatú támogatója: kancellar.hu
Kiemelt WI-FI támogató: Aruba - Biztributor
Ezüst fokozatú támogató: ESET, VirusBuster
Bronz fokozatú támogató: T-Systems, Microsoft, HP, McAfee, Cisco, BalaBit, Symantec, Security.hu, ASC, Ormós Ügyvédi Iroda
Technikai támogató: Qwerty Computer, Formula Mérnökiroda
Szakmai támogató: BME – Híradástechnikai Tanszék, ZMNE – Bolyai János Katonai Műszaki Kar, PTE Állam- és Jogtudományi Kar Informatikai és Kommunikációs Jogi Kutató Intézet, IVSZ, SZVT, ISACA, Hétpecsét Információbiztonsági Egyesület

Médiapartnerek: IT Business, IT Cafe, Prohardver, Origo, Computerworld, PC World, PC Dome, Chip Magazin, Klub rádió, Prim online

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1354635

Kommentek:

r@ek (törölt) 2009.09.02. 10:50:49

"Az a szakember, aki a Hactivity-n akar előadni, annak nem csak a legjobbak között kell lennie, de pályáznia is kell, itt megszólalni ugyanis a szakma egyik legrangosabb elismerésének számít."

!MEGALOL!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.02. 17:42:01

- szól az idézet az eredeti hivatalos sajtóközleményből...

És bár az előadások színvonala tavaly is hullámzott valamilyen szinten, de azért így is volt jó pár, amiért érdemes volt elmenni. Hogy csak egyet emeljek ki példának, Major Marcell és Barta Csaba előadása, vagy Baki Gáboré szerintem nagyon ott volt.
antivirus.blog.hu/2008/09/21/hacktivity_masodik_nap

Régi és új trójaiak a lista élmezőnyében

2009.09.07. 15:30 | Csizmazia István [Rambo] | 4 komment

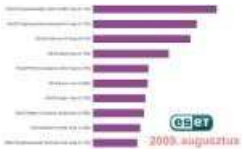
Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

Az ESET szakértői szerint ebben a hónapban is a különféle trójai programok túlsúlya érzékelhető, és **nem tűntek el a nyári szezonban az online játékok jelszavaira vadászó kártevők** sem. Érdekes módon **a Conficker féreg két hónap után lekerült az élről**, a magyar toplistát most az a Win32/TrojanDownloader.Swizzor.NBF trójai vezeti, amely már több, mint egy éve jelent meg.

Talán mostanában a Windows frissítéseket is komolyabban vették a felhasználók, mindenesetre az elmúlt két hónapban listavezető pozíciót elért Conficker féreg ebben a hónapban nagy meglepetésre visszaszorult a harmadik helyre. Helyébe a Trojan.Downloader.Swizzor.NBF lépett, amely egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat töltöget le és telepít. A Swizzor.NBF terjedéséhez a hiszékenységet is kihasználja, például olyan programokba is bele szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a csomagban.

Lassan, de biztosan erősíti pozícióját a Win32/TrojanDownloader.Bredolab.AA, a korábbi negyedik valamint harmadik helyről ezúttal a második helyezésre elegendő fertőzést okozva. Ez egy olyan trójai kártevő, amelynek megkísérel távoli oldalakról további kódokat letölteni és végrehajtani. **Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni**. Emellett a Registry adatbázisban is bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI, Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

Újoncunk a listán a 9-ik Win32/Adware.Funweb trójai. **Jelenléte a bizonyíték arra, hogy még mindig sok olyan felhasználó van, aki óvatlanul maga telepít mindenféle kéretlen reklámokat** megjelenítő alkalmazást különféle weblapokról. A Funweb működése során azt a Win32/Toolbar.MyWebSearch kártevőt telepíti a számítógépre, amely szintén rendszeresen fel szokott bukkanni a havi kártevő toplistánkban. Ez utóbbi **lassítja a számítógép működését, és a felhasználói szokásainkat is igyekszik kikémlelni**.



Végezetül következzen a magyarországi toplista. Az **ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere** szerint 2009 augusztusában az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek együttesen 34.74%-ot tudtak a teljes tortából kihasítani maguknak.

1. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége az augusztusi fertőzések között: 6.11%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amelyek látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálják, valójában azonban maga a kártevő lapul a csomagban. Emellett hátsó ajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a

számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-nbf

2. Win32/TrojanDownloader.Bredolab.AA trójai
Elterjedtsége az augusztusi fertőzések között: 5.12%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, melynek segítségével a távoli oldalakról letöltődnek és végrehajtódnak ezek a kódok. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is a bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI - Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-bredolab-aa

3. Win32/Conficker.AA féreg
Elterjedtsége az augusztusi fertőzések között: 4.81%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.

A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: http://www.eset.hu/virus/conficker-aa

4. Win32/Agent trójai
Elterjedtsége az augusztusi fertőzések között: 3.73%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

5. Win32/PSW.OnLineGames.NNU trójai
Elterjedtsége az augusztusi fertőzések között: 2.72%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nnu

6. INF/Autorun vírus
Elterjedtsége az augusztusi fertőzések között: 2.69%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

7. Win32/Kryptik trójai
Elterjedtsége az augusztusi fertőzések között: 2.57%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani. Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/kryptik-gt

8. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége az augusztusi fertőzések között: 2.50%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

9. Win32/Adware.FunWeb trójai
Elterjedtsége az augusztusi fertőzések között: 2.32%

Működés: A Win32/Adware.Funweb trójai működése során azt a Win32/Toolbar.MyWebSearch kártevőt telepíti a számítógépre, amely korábban rendszeres szereplője volt a havi kártevő toplistánknak. Futása során különféle Registry bejegyzéseket és kéretlen állományokat hoz létre a Program Files és a Windows System 32 mappákban. A több tucatnyi DLL és EXE állomány. Mint ismeretes, a MyWebSearch alkalmazás figyeli a felhasználó böngészési szokásait, és adatokat gyűjt ezekről, de működésével lassítja a számítógépet is. Ezenkívül megváltoztatja a böngésző kereséssel kapcsolatos beállításait és az alapértelmezett kezdőlapot is.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-funweb

10. WMA/TrojanDownloader.GetCodec.gen trójai
Elterjedtsége az augusztusi fertőzések között: 2.17%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1363783

Kommentek:

Ultravoice 2009.09.10. 09:15:29

Sziasztok,
Én nem vagyok egy számítógép-internet zseni, ézért is fordulok hozzátok. Volt a gépemen egy RkChimaira nevű kis vírus vagy nem tudom mi, mindíg a gép bekapcsolása után jelent meg és adobe photoshp c4-re hivatkozott, de végül is nem lehetett semmit kezdeni vele. A gépemen szoktunk intézni bankos ügyeket(pénz utalás,stb..), most nem kevés many van a számlán... ok. elvileg a nod 32 leszedte ezt a sz..t, de érdemes most megváltoztatni a bankos jelszavakat? attól félek, h valaki esetleg hozzáférhet a bankos cuccokhoz?
Üdv: Cs

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.10. 10:12:42

Szia Ultravoice!

Amit én így látatlanban tennék, hogy ellenőrizném a NOD beállításait, legyen minden a maximumon és csinálnék egy teljes keresést.

Szerintem vedd a fel a kapcsolatot a support KUKAC sicontact PONT hu címmel, és a supportos fiúk megnézik pontosan, mi is ez, és segítenek a jó beállításokban is.

Ultravoice 2009.09.11. 01:12:43

Köszi a választ Rambo! Megcsináltam, amit írtál, Semmit nem talált a nod 32, már nincs a gépen az a valami.
Egyébkénr, kik azok a supportos Fiúk?
Üdv: Cs

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.11. 09:37:50

Nem haszontalan a bankolás előtti cache, cookie, session, temp mappa, stb. takarítás, továbbá a bankolás alatt ne legyen másik ablak nyitva, lehetőleg csak a banké.

A support a technikai támogatást végzőket jelenti, tőlük lehet kérdezni problémás esetekben, ők a NOD32 magyaroszági képviselet.

Vigyázó szemetek a Facebookra vessétek

2009.09.08. 14:09 | Csizmazia István [Rambo] | 18 komment

Címkék: facebook csalás hamis antivírus kártevő fancheck stalkercheck

A klasszikus viccben emberünk vízbe esik, és közben kiabál: halászok, halászok! Egy közeli csónakból visszaszól egy borízű hang: mi is, csak mi közben nem kiabálunk. Mi viszont úgy tűnik, **ezúttal okkal kiabálhatunk farkast**, feltűnt ugyanis a Facebookon egy Fan Check nevű alkalmazás, ami alaposabban megvizsgálva **bár vannak dolgai, de nem vírus**, ennek ellenére furcsa módon mégis beleszaladhatunk miatta kártevőkbe.

Az alkalmazás maga elvileg profilunkon keresi meg, hogy mely ismerősünk írt/kommentelt a legtöbbet a dolgainkra, majd egy táblázatszerű képet készít az eredményekkel, amelyet a képeink közé tesz, és betaggol mindenkit, aki rajta van.

Emellett azonban lehet benne valamilyen programhiba is, mert némely felhasználójánál, vagy ha valaki másnak a FanCheckes képén van rajta, akkor **ez a Facebook-os kezdőlapját teljesen összezavarva mutatja, és nem mindig jeleníti meg az új postokat sem, néha régieket tesz előre**, stb. **A FanChecket egyébként nem a FaceBook fejleszti, korábbi neve Stalker Check volt**.

Az igazi baj azonban ott van, ha emiatt aztán valaki szeretné leszedni, és elkezd keresni neten. Például **rákeres arra, hogy hogyan kell ezt a problémát megjavítani (a konkrét keresési kulcsszó "fan check facebook virus")**, ugyanezek a kamu vírusírtós oldalak jönnek be, amelyek letöltetnek velünk egy hamis "vírusirtót", ami igazából a malware. A lenti képeken pedig jól látható, hogy a bamba szkript - a Dr Antivírus benézi... című posthoz hasonlóan **Macintoshon vagy Linux alatt is talál állítólag fertőzött DLL-eket** :-D

A Fan Check alkalmazás kellemetlenségeitől egyébként könnyű megszabadulni, le kell törölni és le kell tiltani, meg persze kijelölni magunkat az ismerőseink képeiből, amiket csinált. Ezenfelül **szükséges lehet még a cookie-kat is kitörölni**.

A Google keresés ezzel kapcsolatos találati eredményeivel való találkozás már nem ilyen egyszerű eset. Sajnos egy átlagfelhasználó számára ez maga lehet a rémálom, gyanakvás és hozzáértés nélkül könnyű egy ilyen csapdába beleszaladni. **Nem kapunk vírust közvetlenül, mégis kellemetlen mellékhatásokkal járhat**. Itt is megvan az a lépremenő öt százalék, akik miatt bőségesen megéri a kártevőterjesztőknek, ehhez számoljunk csak picit: 226 millió Facebook felhasználó csücsül világszerte, ebből 5% benézi a linket, az barátok közt is több, mint 11 millió. Az ilyen **családra és jól becélzott linkek száma várhatóan a jövőben tovább fog emelkedni**.

Polónius főkamarás korábbi intelmei anno decibel imígyen szóltak Arany János veretes fordításában: "Kölcsönt ne végy, ne adj!" **Ma már valószínűleg emellett azt is mondaná az ifjú Hamletnek: "Ja és ne telepíts semmilyen Facebookos applikációt, meg ne kattints minden linkre idióta módon, mert ezek sosem vezetnek jóra."** A kommentelők pedig bátran jelezzék, hogy náluk vannak/voltak-e ilyen jellegű panaszok.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1367672

Kommentek:

Cigiző · http://cigi.blog.hu/ 2009.09.08. 14:41:21

álam volt post nem frissülés, de egy F5 segített rajta mindig. Viszont ezzel az alkalmazással nem is találkoztam, és nem is szoktam mindenféle fasságokat engedélyezni.

csudri82 2009.09.08. 14:41:41

Én nem használom, de mivel ismerőseim igen, ezért nálam jelentkeztek hibák. Ez eddig abban nyílvánul meg, hogy tegnap többször is összekeveverte a kezdőlapon lévő dolgokat, az első dolog szept. 3-i volt, holott én magam is posztoltam azóta...

atko 2009.09.08. 14:57:46

Mandriva 2009.1 Nincs.
Ja és se iwiw, se facebook, se twitter, se hi5, se myvip, myspace... és se egyéb exponenciálisan növekvő álközösségi szájton nem vagyok regisztrálva. Levetkőzni, csak otthon, térfigyelő nélküli nudista strandon szoktam.
Aki meztelenül fekszik a csalánosba viszketni fog hosszú ideig.
Ezt mindenféle vírusirtó nélkül is tudom.
Komolyra fordítva: Ha a user nem képes arra, hogy tanulva netezen és ezáltal evolúciós fejlődésével elősegítse az értelmes netember kifejlődését (homo sapiens cyber), akkor a pénzt zsebre tevőknek (homo lopus) kell arra figyelmet fordítania, hogy a bárány nyírva legyen és a gyapjútermelő készsége és kedve is megmaradjon.
Amíg nem így lesz, addig remélhetőleg egyre többen fordítanak hátat a webx alkalmazások által sugalt felhőtlen szabadságnak és törlik a regjüket mindenféle ismertséget feltáró oldalról.
-Cartmen: "Nézz utána a facebookon kik az ismerősei!
-Stan_"rajta vagyok"

nemethv · http://backtotheukblog.wordpress.com 2009.09.08. 15:01:25

En azt nem ertem pontosan hogy hogyan tudja az en oldalamat osszezavarni, ha nem is hasznalom :) Marmint csak mert esetleg valaki ismeros hasznalja (azt hiszem masok hasznaljak), miert van elerese az en oldalamra. [egyebkent maga az oldalzavar nalam is megvan mar napok ota, de szemely szerint nem hasznalom az appot]

karmapolice 2009.09.08. 15:06:13

"MacIntosh"? Ezt most komolyan? Ugye csak egy szar vicc...

karmapolice 2009.09.08. 15:18:45

Látom, ez a MacIntoshozás nálad nem baki, hanem rendszeres, ami azért elég gáz a blog tematikáját tekintve. Kis i-vel írják, csak szólok.
en.wikipedia.org/wiki/Macintosh

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.08. 16:06:38

"MacIntosh"

Jajaj, bocsanat, mea maxima culpa!

Ez nalam tenyleg valahogy rosszul rogzulhetett, kegyelem arva fejemnek, igerem, mostantol vigyazok. Maris javitok es postitezek a monitor szelere ;-)

Amadeus4 2009.09.08. 16:08:28

Nálam most ugyan tökéletesen mutatja a kezdőlapot, de reggel pl. többször előfordult, hogy csak a tegnap esti update-eket jelenítette meg. És igen, kedves barátaim közül többen használják ezt a remek alkalmazást. Tehát van összefüggés...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.08. 16:12:28

 Atko:

Szia, örülök, hogy írtál, Linux rulez, meg minden ilyesmi.

"Levetkőzni, csak otthon, térfigyelő nélküli nudista strandon szoktam." LOL, ez tecc :-)

A többire pedig csak annyit, már Moldova is levezetett valamiféle evolúciós láncot a Proletar Correctus-tól kezdve a Proletar Linkus-on át a Proletar Sajrensys-ig ;-)

Szerintem az a baj, hogy tizenéves fiatalok körében a Facebookozás, MySpacezés és hasonlók nagyon dívnak, a veszélyek reális észlelése kevésbé, ha meg a felnőtt figyelmeztet, az dacból ignore. Vagyis ők az ilyeneknek az egyik legtökéletesebb célpontjai.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.08. 16:15:27

@Amadeus4:

Az még egy érdekes kérdés lehet, hogy vajon a Fan Check hiba egy véletlen, és a hamis AV egy kihasználása ennek mások által, vagy pedig már eleve az egész folyamat így volt megtervezve, és az egészet egy kéz mozgatta :-O

pill 2009.09.08. 16:31:21

én nem használom ezt az alkalmazást a barátaim lehet h igen, de ezt nem tudom (honnan kéne tudnom?) és mégis összekavarodik a sorrend, meg néha a régieket rakja előre. Akkor most mit csináljak?

daneeka 2009.09.08. 16:37:35

vannak ilyen panaszok...

aron_ha 2009.09.08. 16:45:09

ez a kamuvírusírtó nekem megjelent egyszer de még a fan checkes tegelődés ideje előtt. szerencsére nem szoptam be

Vfair 2009.09.08. 17:29:01

A Fan Check helyett az "All my Friends" app (url vég: pickupfriends) csinált hasonlót nálam.

Ez véletlenszerűen választ ki 12-24 barátot és +/- jelzőkkel látja el őket.
Külön "kedvessége" a dolognak, hogy az ártatlan hülyéskedés megjelenik minden egyes tagelt, random-kiválasztott ismerős személyes adatlapján is!
Óvakodjatok ettől is.

A Facebook nem teszteli az engedélyezett app-okat?

nemethv · http://backtotheukblog.wordpress.com 2009.09.08. 18:08:03

@Vfair: nem, csak a certified appokat tesztelik.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.09. 09:49:09

Megszólaltatták a fejlesztőt:
www.pcworld.com/businesscenter/article/171621/fancheck_developer_defends_app_says_its_not_malware.html

dzsoja-dzsoker 2009.09.10. 03:24:20

aki tudja mi az a Greasemonkey, vagy legalább minimum firefoxot használ, annak ajánlom a Facebook Purity scriptet, ami megszabadit az összes kvízes, nyálas,idegesítő, buta picsás cuccoktól.

userscripts.org/scripts/show/44459

a facebook FB purity nélkül nézve, olyan mint egy firefox adblocker nélkül

atko 2009.09.10. 11:23:42

@Csizmazia István [Rambo]:
Hát igen annak idején a piros zászlós ember szaladgált az automobilok előtt...
Egyébként nem vagyok Linux fan, nekem ez munkára kell, és az dos-win 3.1-98-98se-xp (mellett) aztán csak után ez vált be legkevesebb plusz munkát igénylően, hogy én is jól érezzem magam és mások is békén hagyjanak...
Igazából attól megyek a falnak, amikor a hirdetésben az "barátok már a telefonodon is és nem tévedhetsz el sohasem, mert mindig veled vagyunk" szöveget hallom, mert olyankor mindig az jut eszembe, hogy ahhoz, hogy én ne tévedjek el, vagy megtaláljam a hozzám közel eső akármit egy fontos infóra szükségük van, mégpedig arra, hogy én hol vagyok.
Aki mindig on-line az mindig nyitott ajtónál éli az életét. Ami egy kis faluban nem baj, sőt kötelező. Láttál már régi falusi udvart bezárva csengővel? De a világháló azért nem egy kis falu.

Jelszótörő kisiparosok

2009.09.10. 10:52 | Csizmazia István [Rambo] | 2 komment

Címkék: hack jelszó lopás kisvállalkozás kémkedés bérhacker

Biztosan kellemetlen lehet, ha valakinek a barátjáról csak titokban derül ki, hogy nős. Nos az ilyen helyzetekre is kínál korántsem legális megoldásokat egy kisvállalkozás, amely **potom száz dollárért (csupán 18 ezer forint) AOL, Gmail, Yahoo, Facebook vagy Hotmail jelszót szerez meg, illetve tör fel**.

Elhagyta a barátja? Kíváncsi lenne volt házastársa levelezésére? Vegye igénybe cégünket, megbízható referenciákkal rendelkezünk - imígyen szóla ~~Zarathustra~~ a reklámszlogen. A vállalkozás **több különböző weblapon is** kínálja portfólióját.

Egy postafiók jelszavát sok féleképpen fel lehet törni. Lehet ez puszta találgatás, lehet a közösségi oldalak adatai alapján a jelszóemlékeztető kérdés elleni támadás - mint a Sarah Palin esetnél - de **küldhetnek az adott e-mailcímre olyan levelet is, melynek linkjére kattintva egy kémprogram települ**, és az küldi el a jelszót a támadóknak. A weblapon **még hálálkodó vevők: Maria, Lisa és Danny leveleit is lehet olvasni**.

Korábban mi is írtunk már mobiltelefonos módszerekről, mutattunk a weboldalba helyezett kémprogram terjesztő Iframekért pénzt kínáló vállakozást, valamint a szervízeléskor előforduló furcsa esetekről is értekeztünk. Igazából a feleség számítógépére telepített kémprogramért is született már ítélet a férjnek: és nem is kicsi, 4 év börtön. Viszont a mostani eseteknek ilyen jellegű következményeiről nem tudunk.

Az USA-ban az ilyen cselekmény - ha károkozással nem jár - csak vétségnek számít. Azt jelenleg nem lehet pontosan tudni, helyile hol is üzemel a vállakozás, de gyaníthatóan a tengerentúlon szorgoskodnak. És annak ellenére, hogy a szolgáltatás illegális, **a kereslet iránta a jövőben valószínűleg folyamatosan növekedni fog**.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori

- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1372508

Kommentek:

atko 2009.09.10. 11:09:27

:-D Hát ez már annyira szörnyű, hogy vicces.
Elképzelem azt a szituációt amikor egymás ládájában kutakodnak...
Csak a szolgáltatók a felelősek mindezért, mint azt már többször is írtam. Amikor kolbászt veszek a hentesnél, megbízom benne, hogy nem téglaport használt pirospaprika helyet a dögkútból kiszedett darált húshoz.
Amikor annó 2003-ban reggeltem a wiw-re akkor még egy teljesen más világ volt ott. Aztán a pénz... és akkor kiszálltam, persze előtte szlovákká váltam, lakóhelyet változtattam, mindezt idegen ip címről stb. Mai napig ott vagyok üres négyzettel azoknál az embereknél akik az általam meghívottaktól kapták a meghívót. közeli ismerősöm, aki csak törölte magát még szerepel név szerint tartalom nélkül.
Ezek után már csak a "jó érzés" gátol meg bárkit abban, hogy hasonló vállalkozásokat nyisson. Az meg ügye pénzzel kiváltható "jó érzéssé" konvertálható.
Szóval a szolgáltatók a bűnösek az egész IT bűnözés létéért. A szolgáltatókban benne foglaltatik a szoftver gyártók is!
Lassan ott tartunk, hogy ha privát életet akarsz magadnak, le kell húznod a géped a hálóból, mobilt elhajít és nézed a feleséged szép szemét. :-)

Csizmazia István [Rambo] http: antivirus.blog.hu 2009.09.26. 22:20:27

Kamuzik a cég, átverés az egész, köszi Buherátor az infókat:
buhera.blog.hu/2009/09/25/a_hackelo_szolgaltatasokrol

Tiltsa ki az internetszolgáltató a fertőzött gépeket

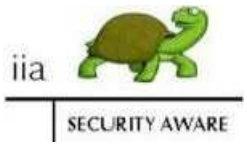
2009.09.14. 21:20 | Csizmazia István [Rambo] | 4 komment

Címkék: ausztrália internetszolgáltató szűrés botnet isp

Az ötlet nem új, most azonban már **konkrét etikai kódex javasolja ezt a lépést**, ami mai botnet sújtotta világunkban állítólag egy lehetséges módszer lehet az infrastruktúra védelmében.

Az Internet Industry Association (IIA) által megfogalmazott irányelvek szerint az internetszolgáltatóknak fel kellene vállalnia, hogy azonosítsák be a kompromittált, fertőzött számítógépeket, **lépjenek kapcsolatba az ügyféllel és figyelmeztessék őt** (pl. Bejelentett Támadó Számítógép a Google féle Bejelentett Támadó Webhely-hez hasonlóan). **Adjanak tanácsot a javításhoz, mentesítéshez, vírusirtáshoz**, és aztán jön a végkifejlet, ami már nem ennyire evidens: valamint **gyanús adatforgalom esetén jelenték azt a nemzetbiztonsági szolgálatoknak**. Na és itt már akár görcsbe is rándulhat az emberjogi aktivisták gyomra. Mi a gyanús, ki dönti majd el, nem jár-e azzal a veszéllyel is a netes forgalom ellenőrzése, hogy például a RIAA és hasonló szervezeteknek is szolgáltatnak majd terhelő adatokat az egyszerű állampolgárokról?

Reméljük, a megvalódítás tükrözni fogja majd minden résztvevő érdekét és szempontjait, ugyanis **a tervezet megalkotásában a kormányzat, a helyi internetszolgáltatók mellett biztonsági szakemberek, valamint a fogyasztók képviselői egyaránt résztvettek**.



Ezek a feladatok nem lennének kötelezőek, csupán ajánlás szinten fogalmazódtak meg, mint követendő és hasznos magatartás. **Az önként vállalt etikai kódex betartását egy teknősbékás logóval** fogják jelezni majd a nagyérdemű felé a programban résztvevő internetszolgáltatók. **Az ausztrálok mindenesetre belevágtak**, valamit tényleg tenni kellett már, és majd az idő eldönti, megvalósulhatnak-e, ha igen, akkor a szolgáltatók megfogadják-e ezeket, illetve hogy **a gyakorlatban milyen hatása lesz mindennek a felhasználókra és persze a botnetekre**.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1380988

Kommentek:

□alay □http:□a□utostat.hu□cikk-kereso 2009.09.22. 13:4□:58

A gáz az, ki honnan tudja, hogy fertőzött? Ez ledobná az átlagfelhasználót. Inkább a támadottak vigyázzanak jobban - de ez persze magánvélemény.

□archy 2009.09.23. 11:24:27

Lefogom tölteni az egész internetet egy pendrive-ra és amíg el nem olvasom offline leszek. Így biztosan nem fertőzöm meg magam és másokat. :)

Bambano 2009.10.01. 20:57:54

Ez ismét egy veretes marhaság. Egyrészt kinek mi a fertőzött? Másrészt ki fizeti ki az internetszolgáltató ezzel kapcsolatos költségeit? Harmadrészt meg sok helyen egy isp van, vagy egy elfogadható módon működő isp van, ha nem teszi ki a teknőst, mi fog változni?
Hint: semmi.

valakik már megint a saját fontosságukat akarják igazolni. a megoldás pedig egyáltalán nem ez: amelyik oprendszer törhető, azt javítsa meg a gyártója. Minden más termék esetén a gyártó felel az általa elvégzett trehány munkáért, miért lenne másképp az internetszolgáltatás esetén? Az isp feccöljön pénzt abba, hogy valamelyik oprendszergyártó szar munkát végzett? Ne vicceljünk már.

xaba99 · http://landf.blog.hu 2010.01.21. 13:16:46

esetleg az ISP blokkolhatná a forgalmat a fertőzött webhelyek meg a botnet szerverek felé...

Megöllek - szólt a teniszezőnő

2009.09.15. 20:15 | Csizmazia István [Rambo] | 2 komment

Címkék: google times williams hamis new york antivírus serena

Egyre **intenzívebb eszközökkel próbálják becserkészni** azokat a Windows felhasználókat, **akik semmilyen védelemmel nem rendelkeznek**. Elmúltak azok az idők, mikor türelmesen kivárták a következő földrengést, Karácsonyt vagy Valentin napot. **A szerénység a lagymatagok virtusa**, talán ezt a szlogent tűzték a zászlójukra a kártevőterjesztők, és heveny izgalmi állapotban akcióba lendültek.

A fertőzött banner hirdetések eddig is előfordultak már, most viszont egy nagyobb weboldalt sikerült becserkészniük ezzel a módszerrel, egészen pontosan a New York Times magazint. Akik itt **óvatlanul kattintgattak a reklámokra antivírus nélküli gépükkel**, könnyen beleeshettek a megtévesztésen alapuló csalásba: nem létező fertőzésre figyelmeztető ál vírusirtó programot töltöttek le, amely pénzt zsarol ki az állítólagos "igazi", irtás is végző változatért. A NYT weboldalán szereplő kártevő a virustotalos ellenőrzés szerint egy Win32/Kryptik változat volt, amit a "nagyok" szépen csipőből hárítottak.

Nem volt szebb napjuk azoknak sem, akik a Google segítségével keresgéltek bővebb információkat Serena Williams vonalbírós afférjával kapcsolatban, mert a találatok között a Symantec észlelése szerint megint csak a hamis antivírut terjesztő oldalak jeleskedtek. A keresőoptimalizációval odaterelt oldalak akkor bukkantak fel, ha például a **"Serena Williams Outburst"** szavakat gépelte be valaki.

Tucatjával jelentek/jelennek meg a videót igérő oldalak, amik vagy hamis kodeket akarnak letölteni, vagy jön a szokásos rogue antivirus próbálkozás. **A cipőt a cipőboltból elv alapján** azt már nem is akarjuk mondani, hogy holmi kétes keresési eredmények helyett :-) a naprakész sport hírekért inkább a Sport Gézát kell előfizetni ;-)

Azt hiszem ezekután illő lenne már levonni a Windows rendszerek használóinak azt a tanulságot, hogy **bármilyen legális gyártó valamilyen valódi antivírusát telepítsenek már fel végre a gépükre**, mert így járhatnak, sőt mert a végén még kiszórhatja őket az internetszolgáltató is.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1383631

Kommentek:

Yann Le Pentrec · http://lnk.bz/t7c 2009.09.16. 23:48:14

Jogos. Csakis ismert gyártó "tűzben edzett" termékét szabad használni.

ardeacinerea · http://www.pallas70.hu/osszetett-kepzesek.php 2009.09.22. 12:09:42

Ennyi naív embert. Nálunk NOD van és kiegészítő tisztió progik, amiket csak a tesóm ismer. Az azonban alap, hogy össze-vissza reklámokra nem klikkelünk.

Vállaljunk állást a West Unionnál

2009.09.16. 17:11 | Csizmazia István [Rambo] | 10 komment

Címkék: csalás hotmail álláshirdetés west union

A mai vérzivataros időkben, amikor a munkanélküliségi ráta az egekbe szökött, az állásközvetítők 6-18 hónap várakozási időket prognosztizálnak a hozzájuk fordulóknak, míg a szerencsés álláshoz jutók kevésbbé válogathatnak, és akár rosszabb feltételekkel is elmennek dolgozni. Egy ilyen helyzetben **érkezhet e-mailen egy multicég ajánlata**, amely mint látjuk, mégsem egészen főnyeremény.

Az első és fő oka talán az lehet, hogy **nem is a West Union küldte a leveleket** - kicsit a "miért nem harangoznak itt fiam - jaj száz oka van annak - na csak egyet mondj - jó, nincs harang" mintájára. Ezt leszámítva minden prima benne: **rugalmas munkarend, magas fizetés, minden adót megfizetnek utánunk (ez már szinte mesébe illő ;-), sőt biztosítást is kötnek** ránk.

A "leendő munkaadó" kizárólag európai munkavállalók érdeklődését várja, akik **az alábbi személyes adataik megadásával jelentkezhetnek**: teljes név, ország, e-mail cím, telefonszám. Aláírás: a West Union Group személyzeti osztálya, no persze ;-)

Van ugyanis a cégnek hivatalos honlapja, és **igen csak kevés (konvergál a nullához) a valószínűsége annak**, hogy a jól bevált kontakt címek helyett **mindenféle szedett-vedett hotmailes helyekre várnák a jelentkezőket**. Hogy élő európai címeket, és identitásokat gyűjtenek valakik valakiknek a megbízásából, az világos.

A nagy kérdés már inkább csak az, a csalók **honnan tudják azt , hogy kiknek küldözgessék ezeket a leveleiket**, mert pont egy munkakereső ismerős postafiókjába érkeztek ezek hosszú tömött sorban, napi 10-20-30. **A véletlenekben meg valahogy nem nagyon hiszünk**, mióta Jungtól a Szinkronicitást olvastuk...

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Ez történik a weben egy perc alatt
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1385995

Kommentek:

Kutyuu 2009.09.16. 18:46:07

Eltekintve attól, hogy sztem kb. mindenki folyamatos munkakereső :) nem csak oda ment levél.
Megnéztem, hogy milyen címeimre ment, a nagy része ritkán vagy soha nem használt címem. Valószínűbb, hogy vették a címlistát valamelyik spamgyárostól, aki valamikor régen scriptekkel lekapta a webről a címeket.

Konspiráció emléletek rulez :)

elegem van 2009.09.16. 18:56:35

Meggyőző az a Hotmailes cím...

Shitting Bull 2009.09.16. 19:02:20

Hümmm... én másfél éve keresek munkát, de ebből egyet sem kaptam. :D

Attus Germanicus · http://attus.hu 2009.09.16. 19:17:40

Nekem a céges(!) e-mail címemre jön naponta 3-4.

A Nép - Te vagy! (törölt) · http://www.kibulizottorszag.net 2009.09.16. 19:23:46

Izé, amiről szó van az nem a Western Union lenne? Vagy létezik West Union is?

Nekem több mint gyanús, hogy a naív becsapni akaró annyira fölkészületlen, hogy még ezt is összekeveri. Akárhogyan is, kaptam már hasonló jellegű önlelelplezően hülye spamekekt. És mennyit!

kovi1970 2009.09.16. 19:24:52

Ráadásul nekem úgy jönnek, mintha én adnám fel.

Yann Le Pentrec · http://lnk.bz/t7c 2009.09.16. 20:05:25

Igen, elég életszerűek azok a randomizált hotmail-es email címek. :) Aki ennek bedől, az másnak is.

Rá Dios 2009.09.16. 21:36:29

@kovi1970: Ügyes. Elalltatja a gyanút, hiszen saját magának csak nem küld smpamet az emberfia :-)

Shitting Bull 2009.09.17. 07:56:51

@Rá Dios: én évekkel ezelőtt spam listára tettem magamat. :)))

PAdrienn 2011.12.14. 23:40:08

Én egy a becsimagyarok oldalról jutottam el a hirdetésükhöz és regisztráltam az oldalukon, arra már nem emlékszem, hogy milyen hivatkozásokon keresztül

Chat in the Middle

2009.09.18. 17:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: chat bank the in csalás jabber rsa citm middle

Mindig van egy friss ötlet, vagy egy régebbi dolog tovább csavarintása, **folyamatosan újabb típusú támadások elől húzodhatunk félre**. A fősodor persze - az érdek a világ ura jegyében - mindig a pénzszerzés, ahogy most is. Ha Móra Ferenc ma élne, bizonnyal erről írná meg a Return of the Csili-csali Csalavári Csalavért ;-)

A banki ügyfelek adatainak megszerzése mindig is elől állt az összes számítógépes csalás vizsgálatánál a táplálkozási láncban. **Kevéssé valószínű**, hogy a bank személyzetise írjon nekünk. Ahogy **előbb lesz shanghai táncosnő az öreganyánk és pucolja baltával az ablakot**, mintsem egy bank e-mailen akarna minket adatfrissítésre kérni. Ezt **jó lenne, ha mindenki már helyből tudná**, de mivel nem tudja, ezért hát lehet próbálkozni. Egy fokkal már jobb ötlet telefonon a bank ügyintézőjeként jelentkezni, de aztán itt is lehet gyanakvóbb az ügyfél, és **esetleg eléggé el nem ítélhető módon nem átallja orvul elhallgatni a PIN kódját a telefonáló elől** :-) Aztán jött az autósokat megcélzó, és tilos parkolás/gyorshajtás miatti hamis linket tartalmazó ál-büntetéscetli a szélvő alá.

Most pedig **itt a hybrid módszer banki remixe**, melyre az RSA kutatói figyeltek fel. Online chat beszélgetésre hívják e-mailben a banki ügyfelet, ahol kap egy linket hozzá, és ez már elég. Látszólag a saját bankja oldalára jut, itt bekérnek néhány személyes adatot. Itt aztán további személyes információkat kérnek: **cím, e-mail cím, telefonszám: ezekre már rögtön tudnak majd hivatkozni a későbbi chat beszélgetés** esetén. Az RSA szakemberei **több változatát is** észlelték a csalásnak, a legviccesebb közülük az, amelyiknél éppen a csalások megelőzése miatt szólítja fel az ügyfelet azonosítóinak begépelésére. Naív ügyfél számlaszám-kód begépel; bűnöző hanyatt dől, hogy csak ilyen rövidke tőmondatokban fessük fel a szituációt. A Jabber IM modult alkalmazó chates módszer előnye, hogy valós időben, **azonnal eljuttatja a begépelt adatokat a támadóknak**. A Chat in the Middle (MITM-re hajazó neve alapján is) képes lehet a jövőben új babérokra törni.

Adathalászat volt, van, lesz. Nem tudjuk, létezik-e akkora Arial betűtipus, amivel mondjuk a Kínai Nagy Falra fel lehetne írni, hogy **a banki weboldalak sosem kérdeznek például PIN kódot senkitől**. A postai értesítési vagy lakcím adatot is **felesleges az ügyfélszolgálatnak megkérdezni, hiszen egyrészt tudniuk kell, másrészt ennek változtatása csak és kizárólag személyes ügyintézés során** végezhető el. Ám ahol nagy mennyiségű ügyfél sok pénzzel van jelen, ott aztán minden ilyen trükk ipari méretekben beindul, és **a jó öreg 5% reményében** tolják ezerrel a bűnözők. Ezek után máris világossá válhat, honnan is ez a sok cabrio Mercedes, ami az utakon szembejön ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1390263

Kommentek:

Nincsenek hozzászólások.

Hacktivity 2009 első nap

2009.09.22. 15:01 | Csizmazia István [Rambo] | 9 komment

Címkék: hacktivity hacker 2009 gólyavár

Újabb Hacktivity találkozóval lehettünk gazdagabbak, **ezúttal új helyszínen** volt az esemény. Mik történtek, hogy éreztük magunkat, erről lesz szó a továbbiakban. Az esemény **megszokott házigazdája most is Krasznay Csaba** volt, aki mellett ezúttal Bártfai Attila segített, hogy a másik teremben is sínen legyenek a dolgok.

A szívünknek **kedves, félhomályos, sörös kriglis Fonó után eleinte kicsit furcsa volt a sok neonnal kivilágított, hatalmas és modern** előadótermek kevésbé barátságos látványa. Persze nyilvánvalóan szükség volt a továbblépésre, és kétségtelen előnyei is megmutatkoztak a tágabb környezetnek, ami a Gólyavár Konferenciaközpont volt. Egyrészt **a látogatók száma elért az 500-at**, ami egy szép kerek szám, másrészt megszűnt a korábbi közelharc a hálózati elosztósávokért, itt aztán **ipari mennyiségben voltak konnektorok, mindenki könnyedén tudott noteszgépet** 230-ról használni. A hangosításon vagy az előadók mikrofonhasználatán lesz még mit csiszolni, hogy a leghátsó sorokban is lehessen mindent hallani, ezen kívül már csak azért lehetett mérgeskedni, ha néha mindkét teremben egyszerre volt érdekes előadás, és Révész Sanyihoz hasonlóan nekünk sem volt két életünk. Ezen viszon **remélhetőleg segít majd az IT Cafe mindkét teremben folyamatos video felvétele**, amit majd hamarosan közkinccsé tesznek, valamint a Hacktivity honlapon is előbb-utóbb várhatóak az előadások PPT fájlai.

Már a kezdés sem volt átlagos, **első ízben hívtak meg külföldi előadókat**, a megnyitóra ezúttal érdemes volt viszonylag pontosan érkezni (bár a szokásosnak mondható késés fertelmes vétkébe ;-) ezúttal is belecsusszantak a szervezők). **Alexander Kornbust neve sokaknak csenghet ismerősen** a Red-Database-Security GmbH színeiben. Kicsit **minden, amit az Oracle hackelésről tudni akartál, de sosem merted megkérdezni** feelingben zajlott a bemutató, amiben rögtönzött, magyar oldalt is érintő hiba felfedezés is szerepelt. Nem volna érdemes neki felajánlani, hogy minden felderített hibáert kap egy százast, mert bizonyosan nem győznénk. **Az 1992 óta az Oracle rendszerekkel fogalkozó** Alender előadása meggyőző és érdekes volt, és bár a téma korábban mások által is be volt már mutatva részben, mindenképpen érdemes volt végignézni.

A "Finding the Hole" kérdésre pedig duplán is választ kaphattak az érdeklődők, hiszen nem csak az adatbáziskezelő biztonságában található lyukakra, de egyúttal a saját cég alapítása, a piaci igényeknek való megfelelés és az erre épülő sikeres vállalkozás is erre a gondolatmenetre épült. Kesernyés megjegyzésekből azért érezhettük, ezen a szinten a kiegyensúlyozott családi élet **a türelmes családtagok támagatása nélkül** már komoly csorbát szenvedhetne a rengeteg számítógép mellett töltött idő miatt.

Buherátor és Veres-Szentkirályi András a tavaly évvégi SSL biztonságával foglalkozó hírek hátterét mutatta be, pontosan mi mit ér, **mit sikerült az MD5 lenyomatok hamisításával elérni, és mit nem**. Az SSL szerintük egyelőre azért köszöni jól van, ennél jobbat még nem találtak ki. Bár az odafigyelés azért nem ártalmas, hiszen a TCP/IP gyengeségei adottak.

Buherátor blogja 2009-ben Goldenblog díjat szerzett az IT kategóriában, András pedig többek közt a 2004 és 2005-ös években hívta fel magára a figyelmet a Wargame-n aratott győzelmeivel.

Igazi ínyencség volt **Pánczél Zoltán és Spala Ferenc előadása, amelyet az Nmap eszközhöz fejlesztett proxy patch** programjukról tartottak. Az Nmap többek közt port szkennelésre is használatos, és arról szólt az előadás, hogy bár külső eszközökkel eddig is lehetett már fatengelyesen proxy szervert, illetve szervereket használni, de megszületett a "mi lenne ha ez benne lenne" elgondolás, amit aztán tett

követett.

Kicsi vargabetű árnyékolta be a fejlesztést, amit az okozott, hogy első körben támaszkodtak a Wikipediás technikai leírásokra, amelynek hitelességéhez aztán kezdett kétség férni, és végül a "tiszta forrásból" jegyében visszatértek a jó öreg RFC-khez. **A közbeláncolt proxykon keresztüli port scan** tetszőleges számú és különböző típusú ilyen szerveren mehet keresztül, lenyomozhatósága pedig igen nehéz.

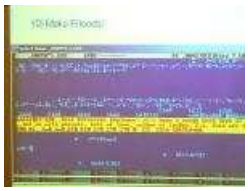
A szünet után is egy már jól ismert szereplő lépett a színpadra, **Barta Csaba ezúttal egy saját készítésű rootkittel, illetve annak továbbfejlesztett változatával jelentkezett**. Korábbi vizsgálódásai, és az internetről letölthető rootkit kódok elemzése után úgy vélte, tud ő is ilyet, sőt esetleg még jobbat alkotni.

Az úgynevezett token lopásos módszere tudomásunk szerint valóban teljesen egyedi és újszerű megközelítése a programozásnak. A Powerpoint ábrák mellett természetesen a rootkit is vizsgázott, állományok, folyamatok rejtődtek el a bemutató gépen.

Ebédszünet után - ahol a Kancellar.hu ingyensörét ihattuk és a Sicontact ingyen virslijét ehettük - szinte folytatása, vagy továbbgondolása volt ezek után T**evesz András előadása, amely stílszerűen a "Nem félünk a rootkittől"** címet viselte. Alapos **elvi áttekintést** kaphattunk a különféle user és kernel módú rootkitekről, az úgynevezett hookolási (eltérítési) technikákról.

Annyi mindenesetre mindenkinek világos lett a végére, hogy bár vannak rootkit felderítő segédprogramok, és számos vírusvédelmi program már modulként is tartalmaz ilyet, azért **száz százalékos felderítési esélye csak a Live CD-ről indított összehasonlító vizsgálatoknak van**.

Egyszerre kezdődött két vírusvédelmi előadás is, mi **a B teremben a kanadai Pierre-Marc Bureau víruskutató** előadását hallgattuk. Az ESET szakembere a klasszikus "Ismerd meg az ellenfelet" mondás jegyében azt gyűjtötte össze, milyen érdekes vagy **jelentős változásokat, meglepő fordulatokat hoz időnként a kártevők elemzése, mit tanulhatunk belőle**, sőt mit kell, hogy megtanuljunk ezekből.

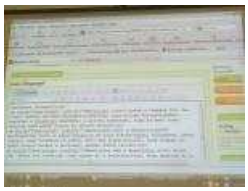


Teljesen más hozzáállást igényel egy kórokozó visszafejtése szemben annak megírásával. Az elemzett kártevők között olyan **vicces kedvű vírusszerzők kódba rejtett üzenetei is szerepeltek**, amelyek mintha egy Csupasz pisztoly epizódból csöppentek volna ide, pél a "Bocs a múltkori kórházas dologért" - egyszerre vicces és morbid.

Ugyancsak a kártevők témaköréhez csatlakozott **Balázs Zoltán Malware és Maffia című előadása** is. A Sinowal bemutatása kapcsán aztán sok mindenről szó esett, rootkitek és MBR módosítás, valamint azt is láthattuk, ha egy **naprakész vírusvédelemmel ellátott gépen - amelyen még a Windows frissítések közül sem hiányzik semmi - is előfordulhat károkozás**. A kártevők és technikáik ismertetése a bankolással kapcsolatosan is megjelent, illetve annak végpontát érintve a banki pénzfelvevő automatákat is érinti.

Példákkal illusztrálva láthattuk, a rosszfiúk nem egyedül az otthoni PC kilensek elleni támadáson törik a fejüket, tömeges **kísérletek vannak az automaták manipulálása felé is**. Ahol a lakásba hazavitt routerekhez hasonlóan ugyancsak előfordul, hogy **a gyártó által beállított alapértelmezett admin-admin típusú név-jelszó páros üzemel** évekig. Nekem személy szerint az volt a kedvencem, amely az ATM-en futva ellopta az accountokat, majd a támadók, mikor **egy speciális bankkártyával a helyszínre mentek, a nyugtaadó nyomtatóval a program kinyomtatta nekik** az addig ellopott kártya és jelszó adatokat.

A PET portál részéről Gulyás Gábor és Paulik Tamás jelentkezett egy olyan böngésző kliensekhez fejlesztettt lehetőséggel, amely a **blogok, közösségi oldalak adatait csak meghatározott körnek engedélyezné megtekinteni**. A Firefox böngészőhöz való BlogCrypt kiegészítő kulcsokkal képes védeni a szövegeket, és a **kulcsokban beállított jogosultsági szintektől függően akár részletekbe menően tudja a tartalom engedélyezését/tiltását** elvégezni.



A még béta állapotban levő fejlesztést a gyakorlatban is megmutatták egy próba blog oldalon, működés közben.

És végül a hivatalos program keretében következett a **kerekasztal az adatvédelemről**. Sok érdekes kérdés felmerült, szinte elrepült az idő közben, a moderálást végző Krasznay Csaba pedig a témákat jól illusztráló video bejátszásokkal igyekezett egy-egy terület problémás eseteit bemutatni. **Szabó Endre (Adatvédelmi Biztos Irodája), Dr. Ormós Zoltán (ügyvéd), Simon Éva (Társaság A Szabadságjogokért), valamint Makai Gyula (Nemzeti Nyomozó Iroda) és Székely Iván (CEU, Közép-Erurópai Egyetem)** vettek részt a társalgásban, melyet a közönség a helyszínen, illetve az IT Cafe fórumában feltett kérdéseivel tudta közvetlenül is befolyásolni.

Bár sok minden elhangzott, azok a műkedvelő hackerek, akik egy-egy rendszerben **hibát észlelve jóindulatúan figyelmeztetik is az érintett rendszer tulajdonosát, sajnos a továbbiakban sem érezhetik magukat biztonságban** a csúnya, gonosz 300/C árnyékában. Talán jó lenne, ha ezek a sokszor és jogosan felvetett problémák **egyszer végre már megnyugtató törvényi rendezést nyernének el**, hiszen az út egy ilyen munkahelyen dolgozó jól kvalifikált pentester számára rendszerint az ilyen fiatalkori, egyetemista tapasztalatokkal van kikövezve, és ahogy az a következő nap látszott is, Magyarország védelmében **egyes szervezetek külföldi támadás esetén akár számítanának is az ilyen értékes hazai tudásra**.

Az első napi összefoglaló végére nem tudok mást írni, mint hogy nem csak végigolvasni volt hosszú, hanem megírni is :-) Azt már **nem merem megkockáztatni**, hogy beleírjam: "aki idáig elolvasta, kap egy korsó sört", mert **biztos vagyok benne, nagyon sokan jönnek majd ide, akár ott voltak személyesen, akár csak kíváncsiak az ott történtekre**.

Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1398755

Kommentek:

cworm (törölt) 2009.09.22. 16:06:28

Jó lenne egy kicsit kevésbé kapkodni az írással, mert rengeteg az elütés, ami förtelmesen zavaró tud lenni. Vagy utólag újra elolvasni az egészet és kijavítani a hibákat. Debug!:)

|Z| 2009.09.22. 16:22:03

Lássuk csak, mindig a cikk végén van a lényeg. Blabla blabla "aki idáig elolvasta, kap egy korsó sört". Ezaz. Hacker sörből lehet kérni? :)

atko 2009.09.22. 22:08:36

Riszpekt minden "kocka" fejnek!
Ők teszi a világot élhetővé. :-)

erdnek 2009.09.22. 22:09:47

jó az összefoglalód, a 300/C-t meg minél előbb finomítani kéne!!!!! mondjuk úgy, hogy egy rés bejelentése a hatóság felé (melyik hatóság? mondjuk az NHH) a hackernek jogot biztosítana, hogy a hibát általánosságban bemutathassa, publikálhassa...

atko 2009.09.22. 22:10:30

Ja igen és a söratom hasításhoz a neon fény elengedhetetlen, merthogy energiatakarékos.

r@ek (törölt) 2009.09.23. 00:21:04

"A szünet után is egy már jól ismert szereplő lépett a színpadra, Barta Csaba ezúttal egy saját készítésű rootkittel, illetve annak továbbfejlesztett változatával jelentkezett. Korábbi vizsgálódásai, és az internetről letölthető rootkit kódok elemzése után úgy vélte, tud ő is ilyet, sőt esetleg még jobbat alkotni."

Tovabbmegyek: ilyet barki tud alkotni. Mindosszesen 3 konyvet kell elolvasni hozza..

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.23. 08:44:41

Szia r@aek!

Én is éppen most fejeztem be az Agysebészet for Dummies című kötetet, remélem ez elég lesz a gyakorláshoz :-)

Azért amikor Tevesz Andris megkérdezte a publikumtól, ki programozott már BÁRMIT kernel módban, senki sem jelentkezett. És akkor ott van a táplálkozási lánc csúcsán az, ha nem csak megértem, ami egy könyvben le van írva, hanem én írom azt a könyvet ;-) Szóval nem azt akartam ezzel mondani, hogy csak félistenek tudnak rootkitet írni, hanem inkább azt, hogy Csabáé a jobbpofább megoldások közül való.

GHost (törölt) 2009.09.23. 09:41:14

Először is Tevesz András vagyok :)

@r@ek: 1 éved van a következő hacktivity-ig szerintem mindenki szívesen veszi, ha addig te is készítesz egy hasonlót. A 3 könyvet szerintem el lehet olvasni elég hamar.

A Barta Csaba kódjában az volt az igazán szép, hogy Windows 2000-től Windows 7-ig képes működni. Ha elolvastad a könyveket esetleg megnézted az előadását, akkor látni fogod, hogy minden service pack-ben változtat valamit a Microsoft és azokat egyenként kell kibányászni a szimbólumok közül vagy az élő rendszerből egy debugge-rel. A 3 könyv elolvasásával képes leszel egy kernel drivert lefordítani, de semmiféle segítséget nem fog adni a nem dokumentált részek felfedezésében.

Egy másik fontos dolog még, hogy rootkit-ből a világban kb. 100 as nagyságrendet találsz. Vírusokból milliósat. Ez azért számomra azt jelenti, hogy a világban nem rohangál annyira sok olyan zseni aki 3 könyv után képes arra amire a Csaba.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.26. 22:02:52

Időközben kikerült egy publikáció a rootkit.com weboldalra is, érdemes volt azt a három könyvet elolvasni :-DDD
www.rootkit.com/newsread.php?newsid=969

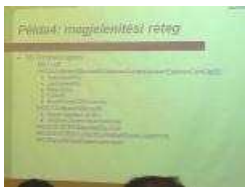
Hacktivity 2009 második nap

2009.09.23. 19:19 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hacktivity hacker 2009 gólyavár

Újabb Hacktivity találkozóval lehettünk gazdagabbak, **ezúttal új helyszínen** volt az esemény. **Mik történtek a második napon**, hogy éreztük magunkat, erről lesz szó a továbbiakban.

A második nap reggelén kissé álmos szemekkel gyűlt egybe a társaság, **látszott az esti nem hivatalos program hatása**, és a Balabit által biztosított alkoholos befolyásoltságú elágazó italkeverékek is eredményesen fokozták az előző napi jó hangulatot. Az első előadást **Illés Zsolt tartotta, aki igazságügyi szakértőként számítógépek vizsgálatával foglalkozik**. Mi történik egy ilyen vizsgálatnál, milyen tanulságos esetek voltak a praxisában, erről mesélt nekünk.



A különböző nyomozásoknál a lefoglalt gép merevlemezének klónózása után mindig a másolat vizsgálata történik, és ilyenkor **a bizonyíték gyűjtés a feladat**. A szakértői munka **részletes szabályozásának híján jelenleg minden az adott szakember tudásán, hozzáállásán múlik**. Mindenesetre az igazságügyi szakértők többsége igyekszik helytállni, csak a 100 százalékban igazolható állításokat erősítik meg. **Munkájuk során felelnek a nyomozószervek feltett kérdéseire, és nem bocsátkoznak találgatásokba**. Mivel az előadását rekordidő alatt elmondta, így a hallgatóság szerencséjére ezek után számos kérdésre tudott a fennmaradó időben választ adni.

Höltzl Péter a naplózó infrastruktúrák jelenéről és jövőjéről beszélt. Érzékeltette **számos hányatott sorsú RFC szomorkás történetét**, és hogy mennyi időnek kellett eltelni ahhoz, hogy legalább nyomokban megjelenjenek a kor kívánalmainak megfelelő nyugtázott, teljes dátumot kezelő módszerek.

Az azért világosan látszott, **az ideális naplózó rendszerek megvalósítása nem is annyira egyszerű** feladat.

Már az előző napi kerekasztalos kérdésekből is érezhető volt, a hackelés jogi háttere még komoly demokráciákban sem teljesen egyértelmű, és olajozottan szabályozott, nálunk pedig kifejezett merev rendelkezések közé van szorítva, amely nem igyekszik megfelelő módon disztingválni, és szeretik a delikvens feje felett lebegtetve hagyni a Daemoklesz kardját. Igen **sok kérdést kapott hát Dr. Ormós Zoltán ügyvéd, akinek specialitása a szoftverjoggal kapcsolatos kérdéskör**.

Néhány tanulságos esetet is mesélt, melyekkel igyekezett bemutatni, milyen menete lehet egy büntető eljárásnak, és a szankciók mértéke is igen súlyosan alakulhat a helyzettől függően, amely **akár 10 évi szabadságvesztés is** lehet. Az világosan kiderült, hogy **akinek ilyen jellegű ügye van, jól teszi, ha már a kezdetekkor ügyvédet fogad**, mert a már elindult eljárások bírói szakba érkezésekor ez már késő lehet. És megint csak dilemma volt, mert Bucsay Balázs adott elő ezzel egyidőben a kriptográfiai hashekről a másik teremben.

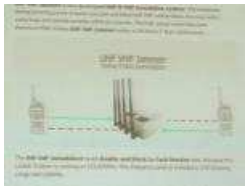
Az ebéd előtti utolsó előadásban **Dr. Dudás Ágnes mesélt azokról a fontos szabályokról, amelyeket az etikus hackereknek, penetrációs tesztet végző szakembereknek** mindenképpen figyelembe kell venniük, amikor egy munkát elvállalnak.

Egyáltalán **nem mindegy, szerepel-e a szerződésben**, hogy a kezdeti feltételek módosíthatóak-e menetközben, és szigorúan szabályozott az is, bejutás esetén mit tehetnek az adatokkal. Ugyancsak szerződésben rögzített kitétel lehet az is, **tisztán informatikai vagy social engineering eszköz is felhasználható-e** a tesztelés során.

Bodó Balázs előadása alatt ugyancsak megtelt a terem. 2007-ben is előadónk volt, ezúttal pedig **filmek torrent letöltése és a mozik helyzete, bevételei közötti összefüggéseket boncolgatta**. Mivel a feltöltés, és a letöltés alatti megosztás is kalózkodásnak számít, igencsak érzékeny és kényes téma került terítékre. Azt is láthattuk, hogy nemzetközi szinten is szorongatják a letöltőket, elég az amerikai RIAA magánszemélyek elleni milliós pereire, vagy a legfrissebb "Csigát eszik, filmet tölt le, börtönbe megy - ki az?" helyzetre gondolni Franciaországban.

Azt már magunk is gyanítottuk, nem a letöltések hozzák nehéz helyzetbe a filmforgalmazókat, **ha ugyan tényleg nehéz helyzetben vannak**. És itt természetesen bár a szűkös anyagi lehetőségekkel rendelkező magyar filmkészítő és forgalmazó cégek is meg lettek említve, de a vizsgálat elsősorban a nemzetközi helyzetet igyekezett feltérképezni. A képet **árnyalhatta volna a DVD forgalmazók bevételeinek ismertetése** is, ám ők a felmérés során elzárkóztak az adatok közlésétől.

A szinte már szokásosnak mondható esti kerekasztal előtti utolsó előadás igazi csemegének számított. Aki elegendő Jack Bauert nézett már, az eddig is gyaníthatta, hogy bár az úgynevezett kiemelt infrastruktúrák nyilvánvalóan valamilyen kiemelt védelemben részesülnek, **lehetetlen ezeket száz százalékosan megóvni**. Csak reménykedünk, hogy az illetetékesek azért igyekeznek, hiszen kívánatosan vonzó célpontjai ezek korunk Matuska Szilvesztereinek. Az **energetika, közlekedés, hírközlés, élelmiszeripar és társainak hatékony megvédelmezése nemzetbiztonsági érdek**, viszont az elemzést meghallgatva sokan először szembesülhettek azzal, hogy **egy rossz szándékú terrorista csoport milyen könnyen informálódhatna ezek gyenge pontjairól, akár az interneten való keresgéléssel**.



Az Index hírportál is ezt a momentumot ragadta ki a kétnapos rendezvényből, amelynek kiegészítéseként **egy felmérés eredményét is megosztották az előadók: Kovács László és Krasznay Csaba**. Az e-mailes kérdőívből az derült ki, a megkérdezett hackerek jó része **bár hiteltelennek, és lejáratottnak tartja a honvédséget, támadás esetén szívesen segítene** az elektronikus védekezésben, vagy támadásban.

Mi más is állhatott volna ezek után a fókuszban, mint a kritikus infrastruktúra védelme Magyarországon. A beszélgetés moderátora ezúttal is **Krasznay Csaba volt, a résztvevők pedig Kovács László (Zrínyi Miklós Nemzetvédelmi Egyetem), Suba Ferenc (CERT-Hungary), Sík Zoltán Nándor (ENO Advisory Kft.), valamint Jakab Péter (Bankszövetség)**.

Bár a valódi vészforgatókönyv részletei nem derültek ki (talán még nincs, de az is lehet, hogy van, csak nem nyilvános), **az látszik a legvalószínűbb esetnek, hogy a CERT-Hungary** irányító szerepe lenne a legfontosabb egy informatikai támadás esetén.

Akit érdekel a vita, ezt, és már több más előadást is megnézhet utólag, mert közben szépen lassan gyűlnek a videó anyagok az IT café honlapján. Windows rendszerek alatt a Silverlight, Linux alatt pedig a Moonlight kiegészítővel lehet megtekinteni a felvételeket. Aki pedig kedvet kapott a fentiek alapján, várják a szervezők sok szeretettel a Hacktivity 2010-re.

Ajánlott bejegyzések:

- yerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1400619

Kommentek:

Nincsenek hozzászólások.

The Happening

2009.09.25. 10:28 | Csizmazia István [Rambo] | 2 komment

Címkék: rfid 2009 találkozó itbn

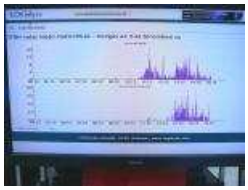
Lezajlott **az ötödik ITBN**, apróbb izgalmakkal, számos külföldi előadóval, rengeteg reklámmal és sok lehetőséggel arra, hogy a szakmabeli ismerősökkel, barátokkal kötetlenül szót váltsunk egy IBM-es ásványvíz mellett.

Az érkezés örömét némileg elhomályosította, hogy a majd két óra autózás után az épületbe érve valaki **váratlanul ránkzárta** a férfi WC ajtaját. Közepesen masszív ajtó, és egy kb. 10 perces **hangos kiabalás és öklöllel való ütés után sem jelentkezett senki**. Na, nem ilyen reggelre számítottunk. Gyors MacGyveres áttekintés, ha dohányoznánk és lenne itt öngyújtó, lehetne WC papírt gyújtani a füstérzékelő alatt, bár akkor jönne a víz is a plafonból. Mivel van térérő, irány a 198 tudakozó, Aréna Plaza felhívása következik. Itt kb. 5 perc után a körbe-körbe lejátszott üzenet hallatszik: **"köszönjük hívását, várjon a kezelő jelentkezéséig... köszönjük hívását, várjon a kezelő jelentkezéséig... köszönjük hívását, várjon a kezelő jelentkezéséig... etc."** tisztán és világosan látszik, élő ember itt nem fog beleszólni a kagylóba.

Komoly ajtókirúgás sajnos nem működik, mert minő pech, befelé nyílik. A svájci bicskával való zárszerelgetés lesz majd az utolsó esély az éhenhalás előtt, de előtte hívjuk a Rendőrséget, akik hamar, pár csörgés után jelentkeznek, elsőre megértenek mindent, és máris szólnak a helyi biztonsági szolgálatnak. Áldott napfény, drága szabadság - így vége lesz a majdnem félórás rémálomnak. **Még arra is van energiájuk, hogy egy jó félóra múlva visszahívjanak, és megkérdezzék, minden rendben van-e**, ezúton hatalmas köszönet érte Serfőző százados hölgynek.

A Hacktivity után szinte mellbevágóan erős a kontraszt, a Hacktivity-n **a Kancellar.hu ingyen söre után itt már szigorú figyelmeztetés a belépőn**: "Alkoholos befolyásoltság vagy láthatóan kábítószer hatása alatt álló személy a rendezvényt még érvényes belépőjegy ellenében sem látogathatja." Szerencsére az öltözködési etikett betartása sem zajlott mereven, így sötét farmerben és színes pólóban is sikerrel vettük az akadályt.

Ami szintén újdonság volt, **az a belépőhöz mellékelt RFID chip**, amely nem titkoltan képes arra is, valós időben ellenőrizze, ki merre húzza maga után a csíkot, sőt **az előtérben a termek fajlagos látogatottságát is figyelemmel kísérhetjük a képernyőkön**. Az mindenesetre érdekes lesz, hogy ezen elektronikus póráz és a mellékelt értékelőlap birtokában az illetékesek összevetik-e, hogy az illető egyáltalán ott volt-e az előadáson, amiről véleményt mond - ezt is meg lehet elvileg nézni a névreszóló csík segítségével. **A belépéshez egyébként nem volt szükség a chipre**, vizuális ellenőrzés volt csak, így aki bármilyen okból levette a matricát magáról, az is simán tudott közlekedni ki-be.



Ennyi izgalom után **a beköszöntőt természetesen Keleti Arthúrtól hallhattuk**, aki az elején igyekezett pedánsan tartani a kezdési időpontot, később aztán kisebb csúszások már jelentkeztek, emiatt nem volt egyszerű dolga annak, aki különböző termek előadásai között akart váltogatni.

Az **nagyon tetszett, hogy érkezéskor nem sóztak rá minden látogatóra azonnal egy három kilós papírzsákot ipari mennyiségű prospektusokkal**, hanem egy 8 centis CD lemezt kaptunk tele PDF állománnyal, és így nem kellett napközben a teherhordó serpák szép, de küzdelmes életébe belekóstolnunk. **Hasznos újítás volt a folyamatos, szünet nélküli előadás rend**, így nem többszáz ember indult el egyszerre hosszú tömött sorban a mellékhelyiségek vagy a szendvicses asztalok felé DoS támadást indítva.

Bár világmegváltó újdonságot nem igazán hallhattunk senkitől, néhány marketing szagú előadás pedig kifejezetten próbára tette a türelmünket - az idő relatíve milyen hosszú is tud lenni 20 percen át ;-) - ennek ellenére jól éreztük magunkat, **sok Hactivity és egyéb ismerőssel, volt kollégával, baráttal sikerült összefutni, szótváltani** és megbeszélni, miért is nem sikerült eddig megváltanunk az informatikai világot.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1405742

Kommentek:

bolhabetu 2009.09.25. 12:49:03

Kalandok a WC-ben. :)
Ez egy nagyon Tékozló Homár érett anyag.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.26. 18:08:15

Kedves Bolhabetu!

Nem kerestem én az ilyen kalandot elhiheted, eddig úgy gondoltam, az ilyesmi mindig csak mással fordulhat elő.

Ahogy a klasszikus sírfelirat mondja :-)

"Itt nyugszom én - olvasod te
Olvasnám én, s nyugodnál te..."

Piedone Hongkongból

2009.09.28. 14:34 | Csizmazia István [Rambo] | 2 komment

Címkék: bank hang csalás hongkong e mail seng yahoo.com.hk

Jövedelmező üzleti javaslat, immár másodszor. Az első Tuskó Hopkins akcentusú Peter Lee, a Hang Seng Bank állítólagos dél-koreai igazgatójától jött, aki valamilyen rejtélyes okból hongkongi yahoos címről írt. Most itt a folytatás, ezúttal is erről a levelező szolgáltatásról **Mr. Patrick K. W Chan tisztel meg minket becses ajánlatával, hát ne habozzunk**!

A nyersfordított levél maga kissé nehezen olvasható elsőre, aminek nem kizárólag a tört magyar nyelv az oka, hanem az ékezetes betűk helyén szereplő cirill karakterek zavarják a megértést.

Gyors cserélgetés után aztán kialakul a szöveg, sok köszönet viszont ekkor sincs benne. **A cirill betűk oka a levélben szereplő Windows-1251 kódolás**, ami miatt arra is gyanakodhatunk, hogy a hongkongi yahoos postafiókokat csak felhasználták a vélhetően ukrán, szerb, bolgár vagy macedón csalók.

Szemlátomást az elkövetői körre korábban komoly hatást tehetett a Hang Seng Bank, mert **mostani "jogszeruen rántás nélkül megteheto" ügyletük is erre a szálra alapozza** a történetet. Vegyük észre már a feladónál az "infohangseng339@yahoo.com.hk" sorszámozott horror címet, **ez kábé olyannyira hiteles, mintha maga Csányi Sándor elnök írna nekünk az otpbank1526@hotmail.com.ru címről**.

Küldjük hát el ezen "derék becsületes" címgyűjtő embereknek **az adatainkat: név, ország, telefonszám, faxszám** - és a levél elküldése után már lesz nekik hozzá visszaigazolt működő e-mail címük is :-) és aztán már **semmi dolgunk sincs, mint hogy várjuk határtalan bizalommal "az átadás nagy halom pénzt"**.

Manapság a Fülig Jimmyk dolga nagyon egyszerű, mert a "Kavarja ez most vagy nem kavarja?" **kérdésre újabban mindig igen a válasz**. Ezért a frissen átadott telefonszámaink (a véletlen tárcsázások mellett) ha másra nem, de további zaklatásokra, emeltdíjas visszahívással kombinált csalásokra vagy kéretlen SMS reklámok érkezéséhez is megfelelő alap lesz.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?

- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1412196

Kommentek:

gothmog 2009.09.28. 17:44:19

Sajnálatos, hogy tudomasul vetuk, nem tartotad be a makszimális diskretio, igy most mar cseszhetyed a nagy halom penz atutalasa.
Marad neked rántás, magadnak.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.09.28. 18:51:32

@gothmog:
Így jártam :-DDD

Új generációs banki kártevők

2009.09.30. 14:22 | Csizmazia István [Rambo] | 5 komment

Címkék: bank csalás trojan kártevő

Manapság **kihalóban a feltűnési viszketegségben szenvedő vírusíró** típus, aki olyan ósdi talmi célok érdekében tényked ne, minthogy benne leszek a TV-ben. A kőkemény üzleti érdekek mentén építkező csoportok mafia szerű szervezettségben, **komoly szakmai tudással és tanítani való social engineering taktikával terítik kémprogramjaikat**, amivel személyazonosságokat, jelszavakat és banki adatokat gyűjtenek. **Ez utóbbi úgy tűnik, kezd szerfelett hatékony lenni**.

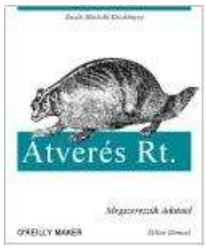
A **Finjan cég biztonsági kutató figyeltek fel egy olyan új banki trójaira**, amely többet tesz már, mint a szokásos elődök. Eddig ugye egy ilyen kártevő igyekezett feltelepülni, billentyűzet leütés naplózót telepített, a keletkezett logokat igyekezett kijuttatni a fertőzött gépről, esetleg botnetes zombivá alakította a gépét a hosszútávú elérési lehetőség miatt. Emellett pedig egy komoly adatbázis alapján azonosította a banki weboldalakat, eléréseket. Ez itt is mind megvan, de a most észlelt új trójai banki oldalra való belépés után **már valós időben figyeli az egyenleget, és ebből számolja ki, mennyt érdemes ellopnia**.

A trójai a kutatók szerint egy meg nem nevezett németországi pénzintézet ügyfeleire specializálódott és Ukrajnából végezték a távirányítást. A Finjan **természetesen értesítette erről a német hatóságokat**, de ami még érdekesebb, **le tudták nyomozni a kommunikációt a kártevő és az ukrán irányító szerver között, ami titkosítatlan csatornán zajlott**, és a Lucky Sploit adminisztrációs konzolt használták fel hozzá a bűnözők. **Sikerült bepillantás nyerni a statisztikákba is, ebből az derült ki, mintegy 90 ezer gépre küldték ki a trójai kártevőt**, amiből 6400 számítógépet (7.5%) sikerült megfertőzni és az irányításuk alá vonni. Az eset még augusztusban történt, és egy **22 napos időtartam alatt a csalók 348 ezer EUR (94 millió HUF) összeget tudtak** így a számlákról ellopni.

A trójai terítését **fertőzött linkeket tartalmazó e-mail üzenetekkel, weblapok kódjába illesztett hivatkozásokkal** végezték, és ha valaki kattintott, akkor egy a webböngészőkben kihasználható exploit kód révén megfertőzte a gépet és **várt, mikor lépnek be a megadott német banki oldalra**.

Ha ezt észlelte, ellenőrizte az egyenleget, és kiszámolt magának egy optimálisan ellopható összeget, amivel nem az volt a célja, hogy rendes legyen, hanem talán a lelepleződés esélyét próbálta sikeresen csökkenteni, hiszen a *.* összeg eltűnése esetén egy ügyfél azonnal reklamálni kezd. Aztán **elküldi a kérelmet a bankba az ellopni kívánt összegről, miközben a böngészőben a felhasználó mindvégig az eredeti egyenleget látja** - na ez a zseniális. Körülbelül ugyanaz a helyzet, mint a DIR2FAT DOS kártevő anno "tartotta a táblát" a lemezparancsoknak, és listázáskor a fertőzés előtti, eredeti fájlhosszt jelenítette meg. A lehívott és máshova utalt összegeket úgynevezett öszvérek segítségével juttatják ki az országból. Az ilyen közreműködők sokszor maguk sincsenek teljesen tisztába azzal, hogy amit tesznek, bűncselekmény. **Jelentkeznek egy helyi álláshirdetésre (napi két óra, otthonról végezhető munka, kiemelt fizetés), és annyi a feladatuk**, hogy jutalékért cserébe megadott számlákra kell továbbutalniuk a nekik érkező, tisztára mosandó pénzeket.

A kártevő ha már ott van, akkor logolja a számla tranzakciókat, képernyőmentéseket csinál és kifürkészi az esetleges Facebook, PayPal és Gmail accountokat is a kutatók szerint. Mindenesetre ha igaz, ez az első olyan banki trójai, amely eltéríti a böngésző sessiont, és közben hamis egyenleget mutat a felhasználónak, így az **már csak akkor veszi észre a bajt, ha a havi egyenlegértesítőt postán kézhez kapja vagy ha időközben egy másik**, tiszta gépről bankol.



Miért van az, hogy az ember már egy ilyen zseniális alkotásnak sem tud önfeledten örülni? Talán mert igaz a mondás: "a villamos alá szorult ember mosolya nem őszinte".

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1417565

Kommentek:

|Z| 2009.09.30. 16:39:21

Tény, hogy ez az első, ami a számlaegyenleget is változtatja, de a Silentbanker is képes volt arra (lassan 2 éve), hogy a böngészőben manipulálja a tranzakciókat - észrevétlenül. És valóban zseniális, hogy itt tart a malware szakma, kíváncsi vagyok 2 év múlva hová jutunk.

atko 2009.10.01. 09:29:17

És küldenek megerősítést kérő sms-t is számlaszámmal összeggel és megerősítő tranzakciós kódszámmal?? Mert anélkül nem igazán lehet utalni az .. banknál.
Ha ezt is tudja majd, akkor én sem fogok felhőtlenül örülni. Így viszont ríszpekt zsoltibékának.
A banki biztonság a bankok felelőssége.

Yann Le Pentrec · http://lnk.bz/t7c 2009.10.01. 19:51:15

@asdfqwert: Remélem oda jutunk, hogy még hatékonyabb anti-malware programok fogják detektálni és eltávolítani az ehhez hasonló kártevőket, még mielőtt valóban baj történik.

Err0r 2009.10.01. 20:40:13

 atko
Szerinted hány ember olvassa el az SMS-beli szöveget? Csak a kódot. A képen azt látod, hogy jó helyre megy a pénz, míg az SMS-ben valóban már a rossz szla szám, de Te ellenőrzöd? Mert én is csak ezek után fogom ellenőrizni. Ja, és boot linux. :)

ui:
a bankbiztonsághoz csak annyit, hogy amíg ott a pénz, igazad van. Ha netbankolsz, már a Tiéd. A bank nem vállal felelősséget a Te géped tisztaságáért.....

atko 2009.10.02. 09:11:09

@Err0r:
Hát nekem a számlaszámot és az összeget küldi sms-ben + a megerősítő kód utolsó x számát. A mobilszámomat nem hiszem hogy a böngésző tudhatja + a telefonkönyvben el van tárolva a netbank telefonszám, ergo ha nem onnan jönne a nemjöhető sms... szóval elég nagy tudás kéne a rendszer megszívatásához.
A netbank rendszer biztonsága pedig a bank felelőssége, mert ha nem épít be több biztonsági pontot, (pl a mobilszámom ők tárolják) akkor hiába szűz a gépem.

Álcázott botnet utasítások

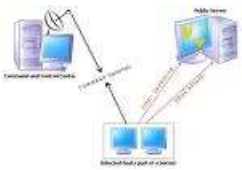
2009.10.01. 19:49 | Csizmazia István [Rambo] | 7 komment

Címkék: szerver jpg botnet irányítás álcázás

Ha harc, legyen harc - **gondolták a botnet pásztorok**. És megint mertek egy nagyot álmodni, majd pedig reggel a JPG állományoknál kellett felütniük az álmoskönyvet.

A **TCP/IP forgalom figyelése sok érdekességgel szolgálhat a botnetek elleni küzdelemben**. Emiatt aztán adja magát az ötlet, álcázni kellene az utasításokat. Eleinte az IRC csatorna volt az kezdet, aztán mára eljutottunk odáig, hogy **már a Twitter üzeneteket is felhasználták** az ilyen kommunikációban. A mostani ötlet pedig az, hogy **álcázzák a zombigépeknek küldött utasításokat, és JPG állományként próbálják azt feltüntetni**. Ehhez egy valódi JPG képállomány fejlécét használják - erre sok parser meg is állapítja, ez itten kérem nagy tisztelettel egy JPEG típusú image - a maradék binárisba meg egyszerűen belapátolják a kívánt utasítást XOR-olva 0x4-gyel.

A network monitorok meg esetleg benézik, mint szokványos webes forgalmat a kliens-szerver között. A leleplezéshez **alaposabb fájl ellenőrzést kellene elvégezniük, ami viszont** már jelentős többlet terhelést okozna.



A **Waledac botnet már alkalmazott hasonló** trükköt, ott ha a bot kap egy valós image fájlt a szerverről, akkor a kártevő kódját XOR-olva hozzáfűzte azt annak végéhez. Ismeretlentől tehát továbbra se fogadjunk el tudatmódosító cukorkát és JPG állományt.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1420849

Kommentek:

szilvacska 2009.10.01. 23:17:05

mivaaan???

lolperec 2009.10.01. 23:47:34

ám ö mekk.. em áj affektid? :D
az új számomnak ez lesz a címe:
"I want a botnet on my Mac" ^^

JohnWatt · http://allas.dolgok.com 2009.10.02. 06:30:59

De most van ilyen, vagy ez csak elmélet?

sonance · http://www.sonance.hu 2009.10.02. 07:00:38

@lolperec: van "mek" botnet, nem kell aggódni, csak nem éri meg a trójai programok fejlesztőinek egy "kisebbségre" fejleszteni mikor van több milliárd winfosos gép a földön. Most azonban kóstolgatják a "meket" és sikerült is létrehozni egy több tízezres botnetet.

futureboy (törölt) 2009.10.02. 09:08:04

ha az Iphone-t is beleszámoljuk, lehet, már megéri az Apple-cuccokra is vírusokat, kártevőket fejleszteni..

grizzancs 2009.10.02. 09:14:41

ismet egy szinvonalas cikk..

mert ha a gepem egy botnet halozat egy tagja, akkor valoszinuleg valaki odaadja a kezembe a jpgt, hogy ugyan nezzem mar meg a botnet-jpg-parser.exe nevu kepnezegetomnek, mi?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.10.02. 10:15:03

A színvonalas cikk ;-) arról szólt, hogy hiába figyel valahol egy network monitor, egy ilyen trükkel át van verve a feje.

Egyébként kézbe venni is lehet, meg játszani is szabad vele ;-) de a képnézegetőd maximum annyit mond, hogy Ooopsz, ez egy sérült képállomány.

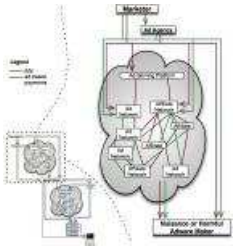
Áradnak a kéretlen reklámprogramok a gépeinkre

2009.10.02. 21:11 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

A félelmetes adatmegsemmisítő vírusok helyett **ebben a hónapban jobbára a kéretlen reklámablakokat megjelenítő kártevőké a főszerep**. Az ESET termékeiben az ilyen programokra főleg akkor vadászhatunk eredményesen, ha a beállításoknál **a „Kéretlen alkalmazások keresése", illetve a „Veszélyesnek tűnő alkalmazások keresése" opciót is bekapcsoljuk**.

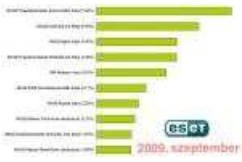
Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melynek elemzése mindig tanulsággal szolgál a felhasználók számára. A toplistán **minimális változások történtek** az élmezőnyben az előző hónaphoz képest. A prímet most is az a Trojan.Downloader.Swizzor.NBF viszi, amely egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. **Többnyire reklámprogramokat töltöget le és telepít**. A Swizzor.NBF terjedéséhez a hiszékenységet is kihasználja, például olyan programokba is bele szokták rejteni, amely látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálja, azonban valójában maga a kártevő lapul a csomagban.



Visszavette viszont a második helyet a Conficker, amely egy olyan hálózati féreg, amely a Microsoft Windows egyik biztonsági hibáját kihasználó exploit kóddal terjed, gyenge admin jelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül is terjed a fertőzés. Bár az RPC (Remote Procedure Call) vagyis **a távoli eljáráshívással kapcsolatos sebezhetőséghez már 2008. októberben kiadták az MS08-67 jelű Microsoft biztonsági javítócsomagot**, amely elhárítja a hiba kihasználhatóságát, ennek ellenére sok Windows alapú számítógépen nem fordítanak elég figyelmet a naprakész vírusvédelem mellett az operációs rendszerre is.

Maradt **az első ötben a Win32/TrojanDownloader.Bredolab.AA**. Ez egy olyan trójai kártevő, amelynek megkísérel távoli oldalakról további kódokat letölteni és végrehajtani. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is bejegyzéseket manipulál, egészen pontosan **kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban**. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

Újoncunk a listán a 10-ik Win32/Adware.WhenUSave. Futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kéretlen reklámokat, valamint saját program frissítésit tölti le. A fertőzött gépen aktív böngésző esetén linkeket, időjárás jelentést és más kéretlen tartalmakat, reklámokat jelenít meg.



Végezetül következzen a magyarországi toplista. Az **ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere** szerint 2009 szeptemberén az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek **együttesen 36.56%-ot tudtak** a teljes tortából kihasítani maguknak.

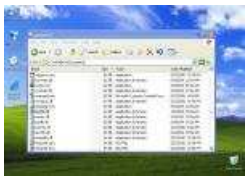
1. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége a szeptemberi fertőzések között: 7.39%

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amelyek látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálják, valójában azonban maga a kártevő lapul a „csomagban". Emellett hátsó ajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-swizzor-nbf

2. Win32/Conficker.AA féreg
Elterjedtsége a szeptemberi fertőzések között: 5.59%

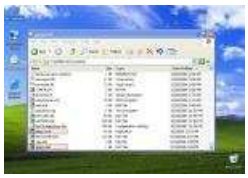
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.



A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: http://www.eset.hu/virus/conficker-aa

3. Win32/Agent trójai
Elterjedtsége a szeptemberi fertőzések között: 4.40%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.



A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

4. Win32/TrojanDownloader.Bredolab.AA trójai
Elterjedtsége a szeptemberi fertőzések között: 4.36%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, melynek segítségével a távoli oldalakról letöltődnek és végrehajtódnak ezek a kódok. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is a bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó

hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-bredolab-aa

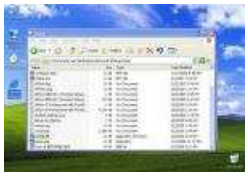
5. INF/Autorun vírus
Elterjedtsége a szeptemberi fertőzések között: 3.81%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

6. Win32/PSW.OnLineGames.NNU trójai
Elterjedtsége a szeptemberi fertőzések között: 2.71%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Tényked ése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.



A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nnu

7. Win32/Kryptik trójai
Elterjedtsége a szeptemberi fertőzések között: 2.29%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.
Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/kryptik-gt

8. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége a szeptemberi fertőzések között: 2.21%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

9. WMA/TrojanDownloader.GetCodec.gen trójai
Elterjedtsége a szeptemberi fertőzések között: 1.92%

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-getcodec-gen

10. Win32/Adware.WhenUSave alkalmazás
Elterjedtsége a szeptemberi fertőzések között: 1.88%

Működés: A Win32/Adware.WhenUSave működése során létrehozza a saveupdate.exe nevű állományt. Az ilyen nem kifejezett kártevő, hanem inkább a veszélyes vagy nem kívánt programok kategóriába tartozó kéretlen reklám programok sok esetben élnek olyan trükkökkel, hogy különféle további könyvtárakban is létrehoznak magukból másolatot. Ennek kettős célja van: egyrészt egy esetleges vírusirtást követően egy eldugott helyen megmaradhatnak a fertőzött állományok, másrészt helyi hálózatokban, megosztott könyvtárakban, peer-to-peer hálózatokban is képesek terjedni. Futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kéretlen reklámokat valamint saját program frissítésit tölti le. A fertőzött gépen aktív böngésző esetén linkeket, időjárás jelentést és más kéretlen reklámokat jelenít meg.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-whenusave

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?

- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1422256

Kommentek:

Nincsenek hozzászólások.

Két éves az antivirus.blog

2009.10.05. 11:41 | Csizmazia István [Rambo] | 8 komment

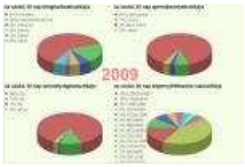
Címkék: 2 évforduló éves antivirus.blog

Annyi minden történt szeptemberben, hogy észre sem vettük a második születésnapunkat. 2007. szeptember 17-én indult el a blog, és volt néhány szigorúbb startlapos szerkesztő, akik akkoriban nem vették fel azonnal az oldalukra, hanem azt írták, **először nézzük meg, üzemel-e egyáltalán három hónapig**, azután majd esetleg lehet szó a link felvételéről.

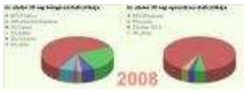
Azóta sok víz lefolyt a homlokunkon, igyekeztünk folyamatosan "testközelből" hírt adni kártevőkről, támadásokról, biztonságról. Ezek voltak a második esztendő legolvasottabb, Index címlapos cikkei:

Vigyázó szemetek a Facebookra vessétek
Álcázott botnet utasítások
Vállaljunk állást a West Unionnál
Harry Kókler és a félvér kodek
Rendőrségi wardriving
DDoS-oljuk meg együtt Obamát!

És íme, ez az utolsó 30 nap böngészőstatisztikája, jól látszik, **a Firefox folyamatosan és durván azóta is lenyomja a többieket**. A gyengülő IE a Chrome-nak adja át a részesedését, az Opera és a Safari aránya nem igen változott.



Az operációs rendszerek küzdelmében a szokásos - **picit gyengülő - Windows dominancia dacára viszont az alternatív oprendszerek csak lassan erősödtek**. Bár én a zsetonjaimat egy éve még a Macintosh komoly erősödésére tettem *(Jövő ilyenkor tíz százalék feletti Macintosh és 8% körüli Linux adatokat szeretnék majd itt látni :-)*, **a Linux rendszerek látogatói legalábbis ehelyütt jobban képviseltették magukat**, ötről hét százalékra tornázták fel magukat.



Ez a tény a Windows7 miatt újraindított OS szavazás eredményein is jól látszik

Sajnos a képernyőfelbontások tavalyi adatai már nincsenek meg, de **a mostanin jól látszik, van egy mobil réteg is (234x232 3%), akik okostelefonról néznek be időnként**. Reméljük, jövő ilyenkorra már okostelefonokra fejlesztett internet security csomagok és tűzfal megoldások tesztjeiről is írhatunk majd ;-)

Továbbra is célunk, hogy **még több "átlagfelhasználó" olvasót sikerüljön idecsábítanunk**, hiszen a károkat többségében ők szenvedik el. Végül ezzel a C64 zenei világával kibélelt klippel búcsúzunk, és a rádiós műsorvezetők felszisszenése ellenére "sok szerettel küldjük mindenkinek, aki szereti :-D" A vírusmentes hétköznapokban pedig senki ne felejtse el majd a saját születésnapját!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1423840

Kommentek:

SzellAndras 2009.10.05. 12:16:01

Első kommentezőként nagyon boldog születésnapot kívánok!

Nagyon értékes nevelési-oktatási munkát jelent a blogod, kívánok még sok ilyen szépn évet!!!!

András

buherator · http://buhera.blog.hu 2009.10.05. 12:51:30

Gratulálok! Többet, gyorsabban, magasabbra!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.10.05. 14:43:00

Sziasztok!

Köszönöm mindenkinek, kis lépes nekem, nagy lépés a blognak, meg minden ilyesmi ;-)

A "Többet, gyorsabban, magasabbra" mozgalomra én már személyesen nem emlékszem, de azért Fidel Castro nyitott Csajkájának még volt szerencsém integetni hurkapálcás magyar zászlóval a Stromfeld Aurél út mellett :-P

atko 2009.10.05. 15:01:47

 Csizmazia István [Rambo]: Nem antivírus, de jómagam a szabadszállási laktanyában még ültem is egy csajkában., bár az hard-top volt.
Az emberiség meg szerencsére nem hülyül, tehát lesz még okod blogot írni. mi meg majd olvassuk és szorgalmasan hozzászólunk címlaptól függetlenül.
Ja és a statisztikát is szorgalmasan javítjuk, bár bár ez is olyan mint a legtöbb statisztika, hogy mögöttes tartalom néklül semmi értelme. Pl. ha ez egy linuxos vírusokkal foglalkozó oldal lenne, akkor valószínűleg az oprendszer arány is más lenne....
Szerencsére az a blog még megírásra vár. :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.10.05. 15:25:01

Volt egy igazán kiemelkedő érdekes pillanat is.

Körülbelül július elején vezettem be, hogy kitettem egy Twitter ablakot, eleinte csak a blogposztokat toltam oda is, de aztán az érdekesebb linkeket is publikáltam benne, főleg magyar, de hébe-hóba angolt is.

Aztán egyszercsak email érkezett szeptember 16-án:
"Mikko H. Hypponen (mikkohypponen) is now following your tweets on Twitter."

Hát ez kábé olyan, mintha egy komoly futball rajongótól Ronaldinho megkérdezné, nincs-e kedve focizni vele egy kicsit vagy engem Stallone tíz évvel ezelőtt meghívott volna egy Rambo forgatásra ;-)

atko 2009.10.06. 12:05:45

@Csizmazia István [Rambo]:
Hát azért a sikorsky helikopterekkel forgatott Mi24-eseket nem vállaltam volna fel. Ezeken anno szét röhögtük magunk a z - klub (z=zászlóalj) hangalámondásos filmvetítésein. Ahogy az egész rambó, deltaforce, amerikai ninja agymenésen is.
Nem tudom lesz e majd film a facebook, hotmail, és egyéb szerver "törésekről"l, és azokon fog e valaki nevetni.

atko 2009.10.06. 12:07:34

Azért a Mikko a kaperskytől cool!
Bár a twitter egy nagy ...
Csak ezt még nem divatos kimondani.

atko 2009.10.06. 12:08:37

jav illetve az f-secure-től. bocsi de emlékeim csalnak.

Akkor most ki babrál ki kivel II.

2009.10.06. 17:34 | Csizmazia István [Rambo] | 2 komment

Címkék: microsoft frissítés káosz zombi biztonsági botnet adatbiztonság

Ha valaki esetleg nem olvasta volna merő véletlenségből az első részt, az a Propeller oldalon találja meg azt. A mostani csörte kicsit ennek a folytatása, egyfajta "Return of the Babrál", ám minő fájdalom, hasonlóan csüggesztő konzekvenciákkal. Soha ennyit még nem idéztünk (és nem is fogunk :-) saját magunktól...

Mogyoróhéjban összefoglalva, az eddigi szituáció úgy nézett ki, hogy a Windows frissítések egy részéhez függetlenül a kópia "színétől", a szürkén át az egyértelműen lopott feketéig bezárólag hozzáférhetünk ugyan, de viszont **a szintén az exploitok célkeresztjében álló Microsoft Officenál már nem ez a helyzet**. Ott csak és kizárólag a fizetős hófehér ügyfelek tölthetik le a biztonsági frissítéseket. *"A Windows egy pénzért árusított operációs rendszer, ezzel így önmagában semmi baj. Viszont ha megnézzük napjaink legújabb fertőzési forrásait, nem lehet nem észrevenni, hogy a manapság olyan népszerű fájlformátumokra készült exploitok (biztonsági sérülékenységet kihasználó támadó kódok) között a Microsoft Office állományai milyen hatalmas arányban vannak jelen (természetesen azért jut még itt hely az Adobe PDF és SWF, valamint az Apple QuickTime típusoknak is). Ám az Office biztonsági frissítései ugyanígy már nem férhetőek hozzá bárki számára, ezeket csak és kizárólag a jogosult, legális felhasználók tölthetik le és futtathatják."*

Le is vontunk akkor a konzekvanciákat, inkább beidézem: "*Így aztán a védtelenül maradt milliók bár valóban jogosulatlanul használják az irodai programcsomagot,* ***mégsem biztos, hogy a biztonsági frissítések visszatartása a legmegfelelőbb módszer a legalizálás kikényszerítésére****. Tömegesen jelennek meg olyan weboldalak, amelyeken preparált, a sebezhetőségeket kihasználó Office dokumentumok találhatóak, amelyek megfertőzik a gyanútlan felhasználó frissítetlen gépét.* ***Ha pedig kiszámolnánk, mekkora kárt okoznak világszerte az így eltérített gépek az általuk végzett nagyüzemi méretekben zajló kártékony tevékenységekkel: spamküldés, információk kiszivárogtatása és illetéktelen kezekbe juttatása, weboldalak támadása, kémprogramok és csalárd, zsaroló trójai kártevők terjesztése, akkor sokkal nagyobb kártételt jelent a számítógépes társadalomnak az ezek miatti káosz, mint amekkora bevételt ezzel egyetlen piaci szereplő, a Microsoft realizálni próbál****. Vagyis a biztonsági frissítések elmaradásának szempontjából nem csak az a szűk keresztmetszet, hogy a felhasználók értik-e a fentieket, érdekli-e őket, legyőzik-e a lustaságukat, elég fontosnak tartják-e, hogy megtegyék, hanem hogy ez nem mindenki számára hozzáférhető."*

És most jön az új "fordulat", amely csak annyiban új, és csak annyiban fordulat, mint ahogy Karinthy felejthetetlen Így irtok ti című művében a nagy Stefan Butler Leacock: A rejtély titkának kifigurázásban olvashatjuk: "És akkor hirtelen és váratlanul ismét nem történt semmi". A **Microsoft kijelentette, az illegális Windows példányt birtoklóknak nem engedik** telepíteni/használni az új ingyenes Microsoft Security Essentialst. (Bár a **telepítéskori Genuine Advantage zaklatás** látszólag csak XP alatt jelentkezett, Windows 7 esetében egy sima, next-next-finish menet után már futásra kész is volt.)

Akkor **képzeljünk el most egy a hatástanulmányt. Kinek a gépén fut ma a botnet? Akit nem különösebben érdekel a gépe**, csak ki és bekapcsolja és használja, mint egy kenyérpirítót (Múkoggy!). Esetleg érdekelné, de sajnos nem ért ért hozzá, nincs ideje és nem is veszi a fáradságot az utánanézésekhez vagy a segítségkéréshez. Nem futtat semmilyen ingyenes antivírust vagy kémprogram elleni védelmet. **Nem vette a Windowst, hanem a szomszéd Stefan, Steve, Estefan, Sztyópa, Pistike, etc. telepítette neki a warezt.** Nem hajlandó tanulni és

nem hajlandó/akar/képes anyagi áldozatot hozni a szoftvervásárlás terén sem - értsd nem futtat semmilyen fizetős antivírust vagy kémprogram elleni védelmet. Nos neked, igen-igen, pontosan neked lenne jó egy olyan automatikusan működő, frissülő cucc, ami megmentene minket, többieket a napi több tízezer új zombitól, a temérdek spamtől, az e-mailben, fertőzött weblapokban vagy csevegő üzenetekben küldött kártevőkre mutató linkektől.

A befejezést megint csak a klasszikusoktól idézem;-) *"□a valaki lopott programot használ, az persze törvénybe ütköző cselekmény és ez a felhasználó felelőssége, ám vannak erre szakosodott ellenőrző szervezetek, ennek pedig főleg jogi kérdésnek kellene lennie. Sajnos azonban technikai kérdés is, ami pedig minden internetezőt veszélyeztet. Az így elmaradt profitért cserébe* ***az egész számítógépes világ kapja büntetésképpen a számtalan és hatalmas méretű zombihadsereget, és ez semmiképpen nem kedvező állapot, ennek változnia kellene****."*

Sajnos azonban **így elég kevés remény marad erre**, olyan kevés, mint vöröshagymában a proletáröntudat. Nagy kár. A letölthető Essentials csomag **így is - úgy is meg fog érkezni különböző letöltési oldalakra, torrentre, rapidshare-re, ahonnan az szedi le majd, aki akarja.** És ez még a jobbik eset, mert később biztosan lesznek megpatkolt, buherált fertőzést terjesztő ál telepítőcsomagok is.

A Microsoft azt mondja: "The company has said that it doesn't want unprotected PCs to host viruses and make the work of computer criminals easier." Ezzel szemben az MSE letöltésének és használatának korlátozása viszont vélhetően pontosan ezt fogja majd erősíteni.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1431235

Kommentek:

load error 2009.10.08. 12:45:13

Most jött ki az Office Genuine Advantage frissítés is. Ezek szerint eddig nem is nézte a Windows, hogy maga az Office legális-e?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.10.12. 11:28:42

Szia load error!

Eddig is nézte, hiszen aktiválni kellett már korábban is. Hogy aztán a felismert warez serialokat pontosan hogy zárják ki a frissítésekből, azt nem tudom.

Kártevőt tessék! Ropogós a zombi!

2009.10.08. 14:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: információ botnet kártevő bolhapiac networkwold

Friss meleg, és olcsó az ára - tehetnénk még hozzá, mint vásári kikiáltó. Ugyanis a hírek szerint üzemel a kártevőket forgalmazó egyfajta bolhapiac egy ismert weboldalon.

A Networkworld számolt be róla, hogy a pay-per-install weboldalon nyíltszínen folyik az ilyen jellegű üzletkötés. A virtuális piactér célja, hogy **összehozza a potenciális megbízókat a botnet pásztorokkal**. Nem lepedődtünk meg persze korábban sem azon, hogy a BBC hogyan és honnan jutott olyan könnyen botnet vezérlésre alkalmas programhoz, hogyan béreltek ki egy ilyet - valószínűleg egyáltalán nem volt nehéz dolguk. De míg az ő akciójuk inkább a figyelemfelkeltést szolgálta, az átlagos kuncsaftok jelentős része persze nem ezért megy oda.

Az árak a beszámoló szerint országonként változóak, egy 1000 tagú botnet hálózat 110 USD-t kostál az Egyesült Királyságban, 60 USD ha mindez Olaszországban van, a franciaországi ezer gépért már csak 30 USD-t kell leszurkolni, és ugyanez Ázsiában mindössze 6 amerikai dollárba fáj. **Biztonsági cégek szerint az ilyen kártékony kódok készítői Kelet-Európában**, illetve a volt Szovjetúnió területéről próbálnak meg ilymódon jövedelemhez jutni.

Az egyik **legkelendőbb árucikk jelenleg is a hamis antivírus** program, ez most éppen 70 USD. Eric Chien (Symantec) szerint **kevés az esély az ilyen ellenőrizetlen piacok bezárására**, mert mindig megfelelő érinthetetlen tárhelyszolgáltatót találnak maguknak, illetve **szükség esetén sűrűn költözködnek** is.

És persze - ezt már mi mondjuk - a prostitúcióhoz és a kábítószer piachoz hasonlóan - olyan igényeket szolgál ki, amire sajnos van kereslet.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1436227

Kommentek:

Nincsenek hozzászólások.

Kicsi fej jobb ide, mint a nagy

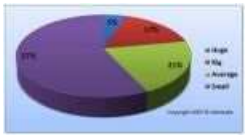
2009.10.12. 11:25 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kis méret botnet damballa

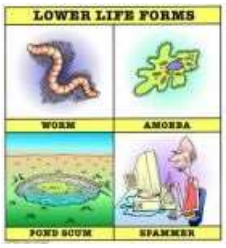
Vajon mindig a méret a lényeg? Ahogy a Lokomotív GT Boksz! című számában fogalmaznak az ökölvívással kapcsolatban, az úgy tűnik, használható lehet a botnetek körében is.

Erik Wu biztonsági kutató a Virus Bulletin 2009 konferencián tartott előadást a botnetek irányításáról. A Damballa cég munkatársai **hatszáznál is több zombihálózatot vizsgáltak három hónapon keresztül**, és úgy találták, a kisebb méretű, száz tag alattiak sokszor veszélyesebbnek számítanak mint a nagyobb, olykor félmillió zombigépből álló társaik. Ezekből temérdek létezik, és ők mintegy kicsit a "radar alatt repülve" sokszor **könnyebben észrevétlenül maradhattak, profin és gyorsan reagálva menedzseltek**, de ha szükséges volt, akár együtt is működtek másik botnet hálózattal: "az úttörő ahol tud, segít" alapon ;-)

Megfigyelhető volt például, hogy ha az egyik kis botnet hálózatból kiesett egy szerver, akkor egy másik kisebb hálózat kisegítette azzal, hogy **ideiglenes megosztotta vele erőforrásait**. Más formái is előbukkantak az érdekes együttműködéseknek, például egy botnet a feladataihoz ha szükséges, képes lehet újabb alhálózatokat is bekapcsolni. Természetesen ezek **a képességek azon is múlhatnak, hogy az aktuális bérlő kizárólagos használatra fizeti-e a díjat** vagy sem.



Az előadáshoz elkészített tortadiagramból szépen kiolvasható, hogy **a kis (<100) méretűek adják a botnetek többségét, az összes ilyen hálózat 57 százalékát** teszik ki. Az átlagos méretű botnetek méretét a kutatók pedig 100 és 500 közötti irányított fertőzött zombigépre becsülik.



A kisebb botnetek igen **sűrűn kerülnek ki kisebb céges hálózatokból**, ezért a tanulmány már csak emiatt is figyelmeztető jel lehet. A helyzetet az is súlyosbítja, hogy sokszor bérlésre sincs szükség, hiszen ha valaki ért hozzá, az egyszerűbb botnet **készletek már pár száz dollárért vagy akár ingyen is letölthetőek** a különféle hacker fórumokról, kalóz torrentekről vagy hírcsoportokról. Mindenesetre **a botnetek forgalmának alapos tanulmányozása** közelebb vihet minket a hatékonyabb védekezéshez.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1444101

Kommentek:

Nincsenek hozzászólások.

Beteg a hóleopárd

2009.10.13. 17:01 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hiba macintosh leopard snow adatvesztés

Úgy tűnik, a Macintoshnál is érdemes lesz előbb-utóbb bevezetni a korábbi Windows szabályt: csak akkor használjunk egy operációs rendszert, ha már a második Service Pack is megjelent hozzá. Durva **adatvesztési hiba az Snow Leopardban**.

A cikk szerző is falbaverhetné a fejét, **ha mostanában guest-ként jelentkezett volna be, áldott szerencsére nem így történt**, pedig már az első héten frissített. A dolog lényege nagyjából annyi, ha a rendszerbe **valaki guest-ként jelentkezik be, majd ezután egy valódi accounttal lépünk be**, akkor ez utóbbinak minden adata, beállítása törlődik.

A hibát igen **sokan észlelték már**, egyes forrásokból szeptember 12-i hibajelzésről is olvashattunk, az Apple pedig nyugtázta is, hogy tud a dologról, ám a javítás azonban mindmáig nem készült el, pedig több milliónyi felhasználót érint. Időközben megjelent egy remedy a Cnet oldalán, mit tegyen az, akinek emiatt elszálltak dolgai, **hogyan hozhatja vissza a Home könyvtárát**.

Amíg viszont végleges javítás nem történik, **tanácsos a guest account átmeneti letiltása**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1447151

Kommentek:

Nincsenek hozzászólások.

Ethical Hacking Workshop 2009

2009.10.16. 18:23 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: béres workshop 2009 hamis péter hacking antivirus netacademia mave ethical juraj malcho gmer

A **Magyar Villamosmérnök- és Informatikus-hallgatók Egyesülete (MAVE)** a hagyományoknak megfelelően 2009 őszén is megrendezte nemzetközi szakmai hetét, más néven workshopját. Igyekeztek egy napjainkban aktuális, nagy érdeklődést kiváltó témát választani, ennek eredményeként döntöttek **az ethical hacking, az informatikai biztonság, valamint a digitális adatvédelem** mellett. A csütörtöki napon jártunk a helyszínen.

Elsőként Juraj Malcho (ESET) tartott előadást "Is there a lawyer in the lab?" címmel. Akik emlékeznek a Zango hirdetési cég és a Kaspersky antivírus fejlesztő közötti perre, annak ismerős lehetett a szituáció. Manapság nem csak a kéretlen (vagy az apróbetűs részben figyelmetlen olvasás miatt megjelenő) **reklámcégek kérik programjuk kivételét a felismerések közül**, de van olyan arcátlan **hamis antivírus készítő is, akik szintén ezt szeretnék**. Úgy tűnik, **a jogászkodás lassan elkerülhetetlenül beszivárog** a víruslaborok mindennapjaiba.

A második előadásban **a trójai programokról szólt**am pár keresetlen szót, honnan hová jutott el a világ, és miért lettek ilyen sikeresek. Érdekes epizód, hogy a sokkal **biztonságosabb Macintosh és Linux platformokon is sikerrel lehet bármit telepíteni, ha a becsapott, megtévesztett felhasználó gondolkodás nélkül telepíti azt, amit elétesznek**, na és persze készségesen begépeli hozzá az admin jelszót.

Itt igyekeztem sok konkét, a blogban is tárgyalt jellemző példát megmutatni a hallgatóknak. Kedvenc példám is szerepelhett benne, az egyszerű szövegállományt .EXE-nek átnevező, majd a letöltő oldalaknak elküldő felhasználó esete.

Meglepetésére számos díjat nyert vele, és volt olyan szerkesztő, aki még e-mailben is gratulált neki.

A záró előadás egy **igazi csemege volt, Béres Péter (Sicontact Kft.) a hamis antivírus programok** áldatlan hatását mutatta be élőben. Nincs egyszerű helyzetben az **az átlagfelhasználó, aki úgy fertőződik meg, hogy semmilyen védelem nincs a gépén**. Péter napi nyolc órában a NOD32 technikai supporton dolgozik, és számtalan esetben segít olyan embereknek megszabadulni a fertőzéstől, akiknek a gépén **a kártevő letiltja az antivírus weboldalak látogatását, vagy éppen a regedit.exe szerkesztő futattását**.

Most **lépésről lépésre nyomon lehetett követni**, hogyan lehet a Laookon szobor csoport kígyóiként számtalan másolatot, és seregnyi kéretlen állományt szétszóró hamis antivírust puszta kézzel, apró segédprogramokkal (Avenger, Gmer, Unlocker, stb.) kipucolni.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1454083

Kommentek:

Nincsenek hozzászólások.

A lepkegyűjtő

2009.10.19. 16:12 | Csizmazia István [Rambo] | 2 komment

Címkék: kína msn csalás adathalász

4-3-2-1. A Tubela Management International bemutatja: **hogyan lopjuk el felebarátaink MSN accountját, színes, szagos, szélesvásznú szovjet egészestés film**, korhatár nélkül megtekinthető.

Kínai barátainkra **senki sem mondhatja, hogy lassan dolgoznak**, vagy hogy megalszik a tej a szájukban. A csalásban **résztvevő domaint 2009. október 16-án jegyezték be**, és amint a nagy nyilvánosság felé fordul, már költöznek is majd tovább. Addig azonban küldözgetik a csalárd üzeneteket - ahogy azt az F-Secure weblogban is láthatjuk. Jön egy üzenet, benne a linkkel, és **aki nem azzal kel, nem azzal fekszik, hogy vigyázni kell a csalásokra**, az a szokásos 5% társaságában szépen begépeli az accountját.

Már szinte minden webes figyelmeztető plugin feketelistázta, a WOT, a Site Advisor, Safe Web, stb. Megnyitni is csak Operaban sikerült, a Firefox már nem is akarta megjeleníteni egyáltalán.

Aki meg nem látta vagy olvasta a címadó művet, annak pedig jószívvel ajánlom John Fowles könyvét. Azt hiszem, azt kellene **megszokni sokaknak, hogy nem csak nagy néha történik egy-egy csalási kísérlet, amit telente az öregek elmesélnek a fialakoknak a fonóban**

tanulságképpen, hanem úthengerszerűen borul ránk napi többszáz próbálkozás, és sokszor éppen a fiatalok tudnak segíteni a gyanútlan idősebbeknek. Messziről nézve meg **ez is egy a sok közül, akik nevünkre-jeszavunkra hegyeznek**. A Tubela Managementnek egyébként meg toll a fülébe, ha csak yta0h8a@126.com e-mail címre futja nekik, legalább a látszatra adhatnának, milyen szánalmas igénytelen konspirálás ez, 007 sünt nekik.

Azért **egy valódi haszna mégiscsak van az adathalász weboldalnak**. Akinek eddig sokat és fáradságosan **törnie kellett a fejét megfelelő beikszelendő lottó számok miatt**, az itt **most ingyen tippeket kaphat minden weboldal frissítésekor** az "Önnek x darab képe van a galériában" szöveg melletti véletlen számból ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1459885

Kommentek:

atko 2009.10.19. 17:20:57

Aki hülye haljon meg.
És ha ez durván hangzik, akkor aki barom, az tanuljon meg bőgni a kérődzőek nyelvén.
Pedig a gondolkodás nem csak a főemlősök privilégiuma.
Múú én szóltam.

HoaxSpecialist · http://hacker.blog.hu 2009.10.22. 20:53:06

Amugy viccesek ezek az arcok, par honapja az egyik szerveruket nekialltunk bruteolni, nmapolni, pingelni par iprol. Utana 2-3 hetig a szinuket sem lattuk a piacon :D

Facebook: Önök kérték, mi telepítjük

2009.10.20. 20:20 | Csizmazia István [Rambo] | 3 komment

Címkék: javascript orosz facebook pdf exploit

Rosszfelé halad a világ, nem is lehet kérdéses. Rémálmaiban mindenféle kártékony Firefox pluginnal találkozom, de aztán a végén szerencsére mindig felébredek, és még csak nem is lóg bele a kezem sehova ;-) Viszont **a Facebook alá telepíthető alkalmazások területén** sajnos egyre inkább kezd elszabadulni a pokol a valóságban is.

Nem számít többé egyedi esetnek a múltkori Fan Check incidens. Divat lett a dologból a Facebook kiegészítők háza táján, és ezekből a kártékony kisalkalmazásokból egy egész csokorra valót nevez meg Roger Thompson, az AVG szakértője.

Ha telepítés után egy PDF is felnyílik, emlegethetjük a fejlesztő felmenőit

A felsoroltak **telepítése során egy orosz oldalról egy kártékony PDF állomány jelenik meg**, és hamis AV-szerűen nem létező vírusfertőzésre figyelmeztet például a Tűzoltós játéknál, **ha a látogató gépe nem naprakész a frissítések tekintetében** (magyarul exploittal támadható).

- City Fire Department
- MyGirlySpace
- Ferrarifone
- Mashpro
- Mynameis
- Pass-it-on
- Fillinthe
- Aquariumlife

Lehetőség szerint érdemes tartózkodni a Facebooktól ;-), vagy legalábbis a letölthető alkalmazásoktól ;-), de legalább a fent felsorolt fertőzöttektől ;-) Vagyis **ha valaki egy extra PDF-et lát kinyílni a telepítés után**, emlékezzen bátran az itt leírtakra.

A weboldal szeretnivaló kódja

A Javascript szépségei, avagy hogyan babráljunk ki az olvasóval

A józan ész diadala a kezdeti zavaros kód felett

Természetesen emellett **a klasszikus csalások is napirenden vannak**, ahol az "Akarod-e tudni, melyik Simpson karakter is vagy?" kérdésre a delikvens **csak az accountjának (név, jelszó) begépelése után kaphatja meg a választ** (Bhalekh Simpson), az adathalász meg a jelszót ;-)

A "megnyert" letöltődő extra PDF, nélküle élni nem lehet ;-)

Mivel **az alkalmazások rendszerint külső külföldi szervereken futnak, azt sem egyszerű ellenőrizni**, pontosan mi zajlik a nevünkben, mikor élnek vissza a személyes adatainkkal. Ez a közösségi portálokon való ügyködés **lassan kezd az önfeledt örömködés helyett egy állandó veszélyekkel járó dzsungelharccá** degradálódni. Fülig Jimmy szavait kissé elferdítve kijelenthetjük: Tapasztalt egyének babonája, hogy a közösségi oldalakon való császkálás ritkán vezet jóra ;-)

Ajánlott bejegyzések:

- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1463204

Kommentek:

nit 2009.10.25. 09:35:03

Szia István!

..sajnos hamarabb lett trojaim nem is egy --hanem igen sok változata, mielött nod32-öm. Egy fénymásolóboltban kaptam a pendriveomra :) :P
Olyan mintha nem igazán akarna a noddal sem javulni a helyzet.
Rootkit irtókkal is probálkoztam... de van egy trojaim ami úgy tünnik folyton módosul? nem igazán értem mi történik a gépemen.
win32/troja gen-nel indult..aztán ennek a variációival? találkoztam..
-az lenne a kérdésem h csak egy újratelepítéssel tudom teljesen leszedni?
(3hete lett újra rakva...ha lehet kihagynám..)
-a telefonomon nem szoktam netezni emiatt nem raktam rá virusirtót..azonban mióta fenn áll ez a helyzet nem merem a gépemhez csatlakoztatni...gondolom nem tenne neki jót?
-a pendriveról pl egyáltalán nem tudtam letörölni az abc összes betüit felvonultató értelmetlen halmazokat...
-pár tanácsot kérnék mit tegyek, mert amiket eddig ismerösök mondtak sajnos nem vezetett célra
Előre is köszönöm.

Üdvözlettel!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.10.25. 21:41:20

Szia nit!

Szerintem meg lehet szabadulni az ilyentől formázás nélkül.

A NOD32-t frissíteném, és ellenőrizném a beállításait: kéretlen alkalmazások keresése, veszélyes alkalmazások keresése, kiterjesztett heurisztika legyen bekapcsolva, és így végeznék egy teljes keresést.

Annak sincs akadálya, hogy a mellétegyünk egy külön kémprogramirtót - én a Spyware Terminatort használom, jól megférnek egymás mellett - hiszen a kémprogramirtó bátrabban nyúl a mentesítéskor a géphez, nem csak a fertőzött fájlt törli, de a kinyesi a Registryből az idevágó összes indítóbejegyzést, plusz a nem fertőző, de felesleges komponenseket is törli, stb.

Ha pedig nem boldogulsz ezekkel, vagy ennek ellenére, keresd bátran a supportunkat, és ők részletesen segítenek, ha kell, távirányítanak:
www.eset.hu/segitseg/kapcsolat

atko 2009.10.26. 14:24:59

"Lehetőség szerint érdemes tartózkodni a Facebooktó"
A bátor harcos bölcs és megfontolt, és mást küld maga helyett meghalni.
És nem mutogatja meg mindenkinek az alsónadrágját.
A közösségi portálok akkora átverések...
Sok birka meg megy a kolomp után a vesztőhelyre.

"Gyárilag" fertőzött Vista kalóz lemez

2009.10.22. 13:01 | Csizmazia István [Rambo] | 16 komment

Címkék: windows office warez fertőzött kártevő

Nehéz igazságot tenni, nyilvánvaló, hogy **a warez oldalak, letöltések egyrészt jó kísérleti terepei az új kártevők terjesztésének,** másrészt **a Microsoft is ujjal mutogathat propaganda-ízűen az eset után**: ugye megmondtam, hogy bontott csirkét, meg csak és kizárólag eredetit kell venni tőlem jó pénzért? Ami biztos, hogy **volt egy olyan warez Vista ISO széria, amely már alapból egy trójai kártevőt tartalmazott**.

Kutyából nem lesz szalonna, ezt bizonyítja az is, hogy a letölthető Windows 7 build 7100 változatból is volt már fertőzött széria, valamint az Office 2010 prerelease verzióból is volt egy hasonlóan kártékony trójai kóddal kibélelt letöltés. Az ingyenes, ám fertőzött kalózváltozatok Win32/Bifrose.EO trójait tartalmaztak, amely hátsó ajtót nyit a rendszeren. Nagy látványos kárt nem okoz, de azért vannak kellemetlen hatásai. **Lekapcsolja a Windows tűzfalát, valamint egy távoli szerverrel kommunikálva további kártékony kódokat** igyekszik a fertőzött számítógépre letölteni.

A hír érdekessége, hogy ellenőrizve minden más hasonló találat egy helyre, a Softpediara mutatott forrásként. Vagyis emiatt a hitelességét százszázalékos nem sikerült bebizonyítani.

Az **sem világos, hogy ezek a mindig naprakész kalózok most mit pepecselnek ósdi Vistákkal, a vadi új Windows7 helyett**, szóval nem egészen értjük. Minden esetre Windows szoftvert csak tiszta forrásból: magától a gyártótól vagy pedig megbízható kínai kereskedőtől ;-) érdemes beszerezni ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1467155

Kommentek:

BKV figyelő.hu · http://bkvfigyelo.hu 2009.10.22. 14:29:00

A Windows 7-tel nem kell vigyázni, a letöltött kalózváltozattal kell.

tomi888 2009.10.22. 14:30:46

Miért a következő címmel került címplapra ez a post???
Elég megtévesztő cím, ráadásul negatív irányban...

Antivírus - Óvatosan a Windows 7-tel
Már a Vistából is volt kint gyárilag fertőzött verzió

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.10.22. 14:56:36

Szia tomi888!

Ezt én sem értem, biztos bulvárosítani akarták.

Én a teljes cikkben igyeztem korrekt és mértéktartó lenni, sőt azt is jeleztem, hogy bár a Win7RC-ből valóban volt több forrásból is megerősítve trójai változat, ez a mostani hír egyedül a Softpedia híre, pl. a TheRegister-en az eset nyomát sem találtam.

Új autentikus címnek javaslom még:
- Hasbaszúrta élettársát, majd megevett egy rúd csabai kolbászt
- Épségben előkerült az elveszettnek hitt Marsjármű a balmazújvárosi kiserdőben
- Hihetetlen, Kiszel Tünde most tényleg megcsinálta!

mykee · http://www.facebook.com/mykeehu 2009.10.22. 14:57:07

Rambo kérlek, szólj az Indexeseknek, mert már megint 10 Ft-ból aranytojást tojó tyúk lett a weblapjukon, mert ezt írták ki:
"Antivírus Óvatosan a Windows 7-tel
Már a Vistából is volt kint gyárilag fertőzött verzió."

Gyárilag nem adott ki a Microsoft fertőzött verziót, az idézőjelet meg lespórolták, ami komoly félreértésre adhat okot.
Köszönöm, és az indexesek meg... :-)))

Mykee

mykee · http://www.facebook.com/mykeehu 2009.10.22. 14:58:14

@Csizmazia István [Rambo]: Na meg is előztél. :-))

hapcika 2009.10.22. 15:20:15

Miért pepecselnek a Vistával? Talán , mert kihirdették egyes Vista változatokat olcsón frissiteni lehet Win7-re.

he boy without a name 2009.10.22. 15:25:01

Most tisztára két shake-be vagyok esve, mert az XP-m már haldoklik, tört Win7-et meg nem merek felrakni.

Arról van infótok, hogy a Release Candidate-et mennyire lehet tartósan és stabilan használni? Igazából meg lehet elkéne menni a Saturnba, azt venni egyet 16 rongyért, az végül is nem tétel érte, főleg ha ez is 8 évig húzza.

karatekutya 2009.10.22. 15:37:54

és ha felrakom a vírusos Win7-et, és utána felrakok egy letorrentezett víruskeresőt, akkor az leszedi a Win7 vírusát? ^_^

it_guru · http://www.itguru.blog.hu 2009.10.22. 15:42:37

Hát igen, nem túl elegáns cím az Indextől.

Nekik azonban a pörgés a lényeg a bannerek miatt. Hogy ez mennyire etikus, az más kérdés. A Microsoft PR részlege mindenesetre nem tapsol örömében, az biztos.

nszóltam 2009.10.22. 15:49:52

Egy még be nem foltozott biztonsági hiba miatt nem ajánlja a Windows 7-re váltást a Free Software Foundation Europe. Az FSFE ugyanis arra hívta fel a figyelmet, hogy a redmondi cég a mai napig nem javította ki azt a biztonsági hibát, amire a Computer Emergency Response Team (CERT) már október hatodikán rávilágított. A CERT-csoport a rést nagyon veszélyesnek minősítette és közölte, hogy a segítségével bárki sikeresen hajthat végre DoS-támadásokat az adott számítógép ellen.

nszóltam 2009.10.22. 15:50:26

Egy még be nem foltozott biztonsági hiba miatt nem ajánlja a Windows 7-re váltást a Free Software Foundation Europe. Az FSFE ugyanis arra hívta fel a figyelmet, hogy a redmondi cég a mai napig nem javította ki azt a biztonsági hibát, amire a Computer Emergency Response Team (CERT) már október hatodikán rávilágított. A CERT-csoport a rést nagyon veszélyesnek minősítette és közölte, hogy a segítségével bárki sikeresen hajthat végre DoS-támadásokat az adott számítógép ellen.

stanyecli 2009.10.22. 15:52:45

Milyen érdekes, hogy akkor jönnek ezzel a "vírusos-a-warez" c. epizóddal, amikor a kanyarban van az új oprendszerük bevezetése. Nahát-nahát.

belagezabela 2009.10.22. 16:48:29

Az egész cikk egy baromság, maga a Windows 7 egy vírus csak már mutáns alakban nagy terjedelemmel.
Nekem kínai kell hogy semmit se értsek belőle.

HoaxSpecialist · http://hacker.blog.hu 2009.10.22. 20:48:59

Hogyhogy mit pepecselnek? Ezt Te sem gondoltad komolyan! 0day, uj team, uj rls, kikell probalni hogy lehessen azt is szidni! Es igen, ha ertenek hozza teleb*sznam en is a netet a trojanos hekkelt win7 + vista distroimmal.. :D

gothmog 2009.10.25. 20:26:22

@mykee: na, aki az egész tetejébe még törött vírusirtót is használ, az bizony azt kapja, amit megérdemel.

zcore 2009.11.06. 13:02:02

Igen, valoban igaz...Aki törött virusirtot használ, az azt kapja amit megérdemel...De manapság már senki nem veszi meg az eredeti Windows-ot...

Bízunk-e a felhőkben?

2009.10.26. 16:49 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság felmérés bizalom felhő cloud

A klasszikus viccben Móricka megkérdezi Taszilótól, hogy van? A válasz egy tömör "Jól". És bővebben? "Nem jól". **Manapság, ha megkérdezik a felhasználókat például Amerikában, bíznak-e a Cloud technológiában**, a válasz eléggé meglepő lehet sokaknak. Szállj le a felhőmről - a legendás Rolling Stones már 1967-ben tudott valamit :-)

Egy felmérés szerint kevés benne a bizalom. A napjainkban **igen divatosan hangzó felhőalapú technológiák** bizonyos esetben valóban vethetnek fel kérdéseket. Aki fejben már eljutott odáig, hogy **cége, vállalkozása irodai munkáját ne webes online office megoldásokkal oldja meg biztonsági megfontolásokból**, az nyilván ugyanennek a gondolatmenetnek a hatására bizalmas adatainál sem fog felhőt, távoli ismeretlen harmadik fél szolgáltatását használni. A kétévenként elvégzett felmérés **emellett minden fajta egyéb biztonsággal kapcsolatos témára is kiterjedt**, így többek között megtudhattuk, az amerikaiak 42 százaléka aggódik a számítógépes vírusok és hatásaik miatt. Emiatt és személyes adataik miatt **szerintünk aggódhatnának egy ekkora országban kicsit többen is ;-)** Persze ehhez azt is hozzá kell venni, hogy mindössze egy ezer fős minta telefonos kikérdezése alapján történt meg ez a felmérés.

De térjünk vissza az eredeti kérdésre. Mi is történik egy ilyen felhős történetben? **Az adat szinkronizálódik, feltöltődik "valahova", ahol végrehajtják, elvégzik, megosztják valahol egy szolgáltató** szerverén. Az **adja magát, hogy a titkosszolgálatok és a rendőrség biztosan NEM fogja az adatbázisait így kezelni**, de lassan már **egy átlag ember, átlag cég esetében is paranoiás félelmet okozhat annak az esélye, hogy személyes adatai esetleg illetéktelen (konkurrens, rosszindulatú) kezekbe kerülhetnek**. A leghétköznapibb személyiség lopás is kellemetlen lehet annak, akivel épp ez megtörténik.

Emellett persze nyilvánvalóan lesz majd az a réteg, akinek szüksége is lesz az ilyen felhős erőforrásra, és adatainak természete sem akadályozza majd meg ebben, **továbbá (vagy főleg) az IT infrastruktúráján spórolni akar**/kényszerül. **A biztonsági incidensek, kihívások tekintetében** nem láthatunk a jövőbe, de mindenesetre annyi egészen biztos, próbálkozások biztosan lesznek majd.

· 1 trackback

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1475505

Trackbackek, pingbackek:

Trackback: Bízzunk-e a felhőkben? 2009.10.26. 20:34:44

Rambo a kérdést Bízunk-e a felhőkben? módon tette fel, a PCWorld egy cikkéből levonható következtetéseket elemezve. Én inkább azt feszegetném, mennyire bízhatunk a cloud alapú szolgáltatásokban. Tipikus Felhő-szolgáltatás a Google féle Dokumentumok, v...

Kommentek:

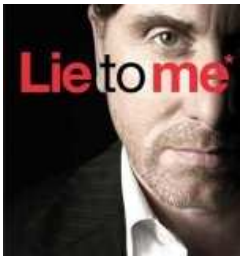
Nincsenek hozzászólások.

Hazudj, ha tudsz

2009.10.27. 16:51 | Csizmazia István [Rambo] | 2 komment

Címkék: spam kínai logo hamis áruház nyersfordítás verisign

Az eredeti sorozat címe a Lie to me!, és talán nem tévedünk túl nagyot, ha úgy vélelmezzük, a hamis vírusirtókat készítő cégek nem pusztán amiatt végzik eléggé el nem ítélhető áldásos tevékenységüket, mert szolgalelkűen csak ezt az utasítást hajtják végre. Egy friss kéretlen spam kapcsán **még Dr. Cal Lightmannek sem kell lennünk, hogy kiszúrjunk pár hamis állítást**.



Az embernek vannak bogarai, rigolyái, és kedvenc történetei, amikre egy idő után olyan sokszor hivatkozik, hogy végül azt mondja: ez olyan jó, hogy mától kezdve én mondtam ;-) Többször is idézve lett már az, amikor főhősünk 2007-ben gondolt egyet, és a nagy semmit becsomagolva elküldte a letöltési oldalakra. A nagy semmi esetünkben egyetlen szövegfájlt jelentett, EXE-re átnevezve. Ebben a szerző nagyjából ezt írta: **"Ez a program egyáltalán nem csinál semmit. Sőt, még csak nem is fut. Azért készítettem, hogy kísérletezzek, vajon hány díjat nyer majd a shareware oldalakon. Az eredményt a www.successfulsoftware.com weboldalon teszem k□zzé."** Mégis, íme a pár hónap alatt elért díjtáblázat, amiket a különböző letöltő oldalak szerkesztői adományoztak neki. Volt, amelyik még **kül□n e-mailben is gratulált, hogy "Great job□" :-D**

Így vesztettük hát el idővel a plecsnikbe vetett bizalmunk egy részét, és mai történetünkben is keletkezik hasonló tanulság, bár egész arzenált láthatunk ezekből. **Nem mindegy, melyik weboldalon látjuk azt a plecsnit**, különösen, ha a domaint előtte két héttel regisztrálták.

(Persze van ez a Brezsnyev effektus, hogy a kitüntetéseket mindig azok kapják, akiknek már van, és az a nagy kérdés, hogyan kapták meg a legelsőt? Mindemellett maga az áruház nem is ezen az egy kőbevésett központi címen, hanem mindig más URL-en érhető el, mint a hamis gyógyszereket árusító helyek.) A most **beesett spam magyarul k□sz□ni ugyan a "Helló"-t**, de egy semmitmondó hotmailes címről érkezett, magára valamit is adó marketinges üzletember ilyet nem tesz. Persze az is igaz, ha a kéretlenül érkező levelet face to face a kaduo-ról írná, akkor is a kukánkban landolna. *"Jó hír gyorsan. talán a helyszín www.kaduo-88.com. adok nektek néhány hasznos információt, amit most már nagyon szeretné birtokolni, nagyszer? felszerelés"*

A szerzők láthatóan translate.google függőségében szenvednek, ezért vélhetően minden náció megkapta már az adagját a kéretlen reklámjukból. Néhány helyen már fent is ülnek a spamfilter feketelistáján, nem ügy. Inkább érdekes lehet **a csalás-megtévesztés gátlástalansága, amit a "McAfee SEC□RE" és a "Verisign" logóval szeretnének elhitetni**.

Ha próbaképpen belépnénk, vagy regisztrálnánk, nyoma sincs a megbízható hitelesítésnek, tanusítványnak, https-nek. Körülbelül az az eset, amikor "parasztvakításnak" **a favicon.ico helyére betesznek egy lakat képet**, és akinek ez elég a tiszta, száraz, SSL érzéshez, azt már sikeresen be is tudják csapni.

Szóval ne legyünk egybites plecsni fetisiszták, kezeljük értékén az információkat, **nem csak az számít mit mondanak, hanem az is, ki mondja. Kételkedem, tehát vagyok - a mai világban nem lehet más a jelige, el kell fogadni**. Nem akarjuk profanizálni a dolgot, hogy aki itt vásárol, az sikeres ember nem lehet. Ezért nyissunk hát lovagiasan egy esélyt, lehetőséget a másik oldalnak is. Aki a fentiek dacára mégis sikeresen nagybevásárolt a jelzett boltban, elégedettség volt, megírhatja nekünk okulásul a sikertörténetét egy kommentben, kíváncsian várjuk. A korábbi Dubai MLM-ben meggazdagodott hazánkfiai mindenesetre mindeddig még nem hívtak meg minket arra a korsó sörre, ami azt bizonyítaná, az odaregisztráltak sikeres milliomosok és az élet császáraivá lettek.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1478154

Kommentek:

□ann Le Pentrec · http://lnk.bz/t7c 2009.11.05. 20:15:18

No igen... sajnos ez is arra épül, hogy x ezer látogató közül majdcsak bedőlnek páran, és akkor már megvan a zsíros bevétel.

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.11.26. 14:14: 7

Végre megtaláltam kedvenc csalással kapcsolatos kommentemet. Megtalálását nehezítette, hogy
- nem tudtam mikor olvastam
- nem tudtam milyen weboldalon olvastam
- ékezetekkel volt-e írva vagy

Azért a barátommal (Google John J.) megleltük ma, buvarpocok kopirajt meg rispekt:

homar.blog.hu/2009/09/28/friss_telefonos_csalas_gepi_hivassal_tamad_az_uj_kamu_nyeremenyjartek/fullcommentlist/1#c7201636

"Múltkor láttam valamelyik műsorban, hogy milyen módszerekkel verik át az embereket.
Volt egy bevásárlóközpont, felállítottak egy kaparós sorsjegyes pultot.
Ha vettél sorsjegyet, annak az árával támogattál valami egyesületet (nem emlékszem mi volt)
Különböző árú sorjegyek voltak. Ha drágábbat vettél, nagyobb nyereményt nyerhettél meg.
Odament két csaj, mind a ketten vettek.
Az egyik nyert egy nyaralást, költőpénzzel, mindennel együtt. Örült mint majom a farkának persze. A pultos csaj adott egy telefonszámot, amit fel kellett hívnia, hogy egyeztessék az adatokat.
A vonal másik végén egy hapsi vette fel, aki a bevásárlóközpont mellett várakozott egy kocsiban. A pasi feladata az volt, hogy sokáig beszéltesse a nőt (emelt díjas hívás volt persze)
A nő pillanatok alatt minden adatát megadta, köztük a bankszámlaszámát is.
Ez volt az egyik lehúzás. Volt még egy csavar persze.
Kiderült, hogy a csaj egy 5 dolcsis sorsjegyet vett, de "véletlenül" egy olyat kapott aminek az ára 30 dollár és hát ki kéne fizetni a különbözetet.
A csaj teljesen el volt kábulva, hogy nyert, így simán kifizette a különbözetet.
Így bukott 30 dollárt, plusz beszélt vagy 15 percet emelt díjas vonalon, megadta a számlaszámát és még csak utazni se utazhatott.
:P"

Evolúció

2009.10.28. 18:01 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook malware password csalás reset bredolab

Jó látni, amint valamely dolog egyre ügyesebb, egyre több dologra figyel oda, és egyre kifinomultabban teszi a dolgát. Azért mégis **van egy hely, ahol ez a fajta törzsfejlődés kevésbé van ínyünkre**.

A számítógépes **kártevők esetében nem repesünk az örömtől**, ha készítőik ismét csavarintanak egyet a dolgok menetén. Nos most ez a Bredolab trójai esetén így esett, jött egy új variáns, amely a **Facebook jelszó cseréléssel kapcsolos e-mailnek látszik**. **Nevén szólítja a nagyérdeműt, és az ügyfelek biztonságára hivatkozva** (a kétszínű piszok ;-) nagy tisztelettel arra kér bennünket a Facebook Team nevében, hogy a mellékelt .ZIP állományból ugyan legyünk oly kedvesek, és gépeljük be a random betűket és számokat tartalmazó kódsort.

A ZIP kiterjesztés természetesen - **aki kitalálta ki ezt a kiterjesztések alapértelmezett rejtése dolgot a Windowsban, azt ütni kéne a legnagyobb számú lópatkoló csavarkulccsal ;-)** - egy futtatható állomány, amelyre kattintva a gyanútlan juzer szanzsén magára ránt egy csomó kártékony letöltött kódot, többek közt hamis antivírust.

A Facebook azóta természetesen elhatárolta magát az esettől, és figyelmeztetnek mindenkit, **sosem küldenek új jelszót levél mellékletben**. Csatolt állományban új jelszót kapni nagyjából ugyanaz, mintha a bank e-mailben érdeklődne bankkártya adataink és PIN kódunk felől: **üzemszerűen sose (Never-ever) fordulhatna elő ilyesmi**.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1481442

Kommentek:

Nincsenek hozzászólások.

Gmail tajvaniaknak

2009.10.29. 18:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: gmail tajvan phishing adathalász

Persze csak egyelőre, érzéseink szerint hamarosan nálunk is lesz majd ilyesmi. Ha nem tekintünk most a Kína vs. Tajvan ellentétre, hanem csak a technikai részt nézzük, a tegnapi evolúciós poszt alapján feltűnhet, már az adathalász levelek is szépen **igyekeznek ötvözni, egybegyúrni több apró, de hatékony megtévesztő ötletet**.

Itt van mindjárt az első, amelyben a célbavett kiszemelt áldozat személyre szóló levelet kap látszólag a kollégájától, munkatársától. Aztán emellett jön a hamis Gmail belépési oldal, ahol **"előzékenyen" a név már ki is van töltve**, már csak a jelszó begépelése kell ahhoz, hogy ~~belépjünk~~ a csaló röhögjön a markába és turkáljon a levelezésünkben.

A **TrendMicro blogjában ismertett módszer miatt érdemes mindenkinek vigyáznia munkatársinak látszó levelekkel**. (Bár aki a webes levelezésébe e-mailben kapott linken lép be, sikeres ember nem lehet ;-) Itt is elég **a hamis oldalaknak tartalmazni a google.com karaktersorozatot**, máris meg van az 5% palimadár.

Szerencsére ennek a mostani levélnek a kínai írásjelek miatt magyar áldozatszedésre körülbelül akkora az esélye, ~~mint Szálasinak a főtárgyaláson~~ mintha a fizetős SMS IQ mérős magyar nyelvű spamet tolnánk ki nekik Tajvanra ;-)

Van egy régi, de igen hasznos szolgáltatás a Gmail webes belépésnél, **a lap legalján mindig ellenőrizhetjük, utóljára mikor és milyen IP címmel léptek be a postafiókunkba**. Érdemes is időnként megtenni, ez talán segíthet idejében észrevenni, ha baj van, emellett mostantól soha ne kattintsunk semmire, az egeret pedig dobjuk is ki kukába ;-)

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek

- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1483979

Kommentek:

Nincsenek hozzászólások.

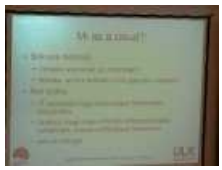
A Linux és a Windows világa

2009.11.02. 18:40 | Csizmazia István [Rambo] | 3 komment

Címkék: windows linux open konferencia 2009 7 source fsf gameshow

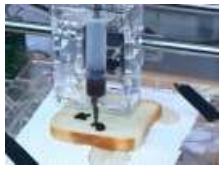
Nem flamewar indul, az összehasonlítás ezúttal pedig **kizárólag azon az alapon történt, hogy egyazon napon zajlott egyszerre két különféle rendezvény a fővárosban**.

Az **FSF alapítvány rendezésében a Szabadszoftver Konferencia a BME Informatika épületében**, míg a **Windows7 bemutatóval egybekötött GameShow pedig a Papp László sportarénában**. Mindkét helyen jártunk, mindkét helyen ingyen lehetett bejutni, más a közönsége a rendezvényeknek, és **a külcsín illetve a belbecs is fényévekre volt egymástól**.



Az FSF rendezvénye reggel kezdődött, és a három teremben párhuzamosan zajló előadások mellett az előtérben kiállítási standokat találhattunk, valamint **az egyes témákra kíváncsi érdeklődők workshopokon beszélgethettek még tovább az előadókkal egy külön teremben**. Volt itt szó felhőkről - ebben az Ubuntu is elöl jár a maga Ubuntu One lehetőségével, Androidról, Open Office fejlesztésről, SyslogNG rendszerről, a Launchpadról és még számos oktatással, virtualizációval foglalkozó kérdésről.

A több száz érdeklődő ezenkívül a folyosói standokon is ismerkedhetett, kérdezősködhettett. Szintén **a teljesség igénye nélkül a BSD-sek, az Ubuntusok, a Fedora, a FLOSSZine, az ULX, Balabit, Andrews, Mozilla, HSPBP** képviseltették itt magukat.



A Hackerspace asztalnál további érdekesség volt, hogy egy 3D nyomtatót is lehetett látni, amely ez alkalommal kenyérszeletekre nyomtatott nutellából hacker logót.

Az ebédszünet utáni részben egy kicsit átszaladtunk a sportarénába, így aztán teljes kontrasztban lehetett részünk a **másik eseménnyel, a GameShow 2009-el**. Itt a téma is más volt: **játékok, konzolok, kiegészítők, karácsony előtti vásárlás és a Windows 7-es ünneplése.**

Hostess girlök, Miss Cyberspace szépségverseny, a belépő karszalaggal autósorsolás, óriás kivetítő óriás színpaddal, és többezres közönséggel.

A forgatagban láthattunk mindenfajta játékkiegészítőt, Windows7 bemutatót, a másik kivetítőn Ozzy Osbourne animált alakja tűnt fel egy röpke pillanatra valamilyen szerepben, voltak moddolt PC házak.

Emellett az ESET jóvoltából azt is megnézhettük, mi a különség egy védelem nélküli és egy vírusvédelemmel futó Windows PC között ;-)

Mivel nem sikerült megnyerni a fekete Toyota autót, és gyorsan sikerült kibeszélgetnünk magunk a jelenlevő pár ismerőssel, kollégával, visszatértünk hát a BME-be. **Az otthonautomatizálás Linux alapokon előadás végét még sikerült elcsípni**, majd Erdei Csaba (Szörpi) zárszava következett, illetve **az FSF-nek felajánlott adó 1%-okból befolyt 4.2 millió forintra kiírt pályázat eredményhirdetése következett**. Nem kellett azonban még hazamenni mindenkinek, aki akart, csatlakozhatott az Ubuntu fanatikusok által szervezett 9.10 (Karmic Koala) megjelenése alkalmából Release Partyhoz.

Egy kicsit **méltatlanul elhanyagoltnak éreztük az FSF rendezvényt, nagyobb hírverésre, több látogatóra, több számítástechnikai magazin, portál részvételére számítottunk**. Az IT Cafe itt is igyekezett segíteni, és élőben közvetítette a honlapján az előadásokat. Nem könnyű kenyér nyíltforráskódú programok népszerűsítése egy ekkora hatalmas multi árnyékában, és a milliárdos szerződések megváltoztatására talán több raklapnyi tojás is kevés lenne nálunk. Az érvelés mellette sokaknak furcsa, akik benne élnek, azoknak pedig sokszor nehéz és érthetetlen akadályokkal teli (pl. pályázat "Windows szerű" szoftverre) szélmalomharcot ígér. **A nálunk sokkal gazdagabb országok ennek ellenére érdekes módon (Francia csendőrség, München örkormányzat, stb.) felismerik, és fontolgatnak ilyen váltásokat**, amikre az egyik sarkalló erő éppen a válság lehet. Mindenesetre itt senki nem érkezett limuzinnal, és **a parkolóban sem láttuk az FSF-001 rendszámú Mercedes terepjárót**. Ennek ellenére kellemes régi és új ismerősökkel sikerült jól elbeszélgetni, elemezni, terveket szőni, és reménykedni, hogy az szabad szoftver és a nyílt forráskód egyszer majd jobban megerősödhet nálunk is.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1492716

Kommentek:

□argnatt 2009.11.03. 19:3□:43

Azér' a hostess csajokról lőhettetek volna egy pár képet, ha már ott voltatok ;-)

Amúgy GameShowra azért nem mentem, mert már hányingerem van a Win7 állandó ajnározásától, komolyan úgy hypeolják a médiában, mintha maga a Messiás érkezett volna meg...

Az FSF-re meg azért nem, mert valószínűleg az előadások 3/4-e alatt nem értettem volna, hogy miről van szó. Meg a regisztráció is plusz macera, még ha nem is túl nagy.

Egy átlagember szerintem soha nem fog elmenni egy olyan konfra, ahová előre regisztrálni kell, és a legtöbb előadásnak már a címét se tudja hová tenni, így persze, hogy nem terjed az ige. Oké, hogy ez részben szakmai konferencia, meg inkább a minőség a fontos, de talán a kicsit kevésbé kockáknak is lehetne valami érdekességet nyújtani, már amennyiben az open source népszerűsítése is a célok között van.

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2009.11.03. 19:44:□3

@:Vargnatt

Szia!

Itt van a te linked :-)
gamestar.hu/budapest-game-show-2009-tuleltuk.html

□ □rgnatt 2009.11.03. 20:2□:□ □

@Csizmazia István [Rambo]: Áá, köszi szépen, leköteleztél :) Volt néhány szemrevaló teremtés, úgy látom...

Dont Steal Our Software

2009.11.03. 18:05 | Csizmazia István [Rambo] | 1 komment

Címkék: kína lopás hamisítás iobit malwarebytes szignatura

Aki idegen tollakkal ékeskedik, az vagy táncosnő az Operettben, vagy hamarabb utólérik, mint a sánta kutyát - mondaná Fülig Jimmy. A nagy kérdésünk az, mi van olyankor, ha egy antivírus cég lop egy másiktól és azt sikerül is bebizonyítani? **Ez egy ilyen bizalomra épülő komoly iparágban (is) megengedhetetlen.**

Réges-régen, mikor a hülyét még pontos j-vel írták, **megjelentek az első DOS alatti antivírus programok. A vírusok akkoriban még 1-2 havonta jelentek meg, a vírusadatbázis floppyn** és BBS-en terjedt, és jópár program ekkor még nyílt, sima TXT formátumban tárolta a vírusismereti szignatúrákat. **Néhány százas darabszámnál ez még nem okozott memóriafoglalási problémákat**, sőt néhány termékbe - pl. HTScan - még a felhasználó saját maga is tudott tételeket felvenni az adatbázisba. Ehhez elég volt tudni a detektálandó minta offsetjét, és annak leírását egy sima hexa vagy jokerekkel átszőtt változata követte. Haladó opcióként megadható volt, hogy a program keressen-e mintát a memóriában is, illetve minden állomány típust vizsgáljon-e, vagy csak adott EXE, COM, whatever típust. Az 1990-ben kiadott Víruslélektan című könyvekben pedig víruszignatúrák is szerepeltek kinyomtatva a mellékletben.

Aztán **egyre jobban kereskedemi termékek lettek az AV programok**, voltak amelyek megszűntek, és kialakult egy mezőny, amely nevet szerzett magának. A **vírusok, férgek változatai egyre gyakrabban jelentek meg, gyarapodott a már heti vagy napi frissítésű adatbázis, és igényelt egy hatékony tömörítést, valamint egy megfelelő kódolást**. Ennek a kódolásnak **kettős célja volt**. Egyfelől a víruslaborok rengeteg munkáját igyekezett megóvni attól, hogy **egy új versenytárs ezt nehogy könnyedén elolvashassa**, feldolgozhassa, munka nélkül a saját termékébe adaptálhassa. Másrészt - és ez is fontos - **a felismerésre vonatkozó részleteket mindenki szerette volna megóvni a vírusíróktól is**, hiszen ezek ismeretében sokkal könnyebben tudnának a védelmet megkerülő kártevőt készíteni. (Most is próbálkoznak persze, de ebben állandó AV mezőnyös tesztelésre vannak utalva.)

Egy éber olvasónk hívta fel a figyelmünket az IT Cafe fórumában szereplő hírre, miszerint **az IOBit egyszerűen ellopta egy konkurens termék adatbázisát**. Az igazság pillanata akkor következett el, amikor a Malwarebytes (a szenvedő fél) furmányos trükkhöz folyamodott, és egy nem létező kártevő szignatúráját is beillesztette saját soronkövetkező adatbázisába. Természetesen **ez is ellopásra került, és amint a képek bizonyítják**, ennél szemléletesebben nem is lehet valakire ráhúzni a vizeslepedőt. Úgy tűnik, a hamis antivírusok, a feltört és meghamisított neves gyártók termékei után újabb módszerek bukkannak fel.

A dolog tehát lelepleződött, és az őszinte beismerés helyett az IOBit saját fórumában tagadták, de állítólag a dolog iránt érdeklődők egy részének kitiltása követte. Úgy véljük, leszűrhetjük azt a tanulágot, hogy a "mindegy hogy jót vagy rosszat, csak beszéljenek rólunk" kezdetű **reklámszabály ez esetben biztosan nem alkalmazható**.

A trükkös végkifejlet egyébként arra hasonlít, mikor a városban járva-kelve **olyan WiFi hálózatba botlik az ember, aminek a neve**

nyilván nem véletlenül: "Na ezt neked, vége az ingyen netednek te tetű!" :-D

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Utaljunk pénzt a S.O.C.A.-nak
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1495106

Kommentek:

Yann Le Pentrec · http://lnk.bz/t7c 2009.11.05. 21:24:04

Cseles... :)

Nem gyengül a Conficker féreg

2009.11.05. 19:50 | Csizmazia István [Rambo] | 2 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

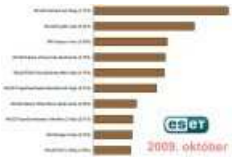
A Conficker férget még korai lenne leírni, hiszen a magyarországi észlelések alapján ismét listavezető lett. Másfelől továbbra is azt láthatjuk, hogy az elmúlt hónapban is sokféle egyéb trójai és kéretlen reklám program keserítette meg a számítógépet használók életét.

Az ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját, melynek elemzése mindig tanulsággal szolgálhat a felhasználók számára. A toplistán minimális változások történtek az élmezőnyben az előző hónaphoz képest. A legfontosabb, hogy **visszavette az első helyet a Conficker, amelyet júniusban és júliusban birtokolt**. A Conficker egy olyan hálózati féreg, amely a Microsoft Windows egyik biztonsági hibáját kihasználó exploit kóddal terjed, gyenge admin jelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül is terjed a fertőzés. Bár az RPC (Remote Procedure Call) vagyis a távoli eljáráshívással kapcsolatos sebezhetőséghez már 2008. októberben kiadták az MS08-67 jelű Microsoft biztonsági javítócsomagot, amely elhárítja a hiba kihasználhatóságát, ennek ellenére sok Windows alapú számítógépen nem fordítanak elég figyelmet a naprakész vírusvédelem mellett az operációs rendszerre is. Emellett a nagy számú fertőzésnek az is az oka lehet, hogy **folyamatosan számtalan új variáns, módosított változat jelenik meg**, melyeknél a készítők rendre igyekeznek tesztelni és kijátszani a felismerést.

Az **INF/Autorun stabil harmadik helye** azt jelzi, hogy még mindig sok Windows felhasználónál okoz problémát a hordozható külső eszközök csatlakoztatásával terjedő vírus. A naprakész vírusvédelem mellett a szakértők folyamatosan hangsúlyozzák, hogy **célszerű az összes külső meghajtó automatikus futtatásának letiltása**.

Hetedik lett a listán a múlt hónapban debütáló Win32/Adware.WhenUSave alkalmazás. Ez futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kéretlen reklámokat, valamint saját program frissítésit tölti le. **A fertőzött gépen aktív böngésző esetén linkeket, időjárás jelentést és más kéretlen tartalmakat, reklámokat jelenít meg**.

A nyolcadik helyen pedig új versenyzőt üdvözölhetünk, **a Win32/TrojanDownloader.Fakealert.Z trójai hamis riasztásokkal igyekszik felhívni magára a figyelmet**. A megfelelő védelem nélküli gépen szándékosan vírust jelez, illetve további állományokat kísérel meg letölteni. A Rendszerleíró-adatbázisban (Registry) számos, többek közt az Internet Explorer működésével kapcsolatos beállítást felülír. Végső célja, hogy a felhasználó megtévesztésével egy bizonyos összegért megvetesse az álvírusirtó „igazi”, állítólag mentesíteni is képes példányát.



Végezetül következzen a magyarországi toplista. Az ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2009 októberében az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. **Ezek együttesen 35.55%-ot tudtak** a teljes tortából kihasítani maguknak.

1. Win32/Conficker.AA féreg
Elterjedtsége az októberi fertőzések között: 7.15%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd

távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.

A számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: http://www.eset.hu/virus/conficker-aa

2. Win32/Kryptik trójai
Elterjedtsége az októberi fertőzések között: 5.34%

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm, illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.
Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/kryptik-gt

3. INF/Autorun vírus
Elterjedtsége az októberi fertőzések között: 3.89%

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

A számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon) terjed.
Bővebb információ: http://www.eset.hu/virus/autorun

4. Win32/Adware.Virtumonde alkalmazás
Elterjedtsége az októberi fertőzések között: 3.79%

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-virtumonde

5. Win32/PSW.OnLineGames.NNU trójai
Elterjedtsége az októberi fertőzések között: 3.74%

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/psw-onlinegames-nnu

6. Win32/TrojanDownloader.Bredolab.AA trójai
Elterjedtsége az októberi fertőzések között: 3.33%

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, melynek segítségével a távoli oldalakról letöltődnek és végrehajtódnak ezek a kódok. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is a bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-bredolab-aa

7. Win32/Adware.WhenUSave alkalmazás
Elterjedtsége az októberi fertőzések között: 2.26%

Működés: A Win32/Adware.WhenUSave működése során létrehozza a saveupdate.exe nevű állományt. Az ilyen nem kifejezett kártevő, hanem inkább a veszélyes vagy nem kívánt programok kategóriába tartozó kéretlen reklám programok sok esetben élnek olyan trükkökkel, hogy különféle további könyvtárakban is létrehoznak magukból másolatot. Ennek kettős célja van: egyrészt egy esetleges vírusirtást követően egy eldugott helyen megmaradhatnak a fertőzött állományok, másrészt helyi hálózatokban, megosztott könyvtárakban, peer-to-peer hálózatokban is képesek terjedni. Futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kéretlen reklámokat valamint saját program frissítésit tölti le. A fertőzött gépen aktív böngésző esetén linkeket, időjárás jelentést és más kéretlen reklámokat jelenít meg.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/adware-whenusave

8. Win32/TrojanDownloader.Fakealert.Z trójai
Elterjedtsége az októberi fertőzések között: 2.07%

Működés: A Win32/TrojanDownloader.Fakealert.Z trójai hamis riasztásokkal igyekszik felhívni magára a figyelmet. A megfelelő védelem nélküli gépen szándékosan vírust jelez, majd további állományokat kísérel meg letölteni. A Rendszerleíró-adatbázisban (Registry) számos, többek közt az Internet Explorer működésével kapcsolatos beállítást felülír. Végső célja, hogy egy bizonyos összegért megvetesse az

álvírusirtó „igazi”, állítólag irtani is képes példányát.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://www.eset.hu/virus/trojandownloader-fakealert-z

9. Win32/Agent trójai
Elterjedtsége az októberi fertőzések között: 2.03%

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://www.eset.hu/virus/agent

10. Win32/VB.EL féreg
Elterjedtsége az októberi fertőzések között: 1.95%

Működés: A VB.EL (vagy más néven VBWorm, SillyFDC) féreg hordozható adattárolókon és hálózati meghajtókon képes terjedni. Fertőzés esetén megkísérel további káros kódokat letölteni a 123a321a.com oldalról. Automatikus lefuttatásához módosítja a Windows Registry HKLM,SOFTWARE\Microsoft\Windows\CurrentVersion\Run bejegyzését is.

Árulkodó jel lehet a sal.xls.exe állomány megjelenése a C: és minden további hálózati meghajtó főkönyvtárában .

A számítógépre kerülés módja: Fertőzött adattároló (USB kulcs, külső merevlemez, stb.) csatlakoztatásával terjed.
Bővebb információ: http://www.eset.hu/virus/vb-el

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1502173

Kommentek:

Tomi1977 2009.12.01. 14:06:34

Szia Rambo!

Hallottam, hogy a Confiker ellen is csak akkor véd a vírusirtó, ha fel vannak telepítve a patch-ek. Ez is érdekelne, de az is, hogy milyen következménye van, ha szimplán csak vírusirtót használok, Windows Update-t nem. Ugyanis hallottam már mellette és ellene is érveket.
Válaszodat előre is köszönöm!

Tamás

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.03. 09:50:10

Szia Tomi1977!

Én is csak mellette tudok érvelni.

Ha olyan Conficker jön, amit a vírusadatbázis vagy a heurisztika felismer, akkor ugye semmi gond. A baj inkább akkor van, ha valami új változat érkezik (nagyon sok Conficker variáns van és készül) és olyan módosított kódja van, amit még az antivírus éppen nem ismer fel abban a pillanatban, amikor a gépedbe belegyalogol.

Ha viszont a kihasználható sebezhetőségek (exploit) útját bezárod (Windows, Office, egyéb alkalmazások naprakész update), akkor 99%-ban bezárod az ajtót a vadi új kártevő kódok előtt is.

Én játszom, te fájlokat törölsz

2009.11.06. 12:15 | Csizmazia István [Rambo] | 4 komment

Címkék: macintosh osx lose trójai symantec

Nem ez a pontos címe **a Macintoshra készült játéknak, hanem Lose/Lose,** de ha távirati stílusban fogalmazhatnánk a lényeget, körülbelül ilyesmi lehetne: "A JATAEK ELINDIITAASA UTAAN FAAJLOKAT TOEROEL A MEREVLEMEZROEL STOP A TOEROELT FAAJLT VEELETLENSZERUEEN VAALASZTJA KI STOP MOST TISZTA IDEG VAGYOK, EGY DARABIG SENKI NE SZOOLJON HOZZAAM STOP".

A játékot **szokatlan működése (űrhajó találatonként egy fájl delete) miatt a Symantec feketelistára vette, és trójaként detektálja** azt OSX.Loosemaque néven. A fejlesztők persze tiltakoznak, szerintük túlzás kártevőnek minősíteni a "játékot". A dolog viszont jól mutatja, **mennyire hasznos a szürke zóna "Kéretlen alkalmazások", "Veszélyes alkalmazások" és hasonló kategóriák bevezetése** az antivírus cégek részéről.

Bár a "játék" a fájl törléseket előre leírja a dokumentációjában, ennek ellenére biztosan nem mindenki olvassa azt végig figyelmesen, bogarássza ki ennyire aprólékosan.

Annak idején a Sircam csinált hasonlóan "kellemes", Szarvasvadász hangulatú orosz rulettet, amikor **egy véletlenszerűen kiválasztott dokumentumot küldött tovább e-mailben valaki ismeretlennek a fertőzött számítógépről**. És ez lehetett bármi, fizetési cetli, bizalmas levél, de persze egy hello world is - Szerencse kisasszony kegyei szerint.

Mi azért úgy látjuk, annyi minden baj, és kár érheti az embert normál viszonyok között amúgyis, **minek ezeket feleslegesen, mesterséges móresre tanításokkal pluszban megfejelni,** de döntse ezt el kiki maga vérmérséklete szerint.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1504222

Kommentek:

Yann Le Pentrec · http://lnk.bz/t7c 2009.11.06. 12:05:49

És akkor ugye a Mac userek fényezik magukat folyton azzal, hogy az ő 'óperenciás' rendszerükre nem készül vírus meg kártevő. Mint látjuk, igen. Minél többen használnak valamit, annál nagyobb a táptalaj és persze a káros programokat írók száma is.

Nyaligátor · http://autostat.hu/technikai-szotar 2009.11.06. 15:30:18

@Yann Le Pentrec:
A gáz az, hogy FOLYTON ezzel jönnek. Tény, kevesebb van, de hogy előbb utóbb megtalálják őket is, attól függően, hogy terjed.

Yann Le Pentrec · http://lnk.bz/t7c 2009.11.10. 11:17:46

Egyre több van belőlük világszerte is immár, mondhatni elég népszerű platform a Mac/OS X. (Úgy értem, régebben, a 68k/PPC érában eléggé USA-specifikus volt a Mac "phenomenon") És ez pont elég ahhoz, hogy egyre többen leljék meg és használják ki a gyenge pontokat...

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.11.10. 11:55:24

Igazából azt sem értem, az Index miért ma teszi ki a címlapra az apple.blogos hírt, mikor én már megírtam 4 napja :-O

A gyenge pont pedig mindig a juzer! PEBKAC :-)

A lustaság nem vírus

2009.11.09. 11:31 | Csizmazia István [Rambo] | 3 komment

Címkék: jelszó iphone ssh démon féreg alpértelmezett

Kedves gyerekek! Remélem ágyban vagytok már, Rémusz bácsi ma a szegény jailbreakelt iPhone telefonokat megtámadó csúnya gonosz vírusokról fog mesélni nektek ;-)

Egy ausztrál [cr/h]acker? visszaélve **a jailbreakelt telefonokat használók tudatlanságával és/vagy lustaságával, az alapértelmezett SSH jelszót felhasználva** írt egy C nyelvű férget, amely távolról belépett mások telefonjába, lezárja az SSH portot és felmásolt néhány állományt, többek közt **lecserélte az iPhone háttérképet Rick Astley-re a tulajdonosoknál**.

Kíváncsi volt, vajon hány ilyen sebezhető készüléket talál, és állítólag száz fölötti darabszámra lelt így rá. A 21 esztendős Ashley Towns **úgy gondolta, csak egy ártalmatlan tréfa, amit tesz**. Mondjuk **úgy tűnik, valóban nem akart kárt okozni**, és a feltűnően lecserélt háttérkép is ez látszik igazolni.

Csak azok a feltört telefonok vannak ilyen veszélyben, amiken fut ez az említett SSH démon. Buhera blogjában a korábbi hasonló holland iPhone-os próbálkozásokról, valamint a védekezésről is lehet olvasni, ami nem más, mint egyedi SSH jelszó beállítása.

Sokan próbálnak különböző okok miatt a korlátozásoktól megszabadulni (függetlenítés=bármely telefonszolgáltatónál lehet használni a készüléket; jailbreak=tetszőleges, ingyenes, vagy feltört programok telepítési lehetősége a különben egyedüli fizetős iTunes helyett) és az ilyen esetek nyilván média értékűek az Applenek, hogy lám-lám, így jár aki nem az egyenes útat választja. Mindemellett **a korlátozások rendkívül zavaróak tudnak lenni, csak egyetlen szolgáltatóhoz való kötöttség vagy 2009-ben egy flash nélküli webböngészés (gátolva az ingyenes játékokat, hogy inkább mindenki pénzért vásároljon az iTunes áruházban) roppant kolonc és idióta megoldás**.

A szabadságra vágyóknak - és akik nem kívánnak feltört eszközöket, programokat használni - talán egy **Nokia N900-as Maemo Linuxos okostelefon lesz majd a hosszútávú jó megoldás**, ahol lesz ugyan Ovi Store, de emellett **mi magunk is szabadon telepítgethetünk kedvünk szerint dolgokat**.

Mivel viszont az Ikex C programja nyilvánosságra került, sajnos hamarosan várhatjuk az első PoC kód után a már kevésbé barátságos, sötétebb payloados verziókat is.

Ajánlott bejegyzések:

- Az XP élt, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1510796

Kommentek:

bolhabetu 2009.11.09. 18:54:38

Az alábbi videóban még többet tudhatunk meg erről a biztonsági problémáról:

www.youtube.com/watch?v=Yu_moia-oVI

:):):):):):):):):):) (Én szóltam)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.10. 09:46:55

Nekem pedig ez a videó a kedvencem, a részletes magyarázattal:

www.youtube.com/watch?v=eqQRN5OWgBw

:-)))

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.10. 09:49:29

Az alapértelmezett jelszó NEM_JELSZÓ, lásd a defaultpasswords.com weboldalt.

Volt régen a Friderikusznak egy hasonló esete, mikor még TV elnök akart lenni, de a gyári default, alapértelmezett jelszó volt beállítva a Pannonos postafiókjában, nem változtatta meg. Mikor Lendvai Ildikó aztán üzent neki, hogy hajrá-előre, akkor ismeretlenek ezt megneszelték, és simán lehallgatták a csak neki szóló üzenetet a 1111-es jelszóval, majd később mp3-ban felteték a netre.

Írjon neked a finn rendőrség!

2009.11.10. 16:52 | Csizmazia István [Rambo] | 3 komment

Címkék: finn adatok csalás iroda nyomozó adathalászat banki

Ez nem egy szilveszteri jókívánság része, mindössze egy jó példa, hogy nem csak angolul lehet nívós adathalász levelet fogalmazni, hanem **tökéletes helyesírással akár finnül is**.

Nem csak az egy főre eső GDP, a szociális juttatások magas színvonala, de az internet biztonságossága is kiemelkedő Finnországban. Mindemellett **próbálkozások mindenütt vannak, sőt lesznek**, így került a felszínre most ez a látszólag **a Finn nyomozó irodától (National Bureau of Investigation, NBI) érkezett e-mail** is.

Az üzenetben a csalók nagy cselesen azt állítják a szervezet nevében, hogy gyorsan adjunk meg adatainkat, mert **visszaélés történt a bankártyánkkal, és éppen a letiltáshoz szükségesek ezek az információk**. Bár számos pénzintézet, és szervezet szendvedett már el hasonlót, **Finnországban állítólag ez az első eset, hogy a helyi rendőrség nevében adathalász** akció történik.

Valószínűleg, arra a kérésre, hogy adjuk meg bankkártyánkhoz tartozó adatainkat, mindenkinek beugrott, hogy **se a bank, se a rendőrség nem kér soha ilyet e-mailben**. Túl a jó finn GDP-n, és egyéb előnyös pozícióikon, remélhetőleg egy olyan országban, ahol többek közt Hypponen bácsi tolja a blogjában a napi biztonsági jótanácsokat, **talán még a szokásos átlagos 5 százalék sem akad ott horogra**.

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1515112

Kommentek:

gothmog 2009.11.10. 19:26:23

ma olyan subjectel kaptam egyet, hogy "your drunk photos published". :)

ipas 2009.11.11. 06:52:02

@gothmog: Ehhez nem kell nagy ész, az egyik ott van a hozzászólásod mellett is. ;)

gothmog 2009.11.13. 17:1□:00

@Pipas: Igaz, igaz.
:)))

Trójai játékok nem csak Akhilleusznak

2009.11.11. 19:55 | Csizmazia István [Rambo] | 6 komment

Címkék: apple játék iphone telefonszám csaló storm8

Sokszor foglalkoztunk már az alternatív operációs rendszerek kapcsán, hogy a Windowshoz képest mennyivel biztonságosabbak. **PEBKAC ellen viszont nincs orvosság**, és úgy tűnik, **nem világos mindenkinek, hogy egy szoftverforgalmazó** felelőssége milyen óriási ebben a bizalomra épülő rendszerben. Nekünk pedig **nagyon nem mindegy, milyen alkalmazásokat** töltünk le és telepítünk például az iPhonera.

Mienk a trójai, magunknak telepítjük - akár így is lehetne fogalmazni, esetleg azt kérdezi tőlünk a medve, hogy **mondd csak te vadász, miért is jársz az iTunes App Store-ba?** Ez az a terület, ahol még a leggyanakvóbb ember is csapdába eshet. **Nem látunk bele a letöltendő programba, így az open source-szal szemben itt jobb híján kénytelenek vagyunk benne megbízni**. Esetleg valamennyire tájékozódhatunk az interneten, de ez is maximum akkor óvhat meg bármitől, ha már egy ideje ismert valamilyen anomália, vagyis jobbára már csak eső után van esélyünk köpönyeget találni.

Most az Egyesült Államokban, Észak Karolinában indult per a Storm8 fejlesztők ellen, mert az ingyenesen letölthető játékaik - mint például a iMobsters vagy a Vampires Live - **egy beépített hátsóajtón titokban továbbították a fejlesztőknek a felhasználó telefonszámát**, illetve telefonkönyvében szereplő számokat, hogy ösztönözhessék őket a teljes változat megvásárlására.

A piszkos trükk kiderült, és most **a fejlesztők azzal védekeznek, hogy ez "véletlen programhiba volt"** :-O Az alábbi programok keveredtek gyanúba: iMobsters, Kingdoms Live, Racing Live, Rockstars Live, Vampires Live, World War, Zombies Live - lehet ellenőrizni a telefonokat. Valószínűleg **az App Store alkalmassági vizsgálat sokkal jobban odafigyel arra, hogy nehogy üzletileg csorbuljon az Apple érdeke**, és csak kevésbé alaposan ellenőrzi a biztonsági hogyant, a miértet és az egyáltalánt.

Esetleg **a Storm8 fejlesztők védekezhetnek azzal**, csak az Apple céges policyt másolták és akarták a magukéva tenni ;-) Az a legszomorúbb, hogy ebbe **a csapdába bármely felhasználó belesétálhatott**...

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1517872

Kommentek:

Sonka Nery 2009.11.11. 21:33:39

Ezt a "telefonon játszani"-dolgot sose értettem.

Watt25 · http://sablonvalasz.blogspot.hu 2009.11.11. 22:28:10

Miért olyan bonyolut megérteni, hogy nem mindenkinek van autója és mondjuk tömegközelekedés közben ideális?

phaidros 2009.11.12. 00:15:40

@Watt25: hádde apró ahho'. Meg meglöknek amikor a sört öntöm a sörös játékkal, oszt kifolyik. :)

há zé · http://indafoto.hu/hhzz 2009.11.12. 06:40:12

"Nem látunk bele a letöltendő programba,"
Miért? Hány olyan játék van, aminek belelátsz a kódjába? És ha belelátsz, mit érsz vele? Te már végignézted a gépedre telepített linuxos szoftverek forráskódját? Alaposan?

espadazo - Játékbolt: · http://aruhaz.nettfilm.hu 2009.11.12. 08:56:00

Telefonon legyen ébresztő, meg legyen akkora, hogy rá lehessen gumizni a Sokol-t, hogy ne unatkozzak a buszon!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.12. 09:00:05

Hali há zé! Üdv a blogon :-)

A különbség a lehetőség, hogy ha akarsz, akár bele is nézhetsz a forrásba, Illetve ha ilyen open source dolog fenn áll, akkor az esélyeid akkor is javulhatnak, ha te magad éppen nem érsz rá, vagy nem értesz hozzá. Valahol a világon valaki ezt (helyetted) kíváncsiságbóléppen megnézi, már megnézte, és ellenőrizte, jajgat, farkast kiált, ha kell, stb.

Abban viszont teljesen igazad van abban, hogy a játékok között ez egyáltalán nem jellemző. Viszont ahogy az új Symbiannal függvényekre lebontva alaposan ellenőrizték az új külsős progrikat, na meg később digitálisan aláírták a csomagokat, ez azért

valahol nagyon hasznos volt.

Adataink védelme péntek 13-án és máskor

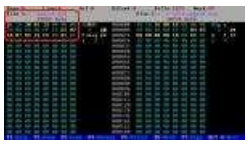
2009.11.13. 15:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: dvd adat péntek év 13 mentés 1000 jerusalem rendszeres cranberry

Azokon kívül, akik 32 milliót keresnek vele hetente, valószínűleg senkinek nem kedvence a vírus, a féreg, **a számítógépes kártevő és az ezzel járó esetleges adatvesztés**. A **saját adataink külső hordozóra történő rendszeres mentése évtizedek óta fontos** kiegészítése kellene, hogy legyen a számítógépes biztonságunknak.

Péntek 13-a lévén természetesen eszünkbe juthatnak olyan régi események, amikor a péntek 13-a vírus miatt bemondták a Déli Krónikában, hogy akinek nem okvetlenül szükséges, az aznap ne kapcsolja be a számítógépét. Azóta persze sokat változott a világ - ma már egy bankban, kórházban, hadseregben, tőzsdén, reptéren, stb. **nem is lehetne ezt az esetleges kikapcsolgatást véghezvinni**. Így is marad még 364 nap, így a régmúlttal maximum talán annyi kapocs maradt, hogy ahogy akkor is, úgy most is kiemelt fontosságú volt a **saját adat, munka mentése, illetve ennek sajnálatos elmaradása**.

A mentés **elkészítésének a legmegfelelőbb ideje az a pillanat, amikor még egyáltalán nincs rá szükség :-)** Emellett egy másik fontos jellemzője is van: **csak a kipróbált, letesztelt mentés ér egyáltalán valamit**. Sokan mentegetnek stochasztikusan egyes dolgokat USB kulcsra, rendszertelenül egyéb helyekre, amikor aztán valami miatt beüt a mennykő és **a "start from scratch" ideje eljön, azonnal ötlik fel a rengeteg dolog, mi is hiányzik még**: jaj a levelezés, a postafiókok beállítási módja, a licenckulcsok, kedvenc programjaink részletes beállításai, a böngésző testreszabott állapota, benne a könyvjelzőkkel és pluginekkel, bejáratott tűzfalszabályok, csevegő programok elmentett naplói, FTP oldalaink jelszavai, digitális aláírásunk publikus és privát kulcsa, a jól belőtt PDF fájlba nyomtatási lehetőség, és **még hosszan lehetne sorolni**.



Talán még az is **előfordulhat valakivel, hogy évekkel korábbi hagyományos CD/DVD mentését elővéve váratlanul hibásnak vagy üresnek látszik a lemez, nyoma sincs a biztonságban hitt adatoknak**. Lehet persze ezt cizellálni, és az eleve maximum 2-5 évet bíró lemezeket minden évben **egyszer egy rendszeres átírással, amikor minden egyes mentés lemezt lemásolunk egy másik üres adathordozóra, a régit pedig megsemmisítjük.** Így minden írásnak csupán egyetlen esztendőt kellene tudni kibírnia, ami talán megy neki, ha nem noname.

Talán ezen segíthet majd egy új fajta DVD írás, amely szerényen ezer évet garantál a problémamentes visszaolvasásra. Ez persze így előre vicces, majd 30-40 éve múlva térjünk vissza rá. Maga **az írási folyamat nem is a felhasználóknál történik, hanem a cég végzi el azt** - itt ugye már van is egy momentum: meg kell bíznunk bennük, átadni az adatokat, hogy ők írják meg. **Illetve titkosított formában is küldhetjük**.

A módszer egy dolgot azonban biztosan nem tud, a saját lustaság legyőzésén még ez sem segít. Nem ismerhetjük, milyen jövő áll a Cranberry DiamonDisc előtt, mindenesetre **kíváncsian várjuk** a konkrét árakat és az idő múlásával pedig az ígéret betartását. Lehet jönni kommentelni 3009. november 13-án az esti órákban :-D

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Majdnem mindenki átverhető adathalászattal
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1522019

Kommentek:

Nincsenek hozzászólások.

Már krómozott az OTP adathalászok horgászbotja

2009.11.16. 14:09 | Csizmazia István [Rambo] | 10 komment

Címkék: kísérlet bank ukrán otp kódolás adathalász windows 1251

De a billentyűzet előtt még mindig a jó öreg Fülig Jimmy ül az ő hamisítatlan helyesírási tudatlanságával, vagyis **még mindig nem elég jó minden egy tökéletes OTP-s csaláshoz**. A trükkös weboldal már szinte megszólalásig hasonló, de **a küldött levélben szereplő cirill betűk eléggé lerontják az összképet**. A korcsolya versenyekről ismert pontozással így 3/10-s táblát tudunk csak a magasba emelni.

Nem panaszkodhat az OTP, hogy Bástya elvtárshoz hasonlóan őket már senki nem akarná "megmerényelni". A számos MKB bankos próbálkozás után ők is kapják már szinte havi rendszerességgel a magukét. Most egy olyan "OTP Bank - Nagyon fontos!!" tárgysorral rendelkező levél jött reggel, melyben furcsa karakterekkel írtak nekünk üzenetet. Veterán blogolvasóknak biztosan rémlik már, hogy látható **cirill betűk oka a levélben szereplő Windows-1251 kódolás**, ami miatt arra is gyanakodhatunk, hogy **vélhetően ukrán, szerb, bolgár vagy macedón csalók írták**.

Már az **ü helyett szereplő "jerü" is annyira viccesen hat**, de a koronát a "Speakeasy Network DSL" teszi fel. Ha ennek ellenére belép valaki az adathalászok oldalára, azt csak sajnálni tudjuk.

"Tisztelt Ügyfelünk!

Ez a hivatalos értesítést arról, hogy a hitelkártyáját korlátozott volt. A közelmúltban felülvizsgálták a kártyát, és úgy tűnik, hogy a vele kapcsolatban álló több mint egy számlák. ***Összekapcsolja a hitelkártya több sokszoros számlák szigorúan tilos, és azt is törvény bünteti****. Ön most már felkértük, hogy nyújtson információkat a hitelkártyáját. Az OTP Bank azonnal kivizsgálja az ügyet, és ha a vizsgálatot az Ön javára fogjuk visszaállítani a fiókját.*

Hogyan állíthatom vissza a számláját?

Kattintson ide, és végezze el a lépéseket, hogy eltávolítsa korlátozásokat.

The OTP Bank Team

(C) copyright 2009 OTP Bank"

A bank adathalászatra figyelmeztető közleményét valamilyen rejtélyes ok folytán már nem másolták le a tükrözéskor

Hát ennyi volt a kísérlet, **jó lesz már most összehegeszteni valami ékezetes karaktercserélgető Perl scriptet, mert lesz még ebből várhatóan sok hasonló**. Érdemes a weboldalak képét, valamint a főoldal forráskódjának különbségeit is megnézegetni. **Sajnos vagy hál Istennek, a weboldal hiába nagyon jó másolat, a kísérő e-mail annyira gagyi de luxe**, hogy komoly zavart semmiképp nem okozhat az Erőben.

További jópofaság, hogy egy ártatlan, más meglévő oldalra, az IKE KLIGERMAN BARKLEY ARCHITECTS P.C. - New York - San Francisco **belsőépítészeti vállalkozásának weboldalába helyezték el a csaló OTP aloldalt**, így a vállalkozó majd nagyot nézhet, ha letiltják a weboldalát, persze miért is nem vigyázott jobban ;-) Annyi mindenesetre látszik, az árnyékos oldalon **a 1251-sek ilyen hűvös őszi időben sem pihennek**.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1528565

Kommentek:

espadazo - Játékbolt: · http://aruhaz.nettfilm.hu 2009.11.16. 17:41:52

Ilyet minden héten kapok, kb. 4-5 "banktól".

Kuku 2009.11.16. 17:47:12

Azért nem nehéz rájönni, hogy ez nem adathalászat. Ha az lenne, nem ilyen lenne. Érdemes megyezni, hogy mindig ilyenek a levelek, pl. a legutóbbi MKB-s is cirill karakteres volt.
Szerintem csak valakik nagyon ügyelnek arra hogy az e pénz ne tűnjön biztonságosnak.

Igazság Atyja 2009.11.16. 17:49:34

"Összekapcsolja a hitelkártya több sokszoros számlák szigorúan tilos, és azt is törvény bünteti."

Ez ütött! De legalább van önirónia, ha így fogalmaznak. Azt IS. (Akárcsak az adathalászatot). :)

lor 2009.11.16. 17:59:23

miert nem masoljak egy az egyben a honlapot?
mindent le lehetne lopni szepen.

at tudjak valahogy irni a cimsorban az url-t?
azaz letezhet, hogy elmegyek egy hamis oldalra de ott egy hamisitott cimsort latok, ami engem megnyugtat es maris irom amit kell.

azert vigyazok email nekem nem szamit.
mondjuk idegen geprol kepernyo billentyuzet van hasznalva, de ha honlapra megyek akkor ott azzal is bukok.

gitáros 2009.11.16. 18:02:09

Lágyjel az, te, nem jerü...

raklap 2009.11.16. 18:02:52

de mér kell elbaszni egy ilyen hülye levélel... amúgy ezek a cuccok nem infosoknak szólnak... szal ki lehet ezt tárgyalni végletekig de hány olyan ember van aki csak kattintgat... és ezek csak próbálkozások apró szárnypróbálgatások...

ez a biznisz már lecsengett mivel szinte minden bank sms jleszót kér 3 ft átmozgatásához is...

jön majd még sok szép dolog a jövőben és mindenki be fogja szopni mint ahogy ezt is ették az elején az emberek...

sok értelme ezeknek a dolgoknak már nincs nem kecsegtet nagy anyagi haszonnal... de egy dolgot tisztán mutat nem éri meg biztonsági hibákat keresni a bankok rendszereiben ... sok meló és a kivitelezhetősége is kérdéses... meg minek mikor a legnagyobb hibaforrás ott van az orrunk előtt a simpla user...

indapasssucks 2009.11.16. 18:05:51

fura, hogy azt hiszitek, hogy a havonta egyszer internetező nagyik nem is emberek, és nem számítanak.
Ahogy a hamis pénzt sem ismeri fel mindenki, és a hamisításnak is vannak szintjei (gondoljunk a németek által hamisított angol élelmiszerjegyre, ami ugye jobb volt mint az eredeti, és csak ezen lehetett lebuktatni), ugye a phisingnek is.

szerintem tűzzel vassal.

de ti tudjátok...

mark renton 2009.11.16. 21:32:47

én mé nem kapok soha ijet?
nekem csak viagrások jönnek :(

Nyaligátor · http://autostat.hu/technikai-szotar 2009.11.17. 14:10:40

Jaja, nekem is jönnek, habár meglepően csak arra a címre, amit az egyetemre regisztráltam...

roli · http://nivo.blog.hu 2009.11.17. 22:01:20

Még egy Antivírus a blogparódián egy veszélyes kártevőről, mely leemeli a pénzt a számláról, s nem tudsz ellene mit tenni:

blogparodia.blog.hu/2009/11/17/antivirus_veszelyes_teli_kartevo

Használt ATM-et tessék!

2009.11.19. 12:30 | Csizmazia István [Rambo] | 3 komment

Címkék: usa csalás atm e bay bárki vehet

A használt merevlemezekkel kapcsolatosan már kitárgyaltuk, a letörölt fájl, a letörölt particiós tábla nem igazi törlés, az eladott eszközt adathelyreállító programokkal zaklatva sokszor meglepő információk bukkanak fel. Emiatt akinek félteni való adata van, inkább azon gondolkozik, hány fokos szögben fúrja át a leselejtezett winchestert még a tűzbedobás előtt ;-) **Vannak tételek, amiket nem szabadna bárkinek áruba bocsátani**, pláne nem fullos dokumentációval.

Egy **amerikai biztonsági tanácsadó nemrég arról számolt be**, hogy egy bostoni bár eladó eszközei között két biliárd asztal és egy világító Budweiser lámpa között **egy ATM pénzkiadó automatát sikerült neki megvennie.** A mellékelt kézikönyv még arra is adott részletes útmutatást, pontosan hogyan történik az érzékeny adatok tárolása. Ha a korábbi tulajdonos nem veszi a fáradtságot az alapos törlésre, **a szakértők számára nyitva az út a korábbi számla- és tranzakciós adatok visszanyerésére**.

A dolog érdekessége, hogy **az USA-ben nincs szabályozva, korlátozva** az ilyen eszközök adás-vétele, illetve hogy ki birtokolhat, üzemeltethet ilyesmit. Mindenesetre **több, mint meglepő, hogy az E-bayen vagy a Craiglisten lehessen licitálni** pénzkiadó automatára. A bűnözők valószínűleg kapva kapnak az ilyen lehetőségeken, hiszen nem csak egy adott eszközből nyerhetnek ki érzékeny adatokat, de **részletesen megismerve annak működését, szofisztikáltabb csalásokat készíthetnek elő**.

De **akár egy nagyforgalmú helyen fel is állíthatják, és működtethetik**, legalábbis az Egyesült Államokban. Saját automata esetén pedig **jóval kisebb a lebukás esélye a beépített második olvasóval, buherált PIN olvasó kamerával**. A riportbeli utca embere jellegzetesen úgy nyilatkozott, az, hogy használna egy neki megmutatott pénzkiadó automatát, egyedül azon múlik, hogy az éppen mennyi pénzkezelési költséget számít fel.

Siciliano onnan kapta a vásárlási ötletet, hogy korábban a DefConon egy ott felállított hamis ATM-et lelepleztek a résztvevők. Megtartja az eszközt és **előadásain ezzel fogja majd szemléltetni, hogy milyen veszélyei vannak az ilyen jellegű szabályozatlanságnak**, mire kellene kötelezni a korábbi ATM tulajdonosokat a pénzautomata áruba bocsátása előtt, szóval jócskán van volna még teendő az alaposabb biztonság terén.

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1536221

Kommentek:

it_guru · http://www.itguru.blog.hu 2009.11.19. 12:51:43

Uhh, ez komoly.
Minden hazai háztartásba egy amerikai ATM-et!

Kaga · http://autostat.hu/markatoertenetek 2009.11.27. 12:49:01

Ha akarsz, lemezáron vehetsz MiG vadászgépet is, Ukrajnában. Ócskavasáron árulják, repképtelenek, de dísznek királyak ...

teddybear01 2009.12.01. 20:10:29

Mi például az érzékenyebb adatokat tartalmazó vinyókat selejtezés előtt átfurkáltuk egy hatos fúróval, úgy, hogy a lemez nehogy egyben maradjon.

Lehet próbálkozni :-)

Saját automata esetén minek második leolvasó? Egyszerűen el kell tárolnia a kártyaadatokat, és időnként "lefejni..."

Új tanfolyamok, ECSA, NCIH

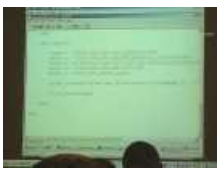
2009.11.20. 08:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: tanfolyam netacademia ecsa chfi forensic

Szerdán a **volt etikus hacker (CEH) hallgatóknak szervezett bemutatót a NetAcademia**. Újabb tanfolyamok kerültek a látótérbe, nincs megállás, láblógatás.

A bemutató előadás keretében megnézhettük, hová lehet továbblépni egy CEH tanfolyam után. Megtudhattuk azt is, többek közt a NATO szakembereit is oktatja a NetAcademia, és ez mindenképpen a remek oktató gárdát, és az erős gyakorlatra kihegyezett módszerüket dícséri.

Fóti Marcell bevezetője után Zsíros Péter következett, aki előadását a kihasználható hibák kereséséről, fuzzerrel való exploit detektálásról és az exploit egyszerű felhasználhatósága okán annak a MetaSploit Frameworkbe való implemántálási lehetőségéről tartotta. Többek közt **ez is a tananyag része lesz majd** az ECSA (EC-Council Certified Security Analyst) tanfolyamnak.



Egy másik előadásban pedig **Barta Csaba révén abba nyerhettünk bepillantást, milyen feladatai vannak egy forensic szakembern** Itt egy bizonyítékként lefoglalt és **látszólag törölt merevlemezről lett visszabűvészkedve számos olyan adat**, amiről egy átlagfelhaszn erős tévhitben azt gondolhatja - hiszen ez üres, már rég letöröltem, "ezt csak NASA tudja visszaállítani" ;-)

A Hacktivityn is elhangzottok alapján egyelőre nincs egységes szemlélet, elvárás, törvényi szabályozás egy számítógépes igazságügyi szakértővel szemben, talán ez a CHFI (Computer Hacking Forensic Investigator) tanfolyam **ezen is segíthet** majd.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1536814

Kommentek:

Nincsenek hozzászólások.

Álmaimban Amerika visszainteget

2009.11.23. 21:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: mac pc amerika felmérés trójai eset adathalász

Az ESET nemrég megbízást adott a Competitive Edge Research and Communications nevű cégnek, hogy ugyanmár **végeznének el egy felmérést az amerikai internetezők körében a biztonságot, az elektronikus bűnözés helyzetét illetően**. Az egyik nagy meglepetés az volt, hogy az átlag amerikaiak **mennyire nincsenek tisztában azzal, hogy a számítógépes csalásokat a szervezett bűnözés irányítja**.

Mint azt Randy Abrams blogjában olvashatjuk, az amerikai számítógép **felhasználók 5□százaléka gondolja úgy, hogy Macintoshnál egyáltalán nincs szüksége vírusvédelmi programra**, és biztonságban van enélkül is, míg a PC - értsd Windows - esetén ugyanez 27 százalék. Pedig a Maces gépek egyre inkább áldozatul esnek a számítógépes csalásoknak, **a trójai módszerek például platformfüggetlenül működőképesek**, lásd media codec telepítés. **Aki nem ismeri a saját rendszerét, és túl naív**, és sikerül megtéveszteni, az akár egy Solarison is bepötyögi a root jelszót hozzá.

Aztán ott van az adathalászat, amire úgy tekintünk, ez már egy olyan lerágott csont, hogy már csak egészen zsenge ifjak és élemedett korú aggastyánok sétálhatnak bele clueless módon ilyen kelepcébe. Hát nem, a számok **tanúsága szerint 50 százaléknál is kevesebben vannak tisztában a phishing fogalmával. Ha csak az adathalászatot vesszük, akkor nem volt jelentős eltérés annak fényében, hogy valaki PC vagy Mac user, hogy szenved-e el ilyen számítógépes támadást**.

A megkérdezettek 84 százaléka viszont biztonságosnak véli az online bankolást a tanulmány szerint. Ugyanakkor a felmérés azt is megmutatta, ami egyébként igen logikusan hangzik, ha viszont egy □ **S□ user mégis adathalász támadást szenved el, akkor az átlagnál több pénzt veszít** ezen. Végül is pont ezért lesz majd vonzó célpont, mert a Mac gép divatos és kultikus tárgy lett, igazi státusz szimbólum. Ha a CTU-nál Jack Bauer és Dr. House is azon csapatja, akkor annak jelentős reklám ereje van, mindenki ilyet akar. És akinek van annyi pénze, hogy dupla áron vegyen egy jó hardvert, annak **az adathalászok helyes feltételezése szerint a bankkártyája is vastagabb lesz, mint az átlag**. Erre az egyik kedvenc posztom a Steve Jobs is megvolt című :-)

Milyen is a jó biztonság□Ami egy jó védelmi programon felül (tűzfal, rootkit detektor, antivírus és kémprogram irtó) még **hatásosan csökkentheti az áldozattá válást, az a biztonság tudatosság, a hozzáértés, a veszélyek illetve a számítógépes rendszerünk alapos ismerete**. Emellett persze figyelmetlen néha mindenki lehet.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben

- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1546246

Kommentek:

Nincsenek hozzászólások.

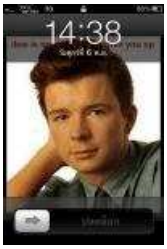
Litvániából szeretettel

2009.11.25. 11:19 | Csizmazia István [Rambo] | 3 komment

Címkék: ing jelszó bank iphone ssh kártevő alapértelmezett

Ilyen című James Bond epizód ugyan nem volt, de még lehet. **Ha egy üzlet beindul**, akkor annak gátat vetni lehetetlen. A jailbreakelt iPhone telefonokon az alapértelmezett SSH jelszó révén nyitott ajtón elsőként benéző hacker után már tömegesen **jelentkeznek a további, szigorúbb tekintetű próbálkozók**. Hogyan jutunk el az Alpokból az "ohshit"-ig, ez lesz a mai kérdés.

Nem is olyan hosszú az út a Pókláb erdőn át. Az alapértelmezett jelszó cseréjének benne kellene lenni azoknak a széles körben alkalmazott számítógépes ismereteknek a tárházában, amit **a hétköznapi embereknek is el kell sajátítani, ha nem akarnak áldozat vagy a digitális analfabéták lenni**. Úgyanígy ha valaki már jailbreakeli azt a telefont, illene az SSH jelszót menten lecserélni (highly recommended). Az első PoC után aztán jött is a második vicces fecske, aki Rick Astley képeket varázsolt készülékekre - emiatt nem is gyanúsítaná az ember rosszindulattal, hiszen csak **az öt perc hírnév mindenkinek jár** alapon cselekedett.



Most viszont itt a harmadik vagy ki tudja hanyadik fecske, és hiába nincs tavasz, vélhetően csapatostul fognak majd érkezni mostantól. Itt is fertőzhető IP címtartományok után kutatnak (hasonlóan az IKEE-hez), de már **szélesebb körben zajlik a keresgélés**, és a szakemberek szerint a holland, ausztrál, osztrák, portugál mellett a magyar tartományok is ezek között vannak. Szintén kevésbbé jó hír, hogy **a féreggel fertőzött iPhone készülékek állítólag egy litván botnet szerverrel maradnak további kapcsolatban**. A dologra egy holland internetszolgáltató hívta fel a figyelmet, miután az általuk tapasztalt **szokatlan hálózati forgalmat részletesen megvizsgálták**.

A BBC oldalain pedig egyenesen egy olyan kártevőről számolnak be, amely a holland ING ügyfelek számára jelent célzott adathalász próbálkozást. Végülis mivel az Ikee/Ikex forráskódja kint csücsül(t) a neten, **nemigen van mit csodálkozni**, ha elkezdenek jönni szépen sorban a variánsok. **Érdekes egy helyzet és nem csak technikailag az**. Egyelőre ugye nem létezik még antivírus program az iPhone-ra, de különben is kérdéses lenne, a cégek pontosan miként akarnának egy nyilvánvalóan törvénysértő (jailbreak) lépés miatti fertőzésre reagálni. (A józan paraszti ész azt diktálná, hogy detektálni, irtani, de **ugyanaz a réteg nem változtatja meg az SSH jelszót, aki antivírust sem venne és futtatna, ördögi kör**.) Az Apple valószínűleg hasonlóan az MS-hez "nem az én problémám" álláspontra helyezkedik egyelőre (Tettszettek volna NEM jailbreakelni), és természetesen az ő szemszögükből ez is valahol érthető.

Akinek annyi pénze van, hogy iPhone-t vegyen, annak érdemes a címjegyzéke, banki adatai után érdeklődni - talán ez lehetne az Ars Poeticaja a bűnözőknek. Minden esetre a profi és kevésbbé látványos lépések már jól jelzik a haszonszerző kártevők lehetséges fejlődési útját, és **a készítők a már emlegetett default "alpine" jelszót is "ohshit"-re cserélik**. Ez persze még mindig lényegesen jobb, mint mikor a Magistr-rel fertőzött számítógépen az összes állományunkat felülírják a "YOUARESHIT" tartalmú elmés szöveggel.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1550789

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.26. 09:15:12

A mai IT Business hírlevélben nagyon találóan fogalmaznak:
"A használókat hibáztatja az Apple képviselője a feltört iPhone-okat mostanában veszélyeztető férgek miatt. Nyilatkozatának lényege: a fenyegetés csak azokat a használókat érinti, akik a megbízhatóságot súlyosan befolyásoló, a gyártó által tiltott változtatást hajtottak végre az iPhone-jukon. Ez egy olyan szemléletet tükröz, mely szerint az (eredeti, sértetlen) iPhone biztonságos, nincs szüksége védelmi szoftverekre. A háttérben talán az áll, hogy az iPhone nem engedélyezi a szoftverek futását a háttérben, ami pedig nem ideális környezet a védelmi programoknak. A Sophos képes lenne féregszűrőt írni az iPhone-ra, de azt is, mint minden külső, iPhone-alkalmazást, jóvá kellene hagyni az Apple-nek – ami a fentiek fényében nem valószínű."

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.26. 09:17:18

Ja és a link hozzá:
www.itbusiness.hu/hirlevel/itsecurity_today/2009-11-26_it_security_today_1333.html

ann Le Pentrec · http://lnk.bz/t7c 2009.11.27. 17:02:06

Puff, megintcsak beigazolódik a képletem a mennyiséggel egyenesen arányos kártevők számával, ahogy azt már vesézgettem az Apple-es témánál. Divat lett az iPhone, divat lett megkeresni a gyenge pontjait is. István, amúgy az az öt perc hírnév tizenöt perc Andy Warhol mondása szerint. :)

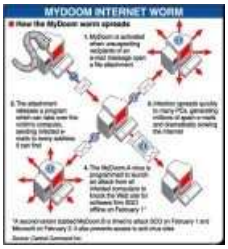
Lehet-e Mengeléből Albert Schweitzer? *Frissítve

2009.11.27. 16:50 | Csizmazia István [Rambo] | 3 komment

Címkék: biztonság szavazás szerző állás bizalom kártevő

Nem igazán szükséges ehhez felütni Prékopa András: Valószínűség-számítási feladatgyűjteményét, mindenki sejtheti a választ. **Az antivírus cégek döntő többsége gondolja úgy, hogy nem**. Hiába a kimagasló technikai tudás, a zseniális elme; **a megbízhatóság, a jellem, a becsületesség, a megfelelő oldalon állás** nem olyasmi, mint mondjuk egy párttagság, amit később ötletszerűen lehet oda-vissza váltogatni.

Az évek során az egyik jelentős változás az volt a kártevők történetében, hogy a fertőzéshez **már nem hónapokra volt szükség - mint kezdetben például a floppy lemezes vírusoknál - hanem napok, sőt akár órák alatt is bejárhatja** az interneten a világot. Akik régóta követik az eseményeket, még emlékezhetnek mikor 2004-ben 250 ezer dolláros vérdíjat tűztek ki az SCO-nál a MyDoom vírus készítőinek fejére.



De a Microsoft is került ilyen helyzetbe, ők pedig a Netsky/Sasser féreg szerzőjének kézrekerítésére ajánlottak hasonló összeget. Ez aztán kellőképpen meg is mozgatta az emberek fantáziáját, és állítólag a személyes környezetéből buktatták le Németországban. (De sosem lehet kizárni ilyenkor azt a forgatókönyvet sem, hogy egy bűntárs vagy barát színleg feladja, aztán később pedig elfelezik a pénzt.) A folytatás aztán meglepő fordulatot vett, mikor állást ajánlottak **Sven Jashannak a német Securepoint IT biztonsági cégnél**.

Eddig ezekről a kivételekről tudtunk, na és persze arról, hogy **Kínában vélhetően nem osztják az ilyen jellegű erkölcsi aggodalmakat**, hiszen ott a Fujack féreg lebukott szerzőjét azonnal elhalmozták állásajánlatokkal. Ezekkel a korábbi esetekkel **csupán bemelegítettünk mai témánkhoz**. **Most éppen arról dúl a vita**, vajon etikus és helyes lépés-e, hogy a jailbreakelt iPhone telefonokat megtámadó IKEE féreg szerzőjét alkalmazták programozónak. A huszonegy éves ausztrál Ashley Towns ugyanis iPhone alkalmazásfejlesztői pozíciót kapott.

Nagyon fontos üzenet lenne, hogy a vírusírás, kártevő készítés továbbra se lehessen egyenes út, követendő példa az álláslehetőségre, karrierre, különösen nem ilyen bizalmi pozíciókban. Ezért ezúttal egy **extra szavazást is beépítettünk**, szavazzon az olvasó: lehet-e kutyából szalonna vagy **rablóból pandúr?**

*** FRISSÍTVE!**

Mivel az eredeti szavazó poll-r.hu oldal láthatóan elhalálozott, ezért próbálunk másik szavazást beépíteni hamarosan.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1555833

Kommentek:

Yann Le Pentrec · http://lnk.bz/t7c 2009.11.27. 16:56:23

Azt hiszem, a számok beszélnek helyettünk a szavazásban. Rendszeres látogatója vagyok a blognak, mondhatom, a top5 kedvencem között van, sok mindent innen tudok meg a kártevőkről, el is ítélem a káros programokat készítőket magamban, mégis másképp gondolom. Valami olyasformán, hogy valószínűleg nem kispályás módon érthetnek a programozáshoz, ezért ha már mód nyílik őket átterelni a "sötét oldalról", akkor ezt kell tenni. Nem mellesleg egy füst alatt csökken is számukkal a vírusírók száma. :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.11.27. 17:08:57

Szia Yann Le Pentrec!

Nem egyszerű a kérdés, az már egyszer igaz. Végülis kevés gyilkost láttunk mi is rendőrkapitánnyá avanzsálni a modern demokráciákban, korábban biztos volt ilyen.

A belinkelt oldalak közt valamelyiken azt láttam, Hypponen kivételesen hajlott az egyik esetben (he was more clueless, then malicious), míg Clueley pedig szigorúan elitél minden egyes ilyen esetet. Tehát még náluk is megoszlik a vélemény.

Jó kérdés még, hogy hogyan ellenőrződ aztán a munkáját, nem épít-e be mégis hátsóajtót, vagy egy év múlva lelép, és visz minden titkot a fejében. Ezek birtokában pedig már egészen jó képességű új kártevőket tudna készíteni.

Yann Le Pentrec · http://lnk.bz/t7c 2009.11.27. 18:16:17

Kétségkívül ül az utolsó bekezdésben hangoztatott kétség, nyilván tűzbe senki nem tenné a kezét értük. :) Aztán mégis lehet, hogy győz bennük a morál, ez is egyénfüggő, attól függ, mennyire hajlik az ember az alkotásra a rombolás helyett.

Rambo a TV-ben

2009.11.28. 10:44 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: tv hírtv műsor negyedik zoltán kulcsár adathalászat

Ezúttal nem lőtt szét semmit, nem szabadított ki vietnami hadifoglyokat, egyetlen benzinkutat sem robbantott fel, hanem békésen adathalászati **kérdésekre válaszolgatott a HírTV Negyedik című adásában** Kulcsár Zoltán kollégával együtt.

Ez a link a televízió weboldalára vezet, aminek **az oldalán található (VIDEÓK: A Hálózat csapdájában) linkre kattintva megnézhető** az archivumból adás online streamje.

Ezzel a poszttal egyúttal a Guiness Rekordok évkönyvének legrövidebb blogbejegyzése címre is pályáztunk ;-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1558126

Kommentek:

Nincsenek hozzászólások.

Örök élet, ingyen sör, ingyen Újhold

2009.11.30. 16:30 | Csizmazia István [Rambo] | 2 komment

Címkék: játék mozi sms csalás hamis new emelt moon kodek díjas

Egyik kedvenc filmemben, mikor a vizsgálati fogoly túszul ejti az őt vizsgáló pszichológust, azt kérdezi tőle, most, ebben **a kiszolgáltatott helyzetben mondja meg pontosan, mit veszített el**. Neki sem megy könnyen, de azért nagy sokára megszüli a helyes választ, ami sokaknak lehet idegen, pedig ideje vele jobban megbarátkozni.

A naívságunkat vesztjük el, **az esemény hatására már gyanakvóbbak és más emberek leszünk, mint annak előtte voltunk. Legalábbis így lenne értelme.** Ha belesünk egy kicsit a bűnözők gépezetébe, felhajtjuk a szőnyeget, mocskos átverést láthatunk mindenütt, amiből tanulni kellene. A keresési találatokat mindig manipulálni fogják, eddig is ez történt, ezután is ez várható. Minden új eseménynél, mozifilm bemutatónál ez történik forgatókönyvszerűen. Az **Újhold - New Moon (Alkonyat 2.) premiert kihasználva gőzerővel terítik a linkeket** a blogok kommentjeiben, digg oldalakon, Google keresésekben.

Bátran mondhatjuk, hogy kiemelten a tapasztalatlan felhasználókat fenyegeti a legnagyobb és legtöbb veszély. Természetesen egyik ilyen jelzett helyen sem lehet megnézni a teljes filmet ingyen, de **a csalók különféle kártékony kódok letöltésére biztatnak minket, illetve a pénzünkre utazva különféle regisztrációkhoz, emeltdíjas játékokhoz kötik** az "ingyen film" állítólagos megnézését.

Kicsit azt is mutatja, hogy a kezdő, ismeretek nélküli felhasználók tábora miért is esik bele különböző csapdákba. **Aki csak nemrég vette a számítógépét a bevásárló központban, nincs a környezetében olyan, aki mindig figyelmeztethetné**, annak a helyzete nem túl egyszerű. Ha kodeknek álcázott kártevőről van szó, ugye ott befigyelhet az antivírus program. De ha valaki gyanútlanul **maga nyom entert, figyelmetlenségből jelentkezik a fizetős SMS játékra, ez ellen semmilyen biztonsági program nem védheti** meg. A **haladók már nem hisznek a mesékben, vásárolnak vagy torrenteznek**, és bár néha ott is vannak fake esetek, de azért ennyire sosem lehangoló a

helyzet, illetve ők már könnyebben meg tudják védeni magukat a felvértezett tapasztalat birtokában.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1562513

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.01. 09:29:25

Új nap, új téma, új mérgezett keresések:
blogs.pcmag.com/securitywatch/2009/11/hackers_exploit_tiger_woods_ca.php

és ez így megy forever...

Dr. iPod 2009.12.07. 00:03:24

Felhasználó ellen nincs orvosság :)

Kártékony linkeket szűr majd a Bit.ly

2009.12.01. 15:20 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság url bit.ly linkrövítés

Elsőnek egy találós kérdés, vajon melyik ország doménjének jele a közkedvelt bit.ly nevében az .LY? Igen, **azok nyerték a hangszórót, akik Líbiát mondták**. Az URL rövidítés szolgáltatásnak ezen túl menően ehhez az országhoz egyébként semmi köze nincs, valószínűleg **a kedvező nyelvtani alak okán lett ilyen**. Az Egyesült Államokbeli cégnél most a működési biztonságot igyekeznek majd megerősíteni az év végéig.

Azt, hogy **a linkek rövítése mire jó és kik használják főként, azt megtárgyaltuk már egy korábbi posztban**. Ugyanitt arról is szó esett, hogy ha egy ilyen szolgáltatást feltörnek, akkor könnyen **manipulálhatóvá tehetők a linkek, akár tömeges méretekben is**.

És beszámoltunk már arról a kedvező fejleményről, hogy készült olyan Firefox plugin, amely képes a kattintás előtt egy buborékban megmutatni, hová is mutat az eredeti, hosszú link. Most újabb tervek kerültek napvilágra, amelyben **a Websense segítségével készülnek megerősíteni a gyenge pontokat. Ennek első eleme egy felhő alapú** megoldás, amely egy naprakész frissítésű adatbázissal **szűrné ki a milliónyi link közül** az adathalász, spam- és kártevő terjesztő weboldalakat.

Ezt **egészítené ki a Verisgn URL és IP adatbázisa, amely ezen feketelisták alapján is** őrködik majd, ne kerülhessen nyilvánvaló rosszindulatú oldalra való hivatkozás. És még mindig nincs vége, a lánc végén **a Sophos kártevő felismerő szolgáltatása, egy viselkedés alapú** elemzése áll. Talán magyar fejlesztő is dolgozik ezen a projekten, annyira süt belőle a "három a magyar igazság" ;-)

A dolog azért roppant örvendetes, mert **azon a területen ügyködnek, ahol az egyszerű felhasználó hatásköre már ér el**. Ha mi naprakész és megfelelő vírus és kémprogramvédelmet használunk, tiltjuk a JavaScriptet, **akkor egyedül mi megússzuk, az internetet böngésző többieknek pedig ott marad a kártékony link**. Így azonban kiszűrik ezeket, és már nem jut el senkihez. Azt persze mindenkinek figyelembe kell vennie, hogy ez egy reaktív technológia, vagyis **mindenképpen eltelik valamennyi idő, amíg egy linkről bebizonyosodik a kártékonyság, és felkerül ezekre a feketelistákra**, de jobb későn, mint soha. Mindenesetre örülünk az újdonságoknak és várjuk a mielőbbi megvalósítást.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés tra□kba□k □íme:

http://antivirus.blog.hu/api/trackback/id/1565839

Kommentek:

Nincsenek hozzászólások.

Pénzt vagy internetet

2009.12.03. 14:40 | Csizmazia István [Rambo] | 5 komment

Címkék: download alkalmazás manager kártevő kéretlen váltságdíj ca ransomware ufast

Valószínűleg senki nem fogja az "internetet" választani ebben az esetben arra zsaroló kártevő által feltett kérdésre, amely **ékes cirill nyelven kér pénzt vagy túszul ejti a számítógépünket**.

Érdekes egy helyzet, **amikor a Windows normál képernyője helyett ezt látjuk és közben eltűnik az internet elérésünk**.

Az első felindulás után (ki, hova menjen, mit tegyen milyen felmenőjével, stb.) szükség lehet a szöveg fordítására, ez angolul nagyjából a következő:

Internet access is blocked due to violation of the
license agreement schedules of uFast Download Manager
You must activate your copy

Get a registration code by sending an SMS with the following
code fw0004199 to number 7122

In response you will receive an activation message.

Enter the activation message received from the SMS response

Vagyis arra hivatkozik, hogy **illegálisan használtuk és ezzel megsértettük uFast letöltési segédprogram licencszerződését**. A vizsgált esetekben **valóban megtalálták ennek a letöltő programnak egy példányát a fertőzött gépeken, de azok kérés és jóváhagyás nélkül települtek** az adott rendszerekre. És **hiába próbálja valaki a Programok telepítése/törlése segítségével uninstallálni, de zsaroló képernyő ettől függetlenül megmarad**.

Ahhoz, hogy újra elérhessük az internetet, fizetnünk kellene **egy emelt díjas SMS küldésével, és cserébe kapnánk meg** a zárlatot megszüntető kódot. **A CA jóvoltából azonban megúszhatjuk a fizetést**, és újra szabaddá tehetjük a gépünket, ugyanis letölthető az oldalukról az aktivációs kód kalkulátor, lesz hát végül öröm, bódottá.

Mindebből leszűrhetjük **akár azt a tanulságot is, hogy** ~~túl sokan végeztek a Lomonoszov Egyetemen és maradtak munka nélkül rengeteg felesleges szabadidővel~~ **mindig érdemes bejelölni a vírusirtó telepítésekor a kéretlen alkalmazások detektálása** nevű menüpontot is.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1570869

Kommentek:

Yann Le Pentrec □http:□lnk.bz t□c 2009.12.08. 15:56:46

Kellemetlen, ha nincs kéznél másik gép, vagy windows installálva másik partícióra/merevlemezre, lévén az internet elérés blokkolva van, és nem tudjuk a CA keygent letölteni. 22-es csapdája. :)

Yann Le Pentrec □http:□lnk.bz t□c 2009.12.08. 16:08:38

Érdekes, miért nem jelennek meg az új hozzászólások - blog.hu motorja rendetlenkedik?

Yann Le Pentrec □http:□lnk.bz t□c 2009.12.08. 16:09:54

Vagy ilyen delay-jel, hogy csak egy második hozzászólás csalja elő az elsőt? WTF! Sorry mindenesetre.

Csizmazia István [Rambo] □http:□antivirus.blog.hu 2009.12.08. 19:05:12

Ez egy kellemesebb dolog, ahhoz képest, mintha az állomanyainkat kódolná el, lásd GPCode.

Én azt szoktam javasolni, hogy a Windows mellé másodiknak érdemes feltenni legalább a vinyó végéből lecsipett 10 GB helyre egy Linuxot, és ha bármi baj van (ilyen, vagy nem indul a Win, világvége, whatever) akkor a Linux alól még simán lehet az NTFS-t vagy FAT32-t olvasni, adatot kimenteni, megnézni, mi történt, vagy csak netezni mosolyogva az ilyen Windows csodakártevők dacára :-)

Yann Le Pentrec □http:□lnk.bz t□c 2009.12.08. 20:56:49

Igen, ez is egy jó ötlet, bár én erre a célra egy aktuális Ubuntu telepítőt tartok RW lemezen, amely ugye képes live cd-ként is viselkedni, és netán elvégezni olyan feladatokat, amelyeket Winnel nem vagy nehézkes legalábbis. Vagy mint legutóbb: lockolt system file-ok törlése NTFS rendszerpartícióról. Arra nem merek gondolni, hogy vírus miatt legyen rá szükség, dehát biztos,

ami sicher.

Hamis antivírus gyári webkamerával

2009.12.04. 15:35 | Csizmazia István [Rambo] | 4 komment

Címkék: cd office webkamera hardver kókusz fertőzött szigetek depot gyárilag markvision

Újabb bejegyzéssel gyarapodott a gyári, boltban vásárolt, de fertőzést okozó hardverek szemelvénye. Most **egy Office Depot-ban beszerzett webkamera CD lemezéről** indult útjára a kártevő.

Ezúttal egy Anna Giesman nevű illető vásárolt egy webkamerát az Office Depo üzletében, hogy majd családtagjaival felhőtlenülül tudjon diskurálni az interneten keresztül. A **gyárilag mellékelt dokumentációt tartalmazó lemezen azonban egy link egy hamis vírusirtót terjesztő kártékony oldalra** mutatott, így a vevő gépe megfertőződött.

Előtte már néhány nappal a Google keresőtől kiérdemelték a lehetséges kártékony oldal megtisztelő címet, de érdemi intézkedés akkor nem történt. Érdekes a hivatalos reakció is: **a vevőknek nem volt szükséges a mellékelt CD lemezt telepíteni az üzemszerű működés érdekében**, csak kisszámú ügyfél lehet érintett ebben a problémában, ez a beszállító (Markvision) már nem is igazi hivatalos beszállító, ~~meg különben is,~~ stb. Azért ennek ellenére az érintett weboldalt időközben ideiglenesen, majd később annak egyes, a fertőzéssel kapcsolatos részeit lekapcsolták.

Az eset arra lehet jó figyelmeztetés, **bármelyikünk belefuthat egy ilyenbe. Az a legjobb, ha egy valódi antivírus már alaphelyzetben működik a gépünkön, és az majd felismeri a később próbálkozó hamis antivírust**. Emellett **éljünk a gyanúperrel bármilyen link esetén** (lásd a látszólag ismerőseink által küldött közösségi üzenet). És bár korábban Kínára hegyeztük ki többször is a kérdést (pl. Kínából jöhet-e normál esetben levelünk), **a Kókusz Szigetekre éppúgy nem vetődik senki véletlenül** egy weblap létrehozással (talán olcsó, talán "rugalmasak" a törvények, talán mindkettő), ahogy ciprusi offshore cége sincs mindenkinek csupa merő véletlenségből, hanem csak keveseknek, de nagyon direkt.

Technikailag a gépeket, CD lemezeket pedig emberek csinálják, akik hibázhatnak, **figyelmetlenek lehetnek, gyártás közben elavult vagy semmilyen védelmet sem használnak vagy akár direkt is rosszat akarhatnak** nekünk. Említhetjük, hogy mennyire **nem óv meg minket az, ha valaki csak átlagos weboldalakat látogatunk**. Tehát érdemes mindig kellő figyelemmel birtokba venni az új műszaki szerzeményeinket, kapott ajándékainkat, még idejében szólunk ;-)

Egyúttal pedig minden kedves Olvasónknak boldog Mikulást kívánunk!

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1573109

Kommentek:

gothmog 2009.12.05. 14:21:17

egy kérdés, az ilyen az milyen?:
imagerz.com/QENEDEtvAw□C□ □fR□A□Q
Illetve, és ezt most így hogy? (direkt nem direktlink)

gothmog 2009.12.13. 14:16:30

nyehehe, leszedték. Rambo, Te voltál? :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.14. 09:50:02

□zia Gothmog!

□rtatlan vagyok, nélkülem vették le, sőt még csak meg sem kérdeztek ;-)))

gothmog 2009.12.14. 18:36:37

□dv!
Akkor viszont nem piti, hogy a kiírás szerint □ 007ta fent volt, és aztán egy héten belül eltűnik, miután linkelek róla egy képernyőfotót egy kommentben.
□zerintem valaki figyel.
;)

Brigitte, de nem Nielsen

2009.12.07. 17:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam kampány email álláshirdetés óvatosság

A "Vállaljunk állást" című sorozatunkban ezúttal a postafiókunkat beterítő és **heti mindössze 3-4 órás munkával megkereshető 2000 eurós** ajánlattal foglalkozunk. Kérdéseink maradtak ugyanazok: hogyan, miért és egyáltalán?

Amikor **az elektronikus csalásokból származó bevétel már évek óta meghaladja a drogkereskedelemét**, és amikor minden harmadik másodpercben a világon ellopják valakinek az identitását, **nem mindegy, mennyire hiszünk** a mesékben az álláshirdetések területén sem.

Természetesen a lenti nézelődések már eleve csupán elviek voltak, az elejétől 99%-ig látszott rajtuk, hogy komolytalan az ajánlat:

- **ugyanaz a feladó, mint a címzett: mi magunk**. Alap hiteltelenség, rögtön egy spamgyanús jel

- **ugyannarra a pozícióra nem küld szét valódi cég több munkatárs nevében** és különböző emailcímekkel szinte szóról szóra egyező állás hirdetést: Brigitte, Todd, Della, Alvaro, Milagros, Szervác, Pongrác, Bonifác, Álmos, Előd, Ond, Kond, Tas, Huba, Töhötöm, stb.

- valódi cég a **központi céges email címre, egyedi hr-es vagy a konkrét egyedi álláshoz kreált, illetve a fejvadász cég központi címére vár levelet**, és természetesen csak attól, aki előtt jelentkezett, írt nekik, vagy szerepel az adatbázisukban

- kéretlenül pénzkereső levelet sosem küldenek, ez **inkább a csalók, a piramisjáték építők, vagy az emailcím gyűjtők** szokása

- **a Re: vagy Válasz: tárgysorral kezdődő, de részünkről előzmény nélküli levél bátran a kukában végezheti**, aki már itt nem mond igazat, annak felesleges további hazug sorait elolvasni

- a "magas kereseti lehetőség, részletek kizárólag felbélyegzett borítékban küldött pénzért" vagy "**emailcímével jelentkezzen most**" típusú becsapásokra eleve kár vesztegetni az időt

- komoly álláshirdetésekben **nem azonnal a fizetés mértékét hangsúlyozzák, hanem az elvégzendő feladatot körvonalazzák**, hogy majd megfelelő jelöltek válaszoljanak. Akár csak a sokadik interjú körben veszik elő majd az ellentételezés kérdését

- a heti 1-4 órával (a variánsok 1-4, 2-3, 2-4, stb. alváltozatokat is tartalmaznak) megkereshető 532 x 4 hét = **2128 E□R (cirka havi 570 ezer □ □ elég vonzó** ahhoz, hogy sokak figyelmét felkeltse, és nem túl magas összeg ahhoz, hogy mindenkinek alapból hihetetlen legyen, de azért elég hihetetlen mértékű ahhoz, hogy a jelzett elfoglaltsághoz képest túlzásnak mondhassuk.

- Valamelyik Moldova könyvben szerepel, hogy a költségelszámoláskor csak a mukinyulak írnak be kerek összeget, ami azonnal árulkodó gyanús jel a könyvizsgálónak, a belső ellenőrzésnek. A tételek rendre véletlenszerű értékekkel símulnak bele az átlag Gauss görbe számaihoz, hogy még véletlenül se tűnjenek "csináltnak". Itt **a heti fizetés 532 E□R összege is ilyennek látszik**, talán a hihetőség látszatát próbálja emelni

- **a munkához szükséges tudás, képesítés, tapasztalat nincs rögzítve**, vagyis a hirdetés lényege, hogy azonnal sok címről jelentkezzenek. Normális helyen nem akarnak temérdek felesleges pályázó adatával is rendelkezni, hiszen később jóval nehezebb a sok szemét közt Augiász istállóját kitakarítani, hanem megélegszenek a valódi potenciális jelöltek elérhetőségeivel, adataival. Mivel itt nem így van, ezért rögtön szembeötlik a kezdeti magas merítés iránti igény, cím vagy identitás kell nekik ipari méretekben

A levelek feladójának címe alapján a domént megvizsgálva az látszik, hogy azt az iráni Omid Jafarzadeh foglalta le. Elviekben **az sem kizárható persze**, hogy a levelező szerverüket feltörték.

Szokták mondani azt is, hogy a mai világban a gaz kapitalsta munkáltató már a privát szféránkat is kifürkészi, és igyekszik jó alaposan felderíteni hátterünket, megbízhatóságunkat, hozzáállásunkat. De **ha ez nem lenne, akkor is javasolt ugyanennek a fordítottja nekünk, nyilván a munkavállalónak sem mindegy** hova menne, milyen körülményel közé, illetve hogy egyáltalán valódi ajánlatról szól-e a toborzó levél. Ha valaki egy öszvér-szerű (mule) állásban kezd el tényked ni, az aztán később ne csodálkozzon, ha egyszer **mikor hazamegy, ég majd a villany, az ajtó résnyire nyitva lesz, és a kulcs is belül** van. Fekete bőrkabátos emberkék pedig élénken érdeklődnek majd ilyen "banki átautalás", "pénzmosásban való részvétel", "tudta-e hogy ez törvénytelen" és egyéb hasonló varázsszavak után. Akinek nincs meg a tudása, kíváncsiága, intelligenciája, motivációja, türelme, hogy ilyeneknek utánanézzen, **vagy csak a gyanakvása, hogy ne higgyen el mindent**, az sajnos ezzel **elbukja a képzeletbeli felvételi nulladik lépcsőfokát**, amivel később esetleg kellemetlen helyzetekbe hozhatja magát.

□ **entsük hát meg a fákat, együnk hódot**, és egyáltalán ne válaszoljunk semmilyen e-mailre ;-)

□jánlott bejegyzések:

- Gyerek-barát netezés
- Ez történik a weben egy perc alatt
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

□ bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1579680

Kommentek:

Nincsenek hozzászólások.

Nincs gondja a vírusirtóknak az új Windowssal

2009.12.08. 15:28 | Csizmazia István [Rambo] | 6 komment

Címkék: teszt díj nod32 59 100% windows7 virusbulletin

A brit **Virus Bulletin először vizsgálta Windows 7 platformon** az antivírus programok teljesítményét. A független tesztre rekordszámú nevezés érkezett, a programok többsége pedig sikerrel vette az akadályokat.

A Virus Bulletin szakemberei legutóbbi, **Windows 7 Pro platformon végzett tesztjükön 43 vírusirtó program teljesítményét** hasonlították össze. A résztvevők kiemelkedően magas számának egyik oka, hogy számos gyártó több termékkel képviseltette magát, a másik pedig, hogy ismét megjelent néhány eddig szinte ismeretlen nevező is.

A VB100% díj megszerzéséhez a védelmi programoknak az összes vadon élő vírust fel kell ismerniük anélkül, hogy téves riasztást adnának. A laboratórium szakemberei ezen felül vizsgálják a különböző férgek és trójai kártevők találati arányát, valamint a programoknak azt a képességét is, hogy **a nevezés előtti és utáni hetekben gyűjtött károkozók hány százalékát képesek** sikerrel felismerni és hatástalanítani. A nevezés után beérkezett minták tesztelése **elsősorban a szoftverek proaktivitásának mérése miatt fontos, hiszen ilyenkor a vírusirtóknak - frissített adatbázis híján - már mesterséges intelligenciájukra** kell hagyatkozniuk.

A teszteléshez használt kártevők között ezúttal **ismét szerepelt a Conficker számos variánsa, valamint az Autorun alkalmazások különféle változatai**, melyek szintén hosszú ideje szerepelnek a magyarországi vírustoplistán. Az újabb károkozók közül elsősorban a közösségi hálózatokat és az online játékosokat támadó fenyegetések kerültek be a teszteléshez használt mintába.

Ezúttal a vírusirtók **nagy része sikerrel teljesítette a VB100% minősítés megszerzéséhez** szükséges feltételeket: a 43 résztvevő közül 35 detektálta az összes vadon élő vírust úgy, hogy közben nem adott téves riasztást. Közülük a rekordtartó ESET NOD32 Antivirus 1998 óta vesz részt rendszeresen a Virus Bulletin független tesztjein. **A szoftver az elmúlt 11 évben 59 VB100% díjat szerzett, ami mutatja a NOD32 folyamatosan megbízható teljesítményét**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1583469

Kommentek:

Yann Le Pentrec · http://lnk.bz/t7c 2009.12.08. 15:51:12

Sajnos a mellékelt linktől nem lettem okosabb, nem lévén VB előfizető. (A legolcsóbb megoldás 175 dezső? OMG) Lehet tudni az eredményességi listát? Persze tudom, hogy mint NOD disztibútor, nem szívesen hype-olnád a konkurens termékeket, ám mégis jó lenne valami összegzés a non-subscriber egyorrúaknak is. :)

Yann Le Pentrec · http://lnk.bz/t7c 2009.12.08. 15:51:59

Na most meg hova tűnt a hozzászólásom...vagy duplázódni fog?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.08. 18:59:28

Sorry, tényleg rövid az a link. Az csak a dolog egyik része, hogy valóban fizetős. A másik viszont, hogy jogi okokból külön előzetes engedélyük nélkül nem szabad közölni az ottani grafikonokat, részletes teszteredményeket, csak kivonatosan lehet rá hivatkozni, na ezért ilyen ez a poszt is.

A szitu meg a teszten a következő volt: sikertelenül szerepeltek az alábbi szoftverek: AhnLab V3Net I.S., a CA Internet Security Suite Plus és a CA Threat Manager, az eEye Blink Professional, a Filseclab Twister Anti-TrojanVirus, a Kingsoft Anti-Virus 2010 Swinstar, a Microsoft Forefront Client Security és a Norman Security Suite. Az első alkalommal induló Preventon Antivirus, a Sunbelt Vipre, valamint a Qihoo 360 Security sikeresen megszerezte első minősítését.

Yann Le Pentrec · http://lnk.bz/t7c 2009.12.08. 20:51:50

Szerencsére a felsoroltak olyan szoftvernek tűnnek, amelyek nélkül is élhetünk a továbbiakban is. :) Azért az élmezőny furdalja rendesen a kíváncsiságom...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.14. 09:51:39

Hali Yann Le Pentrec!

Rajta vagyok az ügyön, keresek publikálható anyagot ide, és ki fogom majd tenni.

Yann Le Pentrec · http://lnk.bz/t7c 2009.12.17. 15:29:18

Köszi!

Kártevőt tartalmazott a Linuxos képernyővédő

2009.12.10. 15:15 | Csizmazia István [Rambo] | 1 komment

Címkék: linux script waterfall vízesés kártevő képernyővédő .deb gnome look.org

Érdekes esetnek lehettünk tanúi néhány napja, **egy publikus oldalról letölthető vízesés (Waterfall) nevű Linuxos képernyővédőben kártékony kódot azonosítottak**. Önmagában kevés a boldogsághoz ha a Windowst hátrahagyva egy Linux vagy egy Mac figyel a gépünkön, az odafigyelés, a minimális hozzáértés, és **a meggondolt telepítés az, ami kellhet még a tarsolyba a tartósan tiszta géphez**.

A Gnome-look.org oldalon található képernyővédő "érdekességeiről" két külön topikban is értekeztek, egy UbuntuForumos és egy másik Kubuntus beszélgetés is ír a részletekről. Az történt, hogy a képernyővédő mellé titokban érkezett még **egy DDoS támadásokhoz is használható extra script az áldozatok számítógépére**. A gyanús .DEB csomagot időközben már leszedték a Gnome-Look.org weboldalról.

A nagy tanulság annyi, hogy **hiába van ott a nagyságrendekkel biztonságosabb alternatív platform (vírusok és férgek szempontjából), ha helytelen hozzáállással ellenőrizetlen és megbízhatatlan forrásból való telepítéssel saját magunk** ártunk magunknak. **GPG-vel alá nem írt, illetve nem hivatalos tárolókból, nem megbízható fejlesztők weboldaláról letöltött tartalom mindig lehet ilyen** gyenge láncszem.

A Firefox böngésző esetében is járhatunk hasonlóképpen a megbízhatatlan kiegészítőkkel. Igaz nagy ritkán még a korábban teljesen biztonságosnak vélt kiegészítőről is derülhet ki utólag komoly disznóság, de ez tényleg kivételes eset.

Mindenesetre fő csapásiránynak, vezérfonalnak érdemes idézni CVK kollégát, aki ezt szemléletesen így fogalmazta meg egyszer: "**Nem mindegy hogy a plugint a firefoxhoz a https://addons.mozilla.org-ról szeded, vagy a pistike.firefoxplugin.pistikeoldala.ru-ról**".

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1587870

Kommentek:

atko 2009.12.17. 09:45:04

Most már nincs félni való, mert már van nekünk is nod32-önk! Itt most egy bő-bő is kívánkozna, ha még óvodások lennénk. MindenESETre megnyugvással töltöttem le és próbáltam ki a még béta verziót, de nekem bejött és tökéletesen működik a Mandrivámon. Persze 0 kártevő, de hát az ördög szeme nem véletlenül karikás.

Conficker, te féreg

2009.12.14. 10:35 | Csizmazia István [Rambo] | 4 komment

Címkék: magyar adatok nod32 eset havi threatsense vírusstatisztika

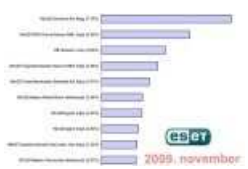
Az ESET szakértői szerint a 2008 decembere óta toplistás **Conficker féreg elképesztően sokáig szerepel a 10 leggyakoribb kártevő között**. Ebben a hónapban ráadásul **ismét listavezető, pedig elvileg minden információ és segítség adott** lenne a géptulajdonosoknak ahhoz, hogy megszabaduljanak tőle.

Az **ESET minden hónapban összeállítja a Magyarországon terjedő számítógépes vírusok toplistáját**, melynek elemzése mindig tanulsággal szolgálhat a felhasználók számára.

A toplistán továbbra is minimális változások történtek az élmezőnyben az előző hónaphoz képest. C-vel kezdődik, nem a Jézuska hozza, vízszintes 9 betű, és csak kevesen örülnek neki, mi az? **Tartja az első helyet a nemrég születésnapos Conficker**, amelyet júniusban, júliusban és októberben is birtokolt. A Conficker egy olyan hálózati féreg, amely a Microsoft Windows egyik biztonsági hibáját kihasználó exploit kóddal terjed, gyenge admin jelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül is terjed a fertőzés. Bár az RPC (Remote Procedure Call) vagyis a távoli eljáráshívással kapcsolatos sebezhetőséghez **már 2008. októberben kiadták az MS08-67 jelű Microsoft biztonsági javítócsomagot**, amely elhárítja a hiba kihasználhatóságát, ennek ellenére sok Windows alapú számítógépen nem fordítanak elég figyelmet a naprakész vírusvédelem mellett az operációs rendszerre is. Emellett a nagy számú fertőzésnek az is az oka lehet, hogy folyamatosan számtalan új variáns, módosított változat jelenik meg, melyeknél a készítők rendre igyekeznek tesztelni és kijátszani a felismerést.

Láthattuk, hogy számtalan terjedési módot képes igénybe venni, viszont **úgy tűnik, magának az operációs rendszernek a frissen tartását nem tartja mindenki ugyanolyan fontosnak, mint a vírusirtójának naprakészségét**. Pedig már jó sok év óta ez egy olyan fontos alappillére a biztonságnak, ami mellett hiába van jó vírusirtónk, az önmagában nem elengedő a megfelelő védekezéshez. **A Conficker tartós előkelő helyezésének többek közt ez is az egyik oka lehet**, ezért érdemes erre a területre kiemelten odafigyelnünk.

Mit tegyünk tehát, mivel tarthatjuk könnyen naprakészen a Windows rendszerünket? Először is válasszuk a Windows frissítések automatikus fogadását, ezzel minden fontos biztonsági frissítés megérkezik majd a gépünkre. **Az új 4.0-ás NOD32, illetve ESET Smart Security már a tálca ikon narancssárga színével, illetve külön rendszerüzenettel képes figyelmeztetni** a szükséges, javasolt biztonsági frissítésekre. Ezenkívül külső segédprogramokat is igénybe vehetünk, az egyik lehetséges jó választás az ingyenes Secunia Personal Software Inspector (PSI). Ennek segítségével nem csak a Windows operációs rendszerének, hanem a Microsoft Office, illetve minden egyéb más külső gyártó feltelepített programjának naprakészségét is egy gombnyomással megvizsgálhatjuk, a javasolt szükséges biztonsági frissítésekre javaslatot kapunk, illetve ezeket egy táblázatban felkínált linkek segítségével könnyedén elvégezhetjük. Mivel a számítógépes **kártevők döntő többsége kijavítatatlan sebezhezőségeket** (exploit) keres és ezeket kihasználva próbál behatolni, rendszerünk naprakészen tartásával hatékonyan akadályozhatjuk meg az ilyen fertőzéseket.



Végezetül következzen a magyarországi toplista. Az **ESET több százezer magyarországi felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2009 novemberében** az alábbi 10 károkozó terjedt a legnagyobb számban hazánkban. Ezek együttesen 34.45%-ot tudtak a teljes tortából kihasítani maguknak.

1. Win32/Conficker.AA féreg
Elterjedtsége a novemberi fertőzések között: 7.79

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows legfrissebb biztonsági hibáját kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos vírusvédelmi webcím is elérhetetlenné válik a megfertőzött számítógépen.

számítógépre kerülés módja: változattól függően a felhasználó maga telepíti, vagy pedig egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat hordozható külső meghajtó fertőzött Autorun állománya miatt.
Bővebb információ: http://.eset.hu/virus/conficker-aa

2. Win32/PSW.Online[illegible]ames.NN trójai
Elterjedtsége a novemberi fertőzések között: 5.29

Működés: Ez a kártevő család olyan trójai programokból áll, amelyek billentyűleütés-naplózót (keylogger) igyekszenek gépünkre telepíteni. Gyakran rootkit komponense is van, amelynek segítségével igyekszik állományait, illetve működését a fertőzött számítógépen leplezni, eltüntetni. Ténykedése jellemzően az online játékok jelszavainak begyűjtésére, ezek ellopására, és a jelszóadatok titokban történő továbbküldésére fókuszál. A távoli támadók ezzel a módszerrel jelentős mennyiségű lopott jelszóhoz juthatnak hozzá, amelyeket aztán alvilági csatornákon továbbértékesítenek.

számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://.eset.hu/virus/ps-onlinegames-nnu

3. INF/Autorun vírus
Elterjedtsége a novemberi fertőzések között: 3.84

Működés: Az INF/Autorun egyfajta gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó kórokozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul.

számítógépre kerülés módja: fertőzött adathordozókon (akár MP3-lejátszókon terjed.
Bővebb információ: http://.eset.hu/virus/autorun

4. Win32/TrojanDownloader.Swizzor.NBF trójai
Elterjedtsége a szeptemberi fertőzések között: 3.38

Működés: A Trojan.Downloader.Swizzor egy olyan kártevő, melynek segítségével további kártékony állományokat másolnak a támadók a fertőzött számítógépre. Többnyire reklámprogramokat tölt le és telepít. A Swizzor terjedéséhez a hiszékenységet is kihasználja: olyan programokba is bele szokták rejteni, amelyek látszólag peer 2 peer hálózatok sebességét (pl. Torrent) optimalizálják, valójában azonban maga a kártevő lapul a „csomagban". Emellett hátsó ajtót is nyit a megtámadott számítógépen. A bűnözők így teljes mértékben átvehetik a számítógép felügyeletét: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.

A számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://□ □ .eset.hu/virus/trojando□nloader-s□izzor-nbf

5. Win32/TrojanDo□nloader.Bredolab.AA trójai
Elterjedtsége a novemberi fertőzések között: 2.87□

Működés: A Win32/TrojanDownloader.Bredolab.AA egy olyan trójai program, melynek segítségével a távoli oldalakról letöltődnek és végrehajtódnak ezek a kódok. Futása közben a Windows, illetve a Windows/System32 mappákba igyekszik új kártékony állományokat létrehozni. Emellett a Registry adatbázisban is a bejegyzéseket manipulál, egészen pontosan kulcsokat készít, illetve módosít a biztonságitámogatás-szolgáltató (SSPI – Security Service Provider Interface) szekcióban. Ez a beállítás felel eredetileg a felhasználó hitelesítő adatainak továbbításáért az ügyfélszámítógépről a célkiszolgálóra.

□ számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://□ □ .eset.hu/virus/trojando□nloader-bredolab-aa

6. Win32/Ad□are.When□Save alkalmazás
Elterjedtsége a novemberi fertőzések között: 2.46□

Működés: A Win32/Adware.WhenUSave működése során létrehozza a saveupdate.exe nevű állományt. Az ilyen nem kifejezett kártevő, hanem inkább a veszélyes vagy nem kívánt programok kategóriába tartozó kéretlen reklám programok sok esetben élnek olyan trükkökkel, hogy különféle további könyvtárakban is létrehoznak magukból másolatot. Ennek kettős célja van: egyrészt egy esetleges vírusirtást követően egy eldugott helyen megmaradhatnak a fertőzött állományok, másrészt helyi hálózatokban, megosztott könyvtárakban, peer-to-peer hálózatokban is képesek terjedni. Futása során megkísérel a web.whenu.com weboldalhoz kapcsolódni, ahonnan kéretlen reklámokat valamint saját program frissítésit tölti le. A fertőzött gépen aktív böngésző esetén linkeket, időjárás jelentést és más kéretlen reklámokat jelenít meg.

□ számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://□ □ .eset.hu/virus/ad□are-□henusave

7. Win32/□ryptik trójai
Elterjedtsége a novemberi fertőzések között: 2.43□

Működés: A trójai nem rendelkezik saját magát telepítő kódrészlettel, azt a felhasználó maga tölti le és indítja el. A megtámadott számítógépről információkat próbál gyűjteni, amelyeket véletlenszerűen generált néven .htm, illetve .png kiterjesztésű fájlokban tárol el, és azokat különféle weboldalak felé igyekszik továbbítani.
Azért, hogy a trójai gondoskodjon saját indításáról minden egyes rendszerindítás esetén, a rendszerleíró-adatbázisban több különböző bejegyzést hoz létre. Emellett hátsó ajtót is nyit, melyen keresztül a távoli támadó később is könnyen hozzáfér a megfertőzött számítógéphez.

□ számítógépre kerülés módja: a felhasználó tölti le és futtatja.

Bővebb információ: http://□ □ .eset.hu/virus/kryptik-gt

8. Win32/Agent trójai
Elterjedtsége a novemberi fertőzések között: 2.20□

Működés: Ezzel a gyűjtőnévvel azokat a rosszindulatú kódokat jelöljük, amelyek a felhasználók információit lopják el. Jellemzően ez a kártevő család mindig ideiglenes helyekre (Temporary mappa) másolja magát, majd a Rendszerleíró adatbázisban elhelyezett Registry kulcsokkal gondoskodik arról, hogy minden rendszerindításkor lefuttassa saját kódját. A létrehozott állományokat jellemzően .DAT illetve .EXE kiterjesztéssel hozza létre.

□ számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://□ □ .eset.hu/virus/agent

9. WMA/TrojanDo□nloader.GetCodec.gen trójai
Elterjedtsége a szeptemberi fertőzések között: 2.12□

Működés: Számos olyan csalárd módszer létezik, melynél a kártékony kódok letöltésére úgy veszik rá a gyanútlan felhasználót, hogy ingyenes és hasznosnak tűnő alkalmazást kínálnak fel neki letöltésre és telepítésre. Az ingyenes MP3 zenéket ígérő program mellékhatásként azonban különféle kártékony komponenseket telepít a Program Files\VisualTools mappába, és ezekhez tucatnyi Registry bejegyzést is létrehoz. Telepítése közben és utána is kéretlen reklámablakokat jelenít meg a számítógépen.

A számítógépre kerülés módja: a felhasználó maga telepíti.
Bővebb információ: http://□ □ .eset.hu/virus/trojando□nloader-getcodec-gen

10. Win32/Ad□are.Virtumonde alkalmazás
Elterjedtsége a novemberi fertőzések között: 2.07□

Működés: A Virtumonde (Vundo) program a kéretlen alkalmazások (Potentially Unwanted) kategóriájába esik az ESET besorolása szerint. A károkozó elsődleges célja kéretlen reklámok letöltése a számítógépre. Működés közben megkísérel további kártékony komponenseket, trójai programokat letöltő webcímekre csatlakozni. Futása közben különféle felnyíló ablakokat jelenít meg. A Win32/Adware.Virtumonde trójai a Windows System32 mappájában véletlenszerűen generált nevű fájl(oka)t hoz létre.

□ számítógépre kerülés módja: a felhasználó tölti le és futtatja.
Bővebb információ: http://□ □ .eset.hu/virus/ad□are-virtumonde

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1595819

□ommentek:

DeTo□ □ 2009.12.14. 13:46:50

a vírusok 90%át a seggfej userek telepítik maguknak. a seggfejségre miért nincs írtó? :P

□ i□ion 2009.12.14. 14:02:43

@DeToXXX: Hozzánk sok külső anyag fut be, van vírusírtó, de 2 gépen beszívtuk a confickert. Szerencsére a Symantec eltávolítóval leszedtük.

Igaz, az elővigyázatosság fontos, ez az első "védelmi vonal".

□ i□ion 2009.12.14. 14:05:49

A virtumonde meglepő, hogy utolsó. Nagyon komoly, főleg amiket lehúz plusszba... megizzasztott már 1-2×. Mondjuk annyival "jobb", hogy itt látják hogy nagy a baj, és szólnak, a CF meg jól el van, és ezért sokan nem is tudják, h fertőzött a gépük.
Pedig csak a microsoft oldalt kellene próbálni elérni, ha nem megy, akkor ott van a mocsok.

gothmog 2009.12.14. 19:02:04

@◄ViZion: valószínűleg ez a válasz, egy rendesen beépült virtumonde gyakorlatilag használhatatlanná teszi a gépet az állandó hangoskodásával. Muszáj leirtani, nem lehet "ellenni vele".

41 lovas hintó

2009.12.16. 16:30 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: virus új vizsgálat total uploader

Picit megint reszelgettek a fiúk a **VirusTotal Uploaderen, kapott is egy 2.0-ás verziószámot**. Dióhéjban végigfutunk az újdonságokon, és néhány esetleg kevéssé ismert régi tulajdonságon.

Ha valaki esetleg netalántán nem ismerné, mi is az a VirusTotal, az a Vírusok Varázslatos Világa 1-es cikkéből pótolhatja alapismereteinek ilyetén fehér foltjait ;-) A két év alatt aztán a 32 lovas fogatból 41 lovas hintó lett. A sokak által ismert weboldalon felül létezett még egy VirusTotal Uploader nevű letölthető segédprogram is, amely most átesett egy alapos frissítésen. Bár a Windows alá elkészített telepítőcsomag **mindössze 139 kB**, ennek ellenére az aprócska program sok földi jóval szolgál. Az egyik legfontosabb újdonság a méretkorlát változása, amelynek keretében **a korábbi 5MB-tal szemben mostantól 20 MB méretű állomány tölthető fel** így vizsgálatra.

Akik régebben kizárólag csak webes felületen, esetleg e-mailben küldözgettek vírusmintát, azok számára már az a régi feature is egy újdonság lehet, hogy **a program segítségével a futó folyamatok (process) közül bármit feltölthetünk vizsgálatra egyetlen kattintással**. Például ha a sok svchost közül az egyikre valamiért gyanakszunk, **vagy az "en_egy_virus_vagyok_irta_troppauer_humer" nevű munkafolyamat tűnik fel nagy hirtelen a feladat kezelőben ;-)** De emellett a Fájlkezelőben megjelenik a jobb gombos menüben egy kényelmes VirusTotal sor, ez is csak a webes hardcore feltöltőknek lehet újság. Ami **viszont tényleg új, az hogy a program egy önmagában futó alkalmazás lett, és nem csak tallózással lehet fájlt kiválasztani, hanem fogd és vidd** (drag & drop) segítségével is.

Az új verziójú programnak egyébként is vág az esze, mint az intelligens mosópornak ;-) Például **feltöltés előtt kiszámolja az állomány hash-ét, és leellenőrzi azt a VirusTotal oldalon**. Az eredménytől függően pedig beszól, ha egy korábbi riportot már feltöltés nélkül is olvashatunk. Természetesen **semmi akadálya az ismételt ellenőrzésnek**, ha például az előző teszt időpontja esetleg túl régi, vagy ha egyszerűen mégis el akarjuk végezni a detektálást, "mer' csak".

Végül a készítők nagy barátságosan nem csak azt kérik, hogy ha esetleg bármilyen hibát észlelünk, akkor szóljunk nekik, de **ezenfelül bátorítanak minket új hasznos ötletek, kérések, javaslatok elküldésére is.**

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat

- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1599728

Kommentek:

Nincsenek hozzászólások.

Nézegessen eltérített Twittert!

2009.12.18. 15:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: army cyber twitter támadás dns deface iranian

Rövid üdvözlő látogatást tett az Iráni Cyber Army nevezetű testület a twitter címoldalán, amely ettől kissé nagyon megváltozott. A napi nyolcmillió látogatónál is magasabb olvasói számmal rendelkező mikroblog oldal mindenképpen vonzó célpont a támadók számára.

Furán festett a Twitter nyitóoldala az iráni zászlóval és a deface üzenettel. Hogy aztán tényleg iráni elkövetőek voltak-e, biztosan nem tudhatjuk. A Techcrunch cikkéből nem csak arról tájékozódhatunk, ki, mikor és mit vett észre, hanem az update hegyekből az olvasók beszámolói, Youtube videói is továbbárnyalják a részleteket.

A weboldal működése azóta már visszazökkent a régi kerékvágásba, de az oldal üzemeltetőinek érdemes lesz egy alaposabb vizsgálattal kideríteniük, mi és hogyan történt, és fokozni az óvintézkedéseket. Első körben a DNS bejegyzésük manipulálását, átirányítását tételezik fel a szakemberek. Közben egy másik kisebb weboldal is hasonlóan módosítva lett, az még a poszt írásakor is defacelt képet tartalmazta.

A felhasználók számára a beszámoló sok update-je közül **az a jótanács látszik a leggyakorlatiasabbnak, mely szerint ha valakinek minden portálon ugyanaz a jelszava, akkor most érdemes mindenhova újat és mást választania**, mert még nem lehet azt sem tudni, a támadók megszereztek-e innen valamilyen adatot. A módszer mindenesetre jó nagy feltűnést keltett, és nem zárható ki, hogy más, nagy látogatottságú oldalak (Paypal, MSN, Ebay, Facebook) kapcsán nem fogunk majd vele újra találkozni. **Akár a DNS rekordok esetleges jogosulatlan módosítás elleni hatékonyabb monitorozása is hasznos lehetne** a cégek számára.

Egy apró érdekesség a végére: az egyik olvasó egy olyan képernyőképet is beküldött, amikor **a Google keresőbe begépelve a twitter szót, az már a feltöréssel kapcsolatos indexelt találattal szerepelt a legelső** helyen.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben
- Majdnem mindenki átverhető adathalászattal
- "Szósölmédia" és nyaralás
- Küldj pénzt! - Az elveszett poggyász sztori
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1606669

Kommentek:

Nincsenek hozzászólások.

Béták reggelire

2009.12.22. 19:31 | Csizmazia István [Rambo] | 19 komment

Címkék: linux beta macintosh karácsony xmas nod32 hellókarácsony

Megérkezett a **Macintosh és a Linux desktop változat bétája a NOD32 programból**. Hogy játszhatunk vele egy kicsit, az egy dolog, de a másik kérdés, hogy helyén kezeljük az ezzel kapcsolatos dolgokat, igen lényeges.

A **Linuxban a másik remek dolog az ingyenesség mellett az, hogy mentesül a felhasználó a temérdek vírustól**, kártevőtől. Az OS X - amely nem Linux, de szintén Unix alapokra építkezik - **hasonlóan hárítja felépítéséből adódóan a vírusokat, férgeket**. Akkor ezek szerint ezekre a rendszerekre egyáltalén nincsenek vírusok? De igen, de csak inkább PoC, azaz Proof of Concept, azaz néhány kísérleti demonstrációs céllal írt kártevő. **Ezek száma azonban igen csekély, pár száz körüli darabszám áll szemben a Windowst hegyomlás-szerűen ostromló tízmillió feletti** kórokozóval.

A legtöbb felhasználó szerint az internetes kártevők nem veszélyeztetik a Macintosh és Linux operációs rendszereket. Valójában azonban az eddig biztonságosnak hitt platformok is sebezhetőek, terjedésükkel pedig egyre nő a kifejezetten ezekre az operációs rendszerekre írt kártevők száma is. Sok windowsos károkozó ráadásul, még ha nem is okoz károkat a Maces, illetve a Linuxos gépeken, ezekről a munkaállomásokról könnyedén továbbterjedhet a Windows alapú számítógépekre, így gyorsítva meg a vírusok terjedését. **Magyarról magyarra fordítva: Linuxon a Samba share-s dolgokat azért időnként nem árt átnézni nem (csak) magunk miatt is**.

Kell-e mégis védelmi program? Mikor kezdtek megjelenni a felhasználókat átverő első trójai programok, talán néhány embernek megfordult a fejében. Kicsit **ambivalens az érzés, hiszen a trójai elsősorban az embert, a felhasználót téveszti meg**, és ha az úgy gondolja, hogy admin joggal telepít valami szemetet, ettől semmi sem tarthatja vissza. Másrészt mivel egyre több ilyen (főleg Maces) próbálkozás van, jó lenne ha trójai, kémprogram és **rootkit fronton valami mégis figyelne**. Megszűnt ugyanis csak a profik, a számítógépes szakértők használnak Macet, Linuxot világ. **Divat, kultikus tárgy lett a Macbook**, és a Linuxos világban sem egy nagy etwas már egy SuSE vagy Ubuntu telepítése, nem kell hozzá diploma.

Senki nem szeretne tudtán kívül egy botnet része lenni. Eddig is hasznos volt, ha valaki **hetente megnézte a rendszerét a chkrootkit és/vagy rkhunter keresőjével**, de várhatóan **a Mac növekvő piaci tortaszelete miatt növekedni fog a támadások, kártevők száma**. Akármilyen hihetetlen ez sokak számára, **nem a víruskereső vállalatok írják a kártevőket**. Néha elhangzik ilyen alaptalan feltételezés is, igazságszerint egy vírusvédelmi program fejlesztése folyamatos impossible mission munka éppen elég odafigyelést, ellenőrzést kíván, **a kártevők variánsainak óriási száma éppen elég feladatot ad a szakembereknek**, semhogy saját bajaikat így tetéznék.

Az **alternatív platformok egyelőre sokkal szűkebb piacok lesznek**, mint a Windows világa, de azért az utóbbi egy év történései alapján sokakat megnyugtatna, ha nem látatlanban, hanem egy alapos ellenőrzés után dőlhetnének elégedetten hanyatt a karosszékükben. Egyre több hétköznapi, átlagfelhasználó életét könnyítheti meg, ha a támadások ellen valamiféle védelmet még

Akik kísérletezni is szeretnek, azok nézegethetik a bétát, ami csak béta. **les rendszerre csak saját felelősségre tegyük fel**. Saját tapasztalat alapján **a Mac verzió problémamentesen települ** (kisebb font keveredést leszámítva). Az első Linux béta változat néhány gépen a hálózati beállítások problémája miatt jelentősen lelassította gépet (ez a gond nálunk is jelentkezett) - míg a számítógépek döntő többségében az is rendben működött, **az Eicar teszfájlt, éles kártevőket szépen észlelte**. A Macre és a Linuxra kifejlesztett verziók **támogatják a 32 és bites processzorokat**, emellett többek között tartalmazzák a külső adathordozók ellenőrzésének lehetőségét is. A most bemutatott, ingyenesen letölthető béta változatok után **a végleges verziók várhatóan 2010 áprilisában lesznek elérhetőek** - addig még sok egyes és nulla lefolyik a fejlesztők és tesztelők ethernet csatlakozóin.

Mindazonáltal minden kedves olvasónknak Kellemes Karácsonyt Kívánunk

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1615613

ommentek:

atko 2009.12.22. 20:04:34

Az ... oldal cikke után azonnal feltettem és kipróbáltam (mandriva 2010.0) vboxban, majd a problémamentesség után élesben is. (a vboxban futtatok egy "tükör rendszert" amin az új dolgokat kipróbálom, mert egyszer már megégettem magam) Gondom,

kártevőm nincs. :-) Munkahelyem miatt van wines licencem remélhetőleg átválthatom a Linux verzióra és akkor még "sokba se kerül". Ha nem akkor majd az ár ismeretében döntök.

Poll 2009.12.23. 00:13:33

"Az OS X - amely nem Linux, de szintén Unix alapokra építkezik - hasonlóan hárítja felépítéséből adódóan a vírusokat, férgeket. "

Felejtsük már el ezt az orbitális marhaságot. Se az osx se a linux nem véd felépitéséből adódóan jobban a virusoktól, trójaiktól, mint a win. Egyedül az elterjedtségük ami miatt kevesebb a kártékony kód ezekre a rendszerekre. Pontosan a PoC kódok mutatják, hogy felépitésileg pont ugyanolyan sebezhetőek, mint a win, simán lehet teljesen elrejtőző rootkitet rakni ezekre, akárcsak winre. Ugyanúgy teli vannak hibákkal amiket patchelni kell stb-stb.

Rwindx 2009.12.23. 00:5□:53

Hmm, én maradok egyelőre a ClamAV-nál. Mondjuk én smtp szerveren használom, nem desktopon futtatom. Ha valaki megbízható forrásból telepít (mondjuk csak a disztribből) mindent, valamint van egy normális tűzfala, akkor sok meglepetés nem érheti Linux alatt (desktopon). Ha meg összevissza, akkor meg kösse fel a gatyáját egyéb okokból is...

A Nodhoz sokat nem tudok hozzászólni, eléggé megkoptak az emlékeim dualbootos korszakomról. A még korábbi dosos emlékeimet elővéve meg még talán nem is létezett Nod :)

Rambo, az elmúlt 15 évben nem igazán foglalkoztam vírusokkal, de jól érzem hogy újra kezdenek bonyolultabbak/okosabbak lenni?

A DOS időszakban fantasztikus vírusok készültek (szoftverfejlesztői, dekódolói szemmel), de a később megjelent Windowsos vírusok hihetetlen primitivnek tűntek. Mintha ez az utóbbi néhány évben változást mutatna, gondolok itt a terjedési és rejtőzködési technikákra. Még 3-4 éve is elég volt belenézni a registrybe hogy elég jó százalékkal el lehessen dönteni hogy a Windows fertőzött-e. Ma már ebben nem bízok túlzottan.

twollah □bRo□En hOPe, sUppLeX · http://freewaresoftwarenews.blogspot.com/ 2009.12.23. 04:32:05

Ez itt a reklam helye.

Kiirhatta volna a kedves blogolo.

Romkocsmák homályában merengő főállású troll 2009.12.23. 07:57:51

A Linuxban az a remek dolog, hogy nem tudok rajta se játszani, se dolgozni, viszont legalább vírus sincs rá, így biztonságosan tudom használni a gépet a nagy büdös semmire :)))

midnight coder 2009.12.23. 08:04:02

Nos, linuxra valóban kevesebb a vírus, ennek alapvetően két oka van:
1. 1% körüli elterjedtségű oprendszerre jóval kevésbé éri meg bármilyen szoftvert - beleértve vírust is - írni mint 9x százalék körülire. A vírusok már rég nem arról szólnak hogy a hülye Pistike ír egyet szórakozásból, hanem általában határozott céllal - Pl. botnet - készülnek. Így aztán nagyon nem mindegy mi a cél.
2. Olyan hogy linux valójában nincs. Linux disztribek vannak amik radikálisan különböznek egymástól a program szempontjából. Azaz az 1% linux valójában legalább 10 különféle nagyobb disztrib között oszlik meg, amik ráadásul többféle verzióban léteznek. Ez persze a szoftverfejlesztők életét is megkeseríti - ez az egyik oka annak hogy igen kevés a desktop linuxos program, szinte csak openszorszak vannak.

Ami a MacOS-es részét illeti a dolognak, az tényleg vicc. A felépítéséből adódóan biztonságos MacOS a hackerkonferenciák állandó sztárja, a feltöréses versenyek favoritja. :-))

lánczi sixx... izé... suxx 2009.12.23. 08:20:13

@Sün! balázs: ez így, ebben a formában kapitális baromság! Ahogy az is, hogy a linux mindenre megoldás...

Band□r Kandi 2009.12.23. 0□:23:11

ClamAV-t használok, teljesen rendben van és ingyenes (de az Avast! és AVG is), fizetős cucc ezután sem lesz gépeken.

Band□r Kandi 2009.12.23. 0□:24:15

@Sün! balázs: Én ezen dolgozom, ezen játszom, úgyhogy ez meg is dőlt...

midnight coder 2009.12.23. 0□:43:5□

@Krumpl Izsák: Attól függ mit. A flash-es játékok jól elmennek rajta, és van pár openszorsz játék aminek a színvonala kb. ugyanazon a szinten mozog. Meg van néhány windowsos játék ami egész jól elmegy wine alatt. Plusz egyéb emulátorok: dosbox, vice, fuse...

Ami a munkát illeti, van pár javás fejlesztőkörnyezet, unstable lazarus, méginkább unstable mono, és van pár web alapú szutyok.

Csizmazia István [Rambo] □http:□a□tivirus.blog.hu 2009.12.23. 09:05:5□

Szia atko!

Akkor tehát Mandriván is megy. A glibc különböző útvonala, meg egyéb hasonló disztribúciós különbségek miatt sok mindent kell figyelni a fejlesztőknek.

Csizmazia István [Rambo] □http:□a□tivirus.blog.hu 2009.12.23. 09:1□:3□

Szia Poli!

A Mac OS X a Mach kernelen és BSD alapokra épül. A Mac és a Linux sem támadhatatlan, ezt senki nem állította. De a jogosultságok, a fájlrendszer működése sokkal jobb adottságokkal rendelkeznek:

- gondolj a Windows reészeként érkező Outlook Express működésére, rákattintasz egy levélmellékletre, és az hip-hop lefut, nem horror?

- a Windows alapból elrejti az ismert (vagy kettős) fájlkiterjesztéseket

- a Microsoft Office jó sok éven át automatikusan lefutó makrókkal volt megáldva

- az Autorun dolog meg szerintem valóságos Isten csapása

Ez csak néhány dolog, Abban maximálisan egyetértünk, hogy egy OS elterjedtsége a legszorosabb kapcsolatban áll az arra a rendszerre írt kártevők számával. Ezt írtam éne is "de várhatóan a Mac növekvő piaci tortaszelete miatt növekedni fog a támadások, kártevők száma"

Csizmazia István [Rambo] □http:□a□tivirus.blog.hu 2009.12.23. 09:23:3□

Szia Rwindx!

A ClamAV az egyik felismerésben leggyengébben teljesítő program.

Biztonság meg nem létezik, csak annak az illúziója, illetve kockázat kezelés van. Azt, hogy Linux alatt nincs rootkited, hiheted. Biztos akkor lehetsz benne, ha ellenőrzöd, például Rkhunterrel, Chkrootkittel. Ezekkel is csak az ISMERT rootkiteket, meg gyanús logolásokat, stb. nézed. Ha például rendszergazdaként szervereket üzelemtetnél, kevés lenne a "Linux biztonságos, semmi dolgom énnékem" szlogen. Ettől függetlenül a Linux desktopra átültetettet ismerőseim mind fellégeztek vírus kérdésben.

A túlságosan nagy Linuxos tortaszelet miatt viszont úgy látom, egyelőre nem kell aggódjunk, kevesen használnak ilyet, legjobban talán a Wines játékok miatt :-)

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2009.12.23. 09:2□:5□

Szia twollah / bRoKEn hOPe, sUppLeX!

Ki van írva, hol dolgozom, hol itt a meglepetés? Ott áll a névjegy dobozomban is.

Akit meg érdekel a progi, lehet hogy pont innen szerez a fejlesztésről tudomást. Szerintem ha valaki például az Applenél dolgozik, és van mondanivalója az új iPhoneról, megírhatja a blogjában. Ez itt dettó ugyanaz.

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2009.12.23. 09:34:52

Szia Sün! balázs!

Nem tudom pontosan mire akarnád használni a Linuxodat, de ha nem SAP, AutoCAD, Windows játékok, Macromedia programok futtatására, szerintem tökéletesen használható minden egyéb célra.

Gondolom most desktop oldalról közelítünk -tehát a webszerverek LAMP számbeli fölénye most nem szempont.

Évek óta ez a fő OS nálam, de a víruslaborokban sincs másként. A Wines gépet vagy virtuális cuccot csak akkor indítom, ha futtatni, tesztelni akarom rajta a kártevőt.

És átlagfelhasználó számára sem rossz, például ha választhatnék, hogy a te és az én adómból fenrtartott bürokrácia pl. ingyenes Ubuntun ingyenes Open Office-szal működjön, vagy milliárdokért MS-sel, az előbbire voksolnék.De itt egy link, nálunk gazdagabb országokban már sok helyen léptek ilyesmit:
wiki.hup.hu/index.php/Szabad_szoftverek_t%C3%A9rnyer%C3%A9se

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2009.12.23. 09:39:5□

Szia midnight coder!

Szinte mindennel egyetértek veled. Az elterjedtség jelntős mértékű változása meg fogja hozni a Maces kártevők számának növekedését. A rosszfiúk úgy gondolhatják, akinek van anniy pénze, hogy szor kettőért vesz gépet, annak a bankszámlája sem lehet üres, érdemes lesz kémprogramot fejleszteni oda is.

A Mac jelenleg sokkal biztonságosabb, mint egy Win, de valóban, szó nincs arról hogy támadhatatlan lenne, a hacker versenyeken elsőként teszi fel a kezét. Azt kellene a mac usereknek megérteni, hogy nincs igazuk, ha azt gondolják, pusztán az OS X miatt ők eleve és örökre védettek.

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2009.12.23. 09:43:21

Szia lánczi sixx... izé... suxx

Ha levonjuk a szélsősége indulatokat, flamewarokat, minden operációs rendszernek meg van a létjogosultsága, és a feladat dönti el mikor, melyiket kell használni.

Ahol viszont van mozgástér, az a nem játékfüggő átlag otthoni user, aki akár egy Suse vagy Mandriva alatt is mindent (Open Office, VLC, Opera, Thunderbird, Inkscape, Skype, Pidgin,. stb.) szépen tudna használni ingyen, lopott Windows licenc és vírushegyek nélkül. Nekik lenne a legjobb áttérni.

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2009.12.23. 09:4□:04

Szia Krumpl Izsák!

Sokféle szempontból választhat az ember programot magának. Ha az ingyenesség a te fő szempontod, és akkor sem a ClamAV-t ajánlanám, mert az eredményei nagyon szerények. Ha a biztonságról van szó, nálam biztosan nem ez lenne a döntő érv.

Csizmazia István [Rambo] □http:□□antivirus.blog.hu 2010.01.0□. 1□:1□:2□

Ma frissült a letölthető béta a Macintosh-hoz:
www.eset.eu/download/beta

Changelog:
www.eset.eu/support/changelog-eset-nod32-antivirus-4-for-max-os-x

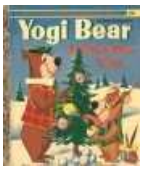
Kellemes Karácsonyi Ünnepeket

2009.12.23. 11:02 | Csizmazia István [Rambo] | 2 komment

Címkék: karácsony xmas hellókarácsony

A tegnapi poszt végén kicsit eltűnt a jókívánság, amely hitünk szerint egy külön posztot is megérdemel, Íme. Aki pedig még ajándékok után futkos, annak a tavalyi bejegyzés adhat egy kis segítséget ;-)

Boldog Karácsonyt és sikerekben gazdag Új Évet kívánunk az oldal minden látogatójának!



Ajánlott bejegyzések:

- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1617499

Kommentek:

Pikk 2009.12.25. 13:34:50

Szia István !

Kellemes Ünnepeket kívánok innen is :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.30. 14:33:55

Szia Pikk!

Köszönöm szépen, neked is hasonló jókat!

Utolsó előtti bejegyzés 2009.

2009.12.30. 16:10 | Csizmazia István [Rambo] | 1 komment

Címkék: összegzés 2009 statatisztika

A **szilveszteri poszt előtt ez az utolsó komolyabb bejegyzés**. Jelszó cserékre bíztatjuk a nagyérdeműt, valamint **visszatekintünk kicsit**, amolyan önjelölt statisztikusként tetszelgünk, sőt **néhány 2010-es biztonsági jóslatatot is belinkelünk**, hogy majd egy év múlva jól ellenőrizhessük.

Vége az évnek, már alig egy nap van hátra. 152 idei posztot hagyunk a hátunk mögött, az ESET **megszerezte az 59. Virus Bulletin 100% díját**, ez éppen most decemberben történt Windows 7 platformon. A blogíró futással teljesített távja az idén összesítve 907 km-re sikeredett. És bár ahogy a "nem az iskolának, hanem az életnek tanulunk" mintájára "nem az Index címlapnak blogolunk", a kétéves évfordulónkon már nézegettük mi volt a pálya böngésző fronton a látógatóinknál, és **mik voltak a nagyobb érdeklődésre számot tartó idei bejegyzések**.

Itt az év vége, mindenki szorgosan készítgesse külső adathordozókra a mentéseit, és szokásos menetrend szerint itt az ideje új, hosszabb és furmányosabb jelszavakra cserélni a régieket.

Ezekből **érdemes néhány fokkal szofisztikáltabb színvonalú jelszavakat választani**, mint amiket a Twitteren már nem engedélyeznek.

Mi várható 2010-ben? Amellett, hogy emeljük poharunkat húsz forintról huszonötre, olvashatjuk Howard Smith kiberbiztonsági szakértő jóslatát, mi várható a Macintoshokon jövőre vagy hogy Kaspersky bácsi mit vél látni az üveggömbjébe tekintve. De retrospektív kiránduláskén megnézhetjük azt is, hogy a tavalyi jóslatokból végül mi vált valóra és mi az, ami nem.

De nem csak az évnek lett vége, Dr. Sör Kálmán sem fog többé üzemszerűen Boáfka Ottokárral és Kovács Brezsnyevkével meetingezni, gyászolhatunk. A magunk részéről viszont töretlenül folytatjuk a számítógépes kártevők (és a kevésbé foglalkoztatott és spamküldözgető bébiszitterek) elleni biztonsági őrjáratunkat az antivirus.blog hasábjain.

Holnap pedig az idei utolsó, nem kicsit másfélkegyelmű bejegyzésünkkel **búcsúztatjuk majd az óévet**.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1632225

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.12.30. 16:38:05

Közben kijött egy McAfee-s jóslat is:
nonstopuzlet.hu/mcafee-mar-nem-a-microsoft-a-celpont-20091230.html

BÚÉK 2010!

2009.12.31. 12:00 | Csizmazia István [Rambo] | Szólj hozzá!

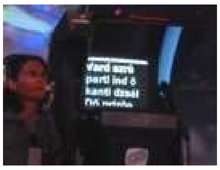
Címkék: móka szilveszter buék 2010

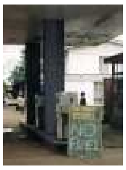
Az esztendő utolsó napján igyekszünk kellemes perceket szerezve kissé elrugaszkodni a pedáns hétköznapoktól. Jöjjön hát a Szilveszteri Szuperbola!

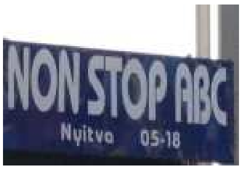
Az alábbi képekkel és a lap alján lévő videókkal **megköszönjük az egész évi figyelmet, és nagyon Boldog, Sikeres, Gazdag Új Évet Kívánunk!**

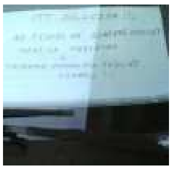

AGYAT
AGYAT AKARUNK

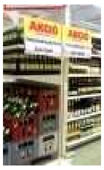

SCISSORS BEAT PAPER






NON STOP ABC
Nyitva 05-18






KEDVES
VÁSÁRLÓINK!

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek

- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/1632796

Kommentek:

Nincsenek hozzászólások.