Beköszöntő

2007.09.17. 20:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: blog beköszöntő antivirus vírusvédelem

A számítógépes biztonsággal még **Commodore 64-es** koromban találkoztam először, és nem igazán voltam érte hálás a sorsnak. Sikerült egy másolásvédelem miatt a 1541-es típusú lemezegységet használhatatlanná tennem. Szétszedés után aztán kiderült, az olvasófej került olyan szélső helyzetbe, hogy csak kézzel lehetett visszaállítani.

A nagy izgalom – hiszen a bécsi út másik végéről nagy nehezen szerzett jószágról volt szó - és az összeszerelés után aztán jött a boldogság: mégsem ment tönkre, újra rendesen működik. Talán ez volt az első számítógépes tapasztalatom arról, hogy **vannak, akik nem becsületes eszközökkel élnek**, akik pusztítani szeretnek és hogy nem árt az óvatosság.

Pár évvel később programozóként érdekelni kezdett, vajon miért potyognak le a karakterek a képernyő aljára. És vajon mitől indul újra a PC péntek 13-án? Az évek során az **F-Secure** és **Kaspersky** magyarországi képviseletén dolgozhattam vírusvédelmi tanácsadóként, bábáskodhattam a **Vírus Híradó** megszületésénél, melynek főszerkesztője lehettem, a **PC World Magazin** online szerkesztőjeként tényked hettem, és a **VirusBuster** víruslaboratóriumában is dolgoztam. Bár jelenleg a **NOD32** magyarországi képviseletén dolgozom, és a példákat sok esetben ezzel a víruskeresővel fogom majd bemutatni, szeretném a bejegyzéseimet elfogulatlan szellemben publikálni.

A napi hírek, a történések tengerében egyre jelentősebb helyet foglalnak el életünkben a webnaplók, a blogok. Sok olyan érdekes ember és szervezet vezet ilyet, akinek van mondanivalója, megfigyelése, felismerése, izgalmas tapasztalata, és sok ilyen naplónak vagyok rendszertelenül, de azért visszatérő olvasója. A számítógépes biztonságot is „elérte a végzet”, számos webnapló méltán tarthat számot érdeklődésünkre, hogy csak az egyik leghíresebbet említsem: az F-Secure weblogja igazi csemege a szakmabelieknek. Induljon hát az Antivírus Blog, ahol igyekszem majd minden érdekes külföldi és hazai biztonsági témáról hírt, képet és véleményt nyújtani.

És hogy legyen valami mottó is: **"A gravitáció nemismerete nem mentesít a zuhanás alól..."**

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/168737

Kommentek:

Nincsenek hozzászólások.

Stoned.Angelina vírus a noteszgépeken

2007.09.18. 13:11 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: notebook vírus németország angelina stoned medion fertőzött

Nemrég a Virus Bulletin hasábjain olvashattunk arról, hogy a németországi **Medion** gyártó Németországba és Dániába küldendő noteszgépein egy 1994-es régi vírust találtak.

A **MD96290** típusjelű notebookok előtelepített Windows Vista Home Premiummal és Bullguard antivírussal voltak felszerelve. A jelentések szerint a bootvírussal fertőzött gépek száma mintegy 10 ezer és 100 ezer közé tehető. Az Aldi áruház láncban is kapható gépekkel kapcsolatban a német Heise Online, valamint maga a Medion cég is részletes közleményt, és mentesítési útmutatót, letölthető mentesítő programot adott közre.

Amint tudomást szereztünk a dologról, megpróbáltunk szerezni egy ilyen gépet. Ausztriában a Hofer Notebook üzletben sajnos már kifogyott, és kitartó telefonálgatás ellenére Ausztiában már egyáltalán nem lehetett hozzájutni.

A Stoned.Angelina a merevlemezek Master Boot Sectorába költözött bele, a 13h interrupt eltérítésével. Akkori munkahelyemen a vírus felbukkanásával - mivel a víruskeresők csak 1-2 havonta frissítették az adatbázisaikat - sikerült egy pár napos kalamajkát okozni, míg megszabadultunk tőle. A vírus hajlékony lemezeken terjedt, amire most biztosan nem képes, hiszen ezekben a laptopokban nincs is flop meghajtó. **"Ez egy intő jel arra, hogy a régebbi vírusok sosem halnak ki teljesen"** - nyilatkozta az eset kapcsán John Hawes, a Viru Bulletin műszaki tanácsadója.

A Medion weboldaláról letölthető FixMD96290.exe program segítségével el lehet távolítani a kártevőt a fertőzött noteszgépről.

Bár viszonylag ritka esemény, hogy egy új hardverrel együtt egy kártevő bukkanjon fel, az ilyen esetek mégsem teljesen példanélküliek. (Bár az ember a józan ész alapján inkább régi floppy lemezes, DAT kazettás, vagy sok éves CD/DVD lemezes mentések visszaolvasásánál lenne résen.) Emlékezetes, hogy az év elején a TomTom autós navigációs rendszer került forgalomba fertőzötten, tavaly októberben pedig vírusos iPod lejátszók bukkantak fel, és USB háttértárak is kerültek már fertőzötten piacra. Szóval nem árt állandóan résen lenni.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- 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/169338

Kommentek:

Nincsenek hozzászólások.

Kipróbáltuk rovat: Rootkit a Sony USB kulcson

2007.09.19. 07:51 | Csizmazia István [Rambo] | 2 komment

Címkék: usb sony pendrive kulcs kipróbáltuk rootkit kártevő usm

Úgy tűnik, van aki semmiből nem tanul. Alig másfél évvel a Sony a BMG eset után ismét magára irányította a közfigyelmet a Microvault USM-F pendrive-sorozatával.

Ez év augusztus 27-én igen érdekes felfedezésről számolt be az F-Secure weblogja. Kiderült, hogy a Sony MicroVault USM 256, illetve 512 FL jelű, ujjlenyomat azonosításra képes flash meghajtója titokban rootkitet telepít a gépekre, és az F-Secure kutatói szerint az eszköz kínai fejlesztésű szoftvere működése közben rejtett könyvtárat hoz létre.

Az eset azért elképesztő, mert úgy gondoltuk, aki korábban már ilyen hatalmas tanulópénzt volt kénytelen elhibázott lépése miatt kifizetni, az nem követi el újra ugyanazt. A Sony cég először cáfolta az értesülést, később pedig nem kommentálta az F-Secure több, mint egy hónapja tett felfedezését, viszont amikor az FL után az USM F jelű termékében is azonosították a rootkitet, hivatalos weblapján elérhetetlenné tette a két eszközhöz tartozó meghajtó programok (driverek) letöltését.

Kíváncsiak lettünk a dologra, és vásárolni indultunk a magyarországi webáruházakba, de első körben nem találtunk rá egyik típusra sem. A Vatera és a német Ebay sem hozott szerencsét. Ezért inkább a meghajtó programcsomagra fókuszáltunk, és nem hiába. Az FL típusra egy drivereket kínáló magyar oldalon, a drivers.hu-n akadtunk rá, míg az F változathoz szükséges programot éppen a Sony oldaláról sikerült letölteni. Ehhez kitartóan kellett próbálkoznunk, és végül találtunk olyan országot – Indiát - , ahol Isten malmai lassabban őrölnek, és az ideiglenes visszavonás ellenére sem távolították még el a programot a helyi Sony honlapról. Igaz a csapnivaló sávszélesség miatt majd félóráig tartott a 28 MB méretű állomány letöltése.

A nagy telepítőcsomagokra a vírusirtó nem jelzett, a telepítés viszont az USB eszközök fizikai megléte nélkül nem hajtható végre. Kis nyomozgatás után aztán a BioSecure\fg.exe (644,608 byte) állományra terelődött a gyanúnk, ez mindkét telepítő csomagnak része. A ProcessMonitorral kísért próbafuttatás során látszik, hogy létrehoz egy új meghajtó állományt C:\WINDOWS\SYSTEM32\DRIVERS\FG.SYS néven (25,043 byte), ezt a NOD32 sikeresen észleli, beállításától függően haladéktalanul törli, illetve karanténba helyezi.

Az USM512FL csomag által létrehozott FG.SYS eredménye

Az eszköz beszerzésére irányuló ismételt kísérletünket pár nap után végül siker koronázta, a Pixmania webáruházból sikerült a SONY MicroVault USM128C típust megvásárolni. A telepítő CD lemezen a már említett BioSecure könyvtár - legalábbis a dátum szerint - 2003 szeptemberi dátummal rendelkező állományokat tartalmaz. Itt is megtalálható a BioSecure\fg.exe, ám a hossza különböző. Egy kis kutatással felfedezhető, hogy UPX (Ultimate Packer for eXecutables) segítségével tömörítették 388,608 byte méretűre. A NOD32 valós idejű védelme ettől függetlenül szépen érzékeli, és blokkolja. A kikapcsolt vírusvédelem mellett itt is keletkezik egy

C:\WINDOWS\SYSTEM32\DRIVERS\FG.SYS állomány, azonban ez kódjában több helyen is eltér az előző változattól.

Bedobjuk őt is a most már 19 nyelven beszélő VirusTotal-ba, és ami a meglepetés: az F-Secure az FG.EXE állományokat rendre szépen észleli, míg az FG.SYS fájlokat nem érzékeli :-O

Az USM128C csomag által létrehozott FG.SYS eredménye

Kísérletünkben bátran írtunk a konkrétumokról, mert a fizikai eszköz hiányában az említett program futtatásával nem kockáztatjuk a rootkit a rendszerbe való feltelepülését.

A teljes telepítésnél azonban az ilyen rejtett könyvtáron alapuló megoldások az előző BMG esethez kísértetiesen hasonló helyzetet okozhatnak. A rejtett könyvtárba másolt állományok nem csak a felhasználók számára, hanem számos vírusvédelmi program előtt is észrevétlen marad, és így szinte „megágyaznak” egy láthatatlan vírusnak.

A kártevők szerzői hamar kihasználják az ilyen kényes információt, és pontosan ebbe a mappába fogják telepíteni „láthatatlan” vírusaikat, kémprogramjaikat. Ezzel a gyártó olyan veszélynek teszi ki a gyanútlan felhasználókat, ami szerintünk nem megengedhető.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/169633

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2008.04.01. 14:25:44

Kalózkodáson kapták a Sony BMG-t
index.hu/tech/jog/sony010408/

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.17. 10:07:12

Ahogy a korlátozások útján halad az Apple is, a végén már csak Linuxot lesz érdemes használni :-O
www.origo.hu/techbazis/hightech/20090316-titokzatos-chipet-talaltak-a-beszelo-ipodban.html

Hamis riasztás a MASA-tól

2007.09.20. 14:14 | Csizmazia István [Rambo] | 3 komment

Címkék: url nod32 antivírus eset antivirus suspicious gyanú mcafee siteadvisor masa

Az egész egy szép őszi napon kezdődött, mikor is a PC World fórumát olvasgatva egy érdekes bejegyzést találtam egy tegnap előtti hozzászólásban. A **Stephan** nevű látogató azt firtatta , hogy az ingyeneses letölthető MASA (McAfee SiteAdvisor) vajon miért jelöli gyanúsnak a **NOD32 programot fejlesztő ESET honlapát**. A www.eset.com URL a hozzászólás szerint az alábbi indoklással szerepelt a gyanús listán:

- Phishing or other scams
- Browser exploit

Mosó masa mosodája...

Magyarul állítólagos adathalász vagy más csalásssal összefüggő gyanú áll fent, illetve a böngésző kliensen keresztül sebezhetőséget használna ki. A dolog teljesen nonszensz, de gondoltam utánajárok.

A további hozzászólások aztán az összeesküvés elméletek irányába ;-) kanyarodott (így büntetik egymást a versenytársak, stb.), amit én személy szerint nem tartok valószínűnek. Az igaz, hogy a konkurensek közt van egyfajta harc a kereskedelem színterén, de a háttérben a technikai emberkéknél, például a víruslaboratóriumok között nagyon sok baráti, korrekt emberi és szakmai kapcsolat létezik, aminek én például nagyon örülök.

Nem vagyok MASA felhasználó - más progamokkal, illetve pluginekkel oldom inkább meg ezt: pl. Finjan, Netcraft Toolbar, stb. -, sőt az időnként megjelenő teszteredményeit látva nem is lelkesedtem érte, de azért most egy próbára letöltöttem a McAfee ingyenes programját.

A www.eset.com **a post írásakor már teljesen tisztának** látszik, úgy tűnik felvették egymással a kapcsolatot és rövid úton elintézést nyert a dolog.

A nagyobb meglepetés akkor ért, amikor a magyar oldalt ellenőriztem, most meg erre jelez gyanút, trójai letöltő oldalnak aposzrofálva a webhelyet :-O

A sárga felkiáltójellel ékesített, a McAfee skála szerinti hármas erősségű figyelmeztetés azt írja, hogy az "ne98hust.exe" - ami a Windows 95/98 változatra készült NOD32 2.7 telepítőcsomagja - állítólag gyanús Iframe.b trójait tartalmaz. **A hamis riasztás miatt** most mi vettük fel a kapcsolatot a NAI-val, és reméljük, hogy pár napon belül ez is a megoldott ügyek dossziéjába vándorolhat.

Azért, hogy a cikk ne kizárólag a MASA-ra legyen kihegyezve, megmutatjuk, hogy más hasonló kiegészítő, például a Robot Genius RGGuard is szokott tévedni.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/171373

Kommentek:

zoltan galantai phd · http://mono.eik.bme.hu/~galantai 2007.09.20. 22:16:30

profi a blog, gratulálok:-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.25. 20:00:20

Köszi szépen :-)

Ati82 2007.10.30. 12:27:19

Tényleg nagyon jó a bejegyzés és tanulságos. köszönjük. :D
Ennek a beállításnak van értelme? Vagy mi értelme van?
Azon kívül, hogy a nod32 ezek beállítások után agresszivebb lesz és csöndben lesz...
Itt a beállítási link: www.wilderssecurity.com/showthread.php?s=45ae2753e90688b4c0933062802645cf&t=37509&pp=25

A hónap markában

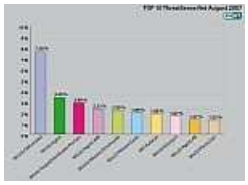
2007.09.21. 08:57 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika toplista nod32 eset kártevők vírusok

Minden valamirevaló vírusirtó cég rendre közzéteszi negyedéves, vagy havi fertőzési statisztikáit. Némely lista kizárólag levelezés szűrésen alapuló adatokat tartalmaz, ami bár e szegmens szempontjából érdekes, nem fedi le a havi vírus statisztika egészét, hiszen a weboldalakon, adathordozókon terjedő fertőzéseket nem tartalmazza. Az ESET havi riportja ezzel szemben **a ThreatSense.Net által gyűjtött adatokra** épül. A statisztika különlegessége, hogy nem pusztán az elektronikus levelekkel terjedő vírusokról tartalmaz információkat, hanem azokat a kórokozókat is figyelembe veszi, melyek más úton – például HTTP protokollon keresztül – támadják meg a számítógépeket.

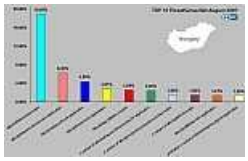
A ThreatSense.Net rendszer sematikus működési ábrája

A korai vírus-előrejelző rendszerként működő megoldás a gyanúsnak ítélt kódokból anonim mintát küld az Eset víruslaboratóriumába, ahol a szakemberek így egyrészt ki tudják dolgozni a kórokozók elleni hatékony védelmet, másrészt hasznos információkat kapnak a kutatók a különböző fertőzések terjedéséről. A NOD32 által védett számítógépeket érő fenyegetésekről **naponta mintegy 80 millió jelentés érkezik** a ThreatSense.Net rendszerbe.



2007. augusztus a világban

Most először kaptunk az ESET-től olyan adatokat, amelyek az eddigi globális havi számok mellett **külön csak Magyarországra vonatkozó számokat**, ami az összes begyűjtött adat 2.1 százaléka.



2007. augusztusi állapotok hazánkban

A különbségek jól érzékelhetőek, bár éppen a listavezető (Win32/Obfuscated trojan) azonos, viszont a magyar első helyezés közel húsz százalékos, ugyanez a másik listán csak 8. Az is érdekes, hogy az animált kurzoros Win32/TrojanDownloader.Ani.Gen még mindig a nemzetközi lista harmadik helyén található, miközben a magyar adatok közt már csak a hetedik. Ez az a trójai, amely a **Windowsnak az animált kurzorfájlok** (.ani) kezelésével kapcsolatos, egy márciusban felfedezett kritikus sebezhetőségét támadja. A felfedezett hiba kihasználásával távoli kódfuttatás valósítható meg az áldozat rendszerén, és áprilisban még vele találkozhattunk a lista tetején.

A teljes magyar TOP20 táblazatot közreadjuk

Remélhetőleg máskor is kapunk majd ilyesmiket. Közben próbáltam visszafelé is kutakodni, és három évet sikerült hátrálnom: **2004. augusztusát** tudtam előhúzni a múltból, erre is érdemes lesz egy pillantást vetni.

A legjelentősebb különbség. hogy napjainkhoz képest **a "retro" 10-es lista** helyein mindössze négyféle kártevő variánsai osztoznak, és a jelenünket annyira megkeserítő kém- és reklámprogramok helyett még számos levelezéssel terjedő féreg tudott ranglistás lenni. Igaz persze, hogy a különböző Bagle variánsok már próbáltak különböző TCP portokon hátsóajtót nyitni a gépekre, illetve a Zafi és a MyDoom pedig szolgáltatásmegtagadási (DoS), valamint elosztott szolgáltatásmegtagadási (DDoS) támadásokat volt képes végrehajtani.

S hogy miért is érdemes néha visszafelé is nézelődni? Külön érdekesség, amikor azt vizsgálják, **az antivírus szoftverek vajon észlelik-e a még ismeretlen vírusokat**. Erre a célra a víruskereső szoftverek régebbi verzióit használják, és azt igyekeznek kideríteni, hogyan azonosítják a később megjelent vírusokat. A 2006 elején elvégzett CheckVir tesztben erről a furcsa versenyről olvashatunk részletesen.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/172100

Kommentek:

Nincsenek hozzászólások.

Fantázia és ötlet a reklámokban

2007.09.22. 20:40 | Csizmazia István [Rambo] | Szólj hozzá!

Biztos sokan emlékeznek, melyik vírusirtó szerepelt 2006-ban a buszok hátoldalán matrica formájában, majd néhány taxi tetején is feltűnt az említett **gepárdos kép**:

Kollégám éppen egy UPX-et töltött le, mikor is ez a reklám banner jelent meg közben (2007-ben):

Maga a termék az Amazon oldalon található, van róla nagyobb kép is:

Azért úgy gondolom, ennyire nem szerencsés másolni egy konkurens termékének reklámját.

1979-ben éppen számítógépes operátorként dolgoztam a FÜTI nevű cégnél - ekkor már javában dúlt a bűvös kocka láz. Nagyon szerettem, a kollégákkal is próbálgattuk, tanulgattuk, későbbi legjobb összerakási időm kb. egy perc volt. **A Rubik kocka** egy nagyszerű találmány, zseniális, szórakoztató. Na de ami utána következett, az már szánalmas volt. Ha betértem egy játékboltba, trafikba, hegyekben állt a bűvös gömb, bűvös háromszög, bűvös fütyfürütty, bűvös akármi, stb. Egy eredeti új ötlet helyett sokan egy meglévő sikertörténet mechanikus másolásával próbáltak felkapaszkodni. Nem is értem, ez honnan jutott az eszembe... ;-)

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/173359

Kommentek:

Nincsenek hozzászólások.

Hacktivity -első nap

2007.09.22. 20:30 | Csizmazia István [Rambo] | 1 komment

Hazaértem a Hacktivity Konferenciáról. Az első nap igen érdekes volt, elméleti és gyakorlati jellegű előadások, **workshopok** voltak, akit érdekel a téma, holnap feltétlenül jöjjön el!

Izelítőnek egy pár fotó:

Krasznay Csaba (Kancellár.hu) hivatalos megnyitója

Dr. Kovács László (Zrínyi Miklós NVA) a cyberterrorizmusról beszélt

Muha Lajos (GDMF) az **orosz-észt eseményeket** vette górcső alá

Szekeres Balázs (CERT-Hungary)

Sokan voltak kíváncsiak az előadásokra

A szamurájkard komoly dolog :-)

Béres László (ULX) a SELinux rejtelmeiről lebbentett fel a fátylat

Safranka Mátyás (Microsoft) a Vista biztonságossága mellett érvelt

Gara Péter a webes kliensek biztonságáról, és az **MPack exploit-kit** veszélyeiről mesélt

Rootkit workshop a Kisterem közönségének - Csiszér Béla (Sicontact)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/178916

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.12. 15:30:28

Érdekes adalék Muha Lajos előadásához.
Nekem az a mondat tetszett a legjobban, hogy "semmiféle illegális tevékenységet nem végeztek, mindössze annyit tettek, hogy bizonyos weboldalakat igen sűrűn látogattak meg, az már az üzemeltetők hibája, hogy ezt a forgalmat nem bírta el a rendszerük" :-)
index.hu/tech/net/2009/03/12/ifjuoroszok_inditottak_az_orosz-eszt_kiberhaborut_/

Hamis riasztás a MASA-tól II.

2007.09.22. 20:11 | Csizmazia István [Rambo] | Szólj hozzá!

Sok cikk, blogbejegyzés, címlapsztori születik manapság negatív tapasztalatok nyomán, hadd szakítsunk ezzel, és örüljünk, ha épp van minek. Megírtam a levelet a **McAfee cégnek** a Hamis riasztás a MASA-tól esetről, és rekordidő alatt, egy nap múlva megkaptam a választ:

Dear Istvan,

Thank you for your request.

You request has been passed on to our Site Advisor team and we have confirmed the scanner false positive has been fixed with the latest DATs, and we will be patching the siteadvisor.com site as soon as possible.

Mire hazaértem este, már meg is történt a javítás, **nagyon köszönjük :-)**

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- 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/173337

Kommentek:

Nincsenek hozzászólások.

Hacktivity - második nap

2007.09.23. 19:10 | Csizmazia István [Rambo] | Szólj hozzá!

Az első napról már tettem be képeket, most csak pár szót mesélnék az első részről. Abszolút pozitív, nagyon tetszettek az előadások is, és helyszín is egy telitalálat, a hátsó fertályban sörös kriglivel a kézben hallgatni és nézni kivetítőt, nagyon jó kis pub feeling :-)

Sok érdekes bemutatóból teljesen szubjektíven fogok mazsolázni, majd lesznek úgyis teljes összefoglalók a hírportálokon, illetve az előadások anyaga néhány napon belül letölthető lesz a Hacktivity weboldaláról.

Nekem az első nap három prezentáció tetszett nagyon, **Dr. Kovács László beszélt az információs terrorizmusról**, és jól összefoglalta az ezzel kapcsolatos tudnivalókat.

Technikai és érdekes volt **Gara Péter megközelítése a webes kliensek biztonságáról**, gyakorlati példákkal illusztrálva, személy szerint ez nekem nagyon bejött.

Nem mindennapi workshop tanúi lehetett a kisterem közönsége, ahol **Csiszér Béla mutatott be rootkites programokat élőben**. A Sony BMG botrány Vanzant CD-je, a német kiadású Mr. és Mrs. Smith DVD-je, valamint az előző hetekben oly sokat emlegetett Sony MicroVault ujjlenyomat olvasós USB kulcs voltak a főszereplők.

A vasárnapi napon talán valamivel kisebb volt a létszám, de érdekes előadásokban itt sem volt hiány. Sok szó esett napjaink oly zavaró problémájáról, **a spamről, itt Krasznay Csaba jól összefoglalt gondolatai** tetszettek a legjobban. Nekem a téma kapcsán olyan el nem hangzott dolgok jutottak eszembe, ami tovább árnyalhatja az ott elhangzottakat. Például a 419-es nigériai csalás kapcsán említést érdemel az a cseh nyugdíjas, aki végső elkeseredésében agyonlőtte a nigériai nagykövetség – pénze visszaszerzésében egyre csak tehetetlenségét hajtogató – konzulját. Szintén érdekes dolog, hogy míg az ISP-k, és egyéb szolgáltatók panaszkodnak, hogy sok a spam - azaz kéretlen (hirdetés) levél - addig például a vipmail levelező rendszerében (de a Citromail és a Freemail is ilyen) nem tudunk addig sikeresen regisztrálni, míg legalább egy területet meg nem adunk, amihez kapcsolódva később majd reklám levekelet küldözgethetnek címünkre. A phising támadásokkal kapcsolatban érdekes felvetéssel élt Mikko Hypponen, az F-Secure cégtől. Azt javasolja, hogy minden pénzintézet egységesen a .bank domain csoportba tartozzon, így könnyebben kiszűrhetőek lennének a csalárd hasonmás oldalak. A Kínával kapcsolatos spam problémák kapcsán érdemes lenne szorgalmazni az ottani enyhe domainregisztrációs szabályozás szigorítását, persze a Spamhouse spamküldő toplistás tagjainak hűvösre tétele sem lenne butaság ;-)

Akit érdekel, készült egy igen érdekes film a spamről "**Spam, the Documentary**" címmel. Az alkotó lépésről lépésre igyekezett felderíteni mindent: elkezdett válaszolgatni a spam levelekre, melyekben az árucikkeket úgy hirdetik, azok egyenesen kijavítják, sőt tökéletesítik életünket, és rendelt is a termékekből.

Interjút készített a spam ellen küzdő szakemberekkel, de megpróbált felkutatni egy igazi hús-vér spamterjesztőt is. Eközben igyekezett tisztázni olyan szakmai zsargonokat is, mint például mi is az a phising kit (adathalász támadás készítő programkészlet), vagy kik azok a zombik.

Kiemelkedő sikere volt **Dallos Zsolt ügyvédnek is, aki a kisteremben a fájlcsere és a szerzői jog** kapcsán mesélt érdekes eseteket, és fejtette ki véleményét. A téma aztán olyannyira felkeltette az érdeklődést, hogy a folyosón még egy jó órás "after party" keretében záporoztak a kérdések, hozzászólások.

Végül **Bodó Balázs**t említeném még, aki nem csak érdekes témáról - **A kultúripar felhekkelése** - adott elő, hanem élvezetes és szemlélete stílusával szerzett egy kellemes háromnegyedórát a nagyérdeműnek.

Aki itt volt, annak viszontlátásra 2008-ban is, aki pedig nem jutott el az idén, annak jó szívvel ajánljuk, hogy jövőre ne hagyja ki, ha érdekli a számítógépes biztonság közelről.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/174486

Kommentek:

Nincsenek hozzászólások.

Magyarázzuk a mechanizmust

2007.09.23. 18:46 | Csizmazia István [Rambo] | 8 komment

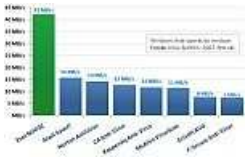
Csak röviden szeretnék ezekkel foglalkozni, két cikket olvastam, és az ott leírtakkal kapcsolatban gondolatok születtek a fejemben. Az első az Index tech blogjában volt, a Skype-on terjedő féreggel kapcsolatban, ahol a Norton nem ismerte fel a férget. A cikk minden megállapításával egyetértek, egyetlen egyet kivéve - és itt jön a lényeges rész, idézek:

"Ha minden egyes új vírus leírását automatikusan letöltené a program, zavaróan gyakran töltene."

Nyilván nem is lehet és nem is érdemes minden vírusra azonnal adatbázist frissíteni, de ha van olyan új támadás, ami széleskörű, sok felhasználót érint és/vagy kiemelt veszélyességű, szerintem teljesen normális a rendkívüli adatbázis frissítés, és meggyőződésem, hogy adott esetben egy **pár óránként frissülő Kaspersky vagy NOD32 nem zavarja a felhasználókat**.

A másik ilyen gyöngyszem az "Egyre trükkösebbek az internetes csalók" című mfor cikkben szerepelt, idézek itt is:

"Mint a Symantec magyarországi képviseletének marketing vezetője elmondta, a cégük filozófiája szerint a vírusokat nem annyira gyorsan, mint inkább alaposan kell keresnie a szoftvereknek..."



Valahogy az jutott eszembe, hogy aki nem elég gyors, az jól megmagyarázza. Nyilván sokféle szempont játszik szerepet egy biztonsági megoldás kiválasztásánál, a megbízhatóság, a technikai és a support háttér, a reagálási idő, frissítési gyakoriság, erőforrás igény, távmenedzsment képességek, platform lefedettség, ár, és még további fontos kritériumok. Azért úgy vélem, hogy NOD32 kiemelkedő sebessége a megszerzett 45 Virus Bulletin 100% Award fényében nem ment a minőség rovására.

Nem az említett gyártó megbántása, vagy kifigurázása volt a célom - igyekszem is a jövőben nem túl gyakran ilyen esetekkel foglalkozni - hanem a sugallt megállapítások voltak olyanok, amikkel én személy szerint nem értettem egyet.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/174450

Kommentek:

Arki · http://www.freegamespalace.org 2007.09.25. 23:00:21

A frissítés zavaró tényezőjével abban az esetben nem értek csak egyet, ha újra kell indítani a gépet egy frissítésnél (nem tudom, hogy ez mennyire gyakori), de szimpla definicó frissítés - pláne háttérben - nem zavaró. Itt arra akartam rávilágítani, hogy az ember az operációs rendszer frissítéseit is sokszor halogatja, ha újraindítás szükséges.

Nem is tudom, talán a heurisztikára gondolt alaposság szóval - mi másra? -, de nem olvastam még olyan visszajelzést, hogy a Symantec akár abban kitünt volna, így adott egy pofont a bizonyosnak.

A 45 VB díjhoz és a gyorsasághoz gratulálok, bár nem tudom melyik után kapta meg a leggyorsabb titulust :).

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.26. 18:31:00

Kedves Arki!
Én is a szimpla definíció frissítésre gondoltam, és ezeknek sosem szükséges újraindítani a gépet.

A sebességnél meg csak arra gondolni, hogy savanyú a szőlő. Ebben a tekintetben egyébként újabban az AVG is hihetlen módon megerősödött.

zoloe 2007.09.28. 16:29:52

Kedves Arki!
Köszönjük szépen, már bele is került a telepítő az adatbázisba.
Eddig csak a telepítéskor kitömörített 2 fájlt fogta meg a NOD32 (heurisztikával), így már magát a telepítőt is felismeri.
Üdv:
zolo

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.28. 16:46:14

Kedves Arki!
Ahogy zolo már jelezte, bekerült a kártevő az adatbázisba, most ellenőriztem a VirusTotalon:
"NOD32v2 2558 2007.09.28 Win32/TrojanDownloader.Zlob.BFI"
Köszi a jelzést :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.28. 19:58:15

idézet következik:
"Kedves Rambo!

Amennyire én tudom, hiába erősít be sebességben, heurisztikában a nod még mindig jobb.

Más: biztos van más módja is, de kérem segítsen eljuttatni ezt a károkozót a vírusirtókhoz:

...törölve.../download/ alatt
hqcodec4158.exe fájl

A TV2 fórumjában lévő botok bejegyzései random domain névvel - melyek először frame tartalmú oldalt töltenek be - átugrasztanak a itsgo.com oldalra, ami a rosszindulatú scripttel feltételenül fel akarja telepíttetni a fájlt a látogató gépére. A böngésző feladatkezelőből való bezárásával elkerülhető (vagy a scriptek tiltásával). Itt - tv2 fórum.. - mondjuk azt sem tudom, hogy kit kellene értesíteni.

Elemzés eredmények:
Antivirus Version Last Update Result
AhnLab-V3 2007.9.28.0 2007.09.27 -
AntiVir 7.6.0.15 2007.09.27 TR/DNSChanger.GH
Authentium 4.93.8 2007.09.27 -
Avast 4.7.1043.0 2007.09.26 -
AVG 7.5.0.488 2007.09.27 -
BitDefender 7.2 2007.09.27 -
CAT-QuickHeal 9.00 2007.09.27 -
ClamAV 0.91.2 2007.09.27 Trojan.Dropper-2644
DrWeb 4.33 2007.09.27 -
eSafe 7.0.15.0 2007.09.23 -
eTrust-Vet 31.2.5169 2007.09.27 -
Ewido 4.0 2007.09.27 -
FileAdvisor 1 2007.09.27 -
Fortinet 3.11.0.0 2007.09.27 -
F-Prot 4.3.2.48 2007.09.27 -
F-Secure 6.70.13030.0 2007.09.27 -
Ikarus T3.1.1.12 2007.09.27 -
Kaspersky 7.0.0.125 2007.09.27 Trojan.Win32.DNSChanger.ph
McAfee 5129 2007.09.27 -
Microsoft 1.2803 2007.09.27 -
NOD32v2 2554 2007.09.26 -
Norman 5.80.02 2007.09.27 -
Panda 9.0.0.4 2007.09.27 -
Prevx1 V2 2007.09.27 -
Rising 19.42.32.00 2007.09.27 -
Sophos 4.21.0 2007.09.27 -
Sunbelt 2.2.907.0 2007.09.26 -
Symantec 10 2007.09.27 -
TheHacker 6.2.6.072 2007.09.27 -
VBA32 3.12.2.4 2007.09.26 -
VirusBuster 4.3.26:9 2007.09.27 -
Webwasher-Gateway 6.0.1 2007.09.27 Trojan.DNSChanger.GH
Additional information
File size: 210275 bytes
MD5: ae009284867ab67d575313c02b5cee8a
SHA1: 4f3d548303c871e76863cf02c65de39605c7c983
packers: BINARYRES, BINARYRES

Üdv:

Arki"

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.28. 20:14:52

Kedves Arki!

Kénytelen voltam kitörölni, es moderálva visszamásolni a hozzászólásodat, mert úgy tűnik, a hivatkozott oldal egy új veszélyforrásnak látszik. Rendszeres időközönként (félóránként?) új exe jelenik meg rajta, és míg az előző fájlt a víruslaboratóriumnak elküldve már bekerült az adatbázisba, a még újabb exe egyelőre még ismeretlen. Több ilyen új EXE is van különböző neveken, és mintha az IP címeket is figyelné, hogy ugyanaz ne töltödjön le kétszer egy gépre.

Bár azt tapasztaltam, hogy a letöltött nagy EXE-t nem is észleli a NOD32 mindig, a benne levő állományokra már rendesen riaszt, de azért biztos, ami biztos: szeretném megelőzni, hogy az adott konkrét link által valakit baleset érjen.

Mellékelem a mostani exe VirusTotalos listáját, és még egyszer köszönöm, hogy felhívtad erre a dologra a figyelmünket.

* * * * *
A(z) hqcodec1000.exe állomány feltöltve: 2007.09.28 20:05:58 (CET)
Antivírus Verzió Utolsó frissítés Eredmény
AhnLab-V3 2007.9.29.0 2007.09.28 -
AntiVir 7.6.0.18 2007.09.28 TR/Dldr.Zlob.NMO
Authentium 4.93.8 2007.09.28 -
Avast 4.7.1043.0 2007.09.28 -
AVG 7.5.0.488 2007.09.28 -
BitDefender 7.2 2007.09.28 -
CAT-QuickHeal 9.00 2007.09.28 -
ClamAV 0.91.2 2007.09.28 -
DrWeb 4.33 2007.09.28 -
eSafe 7.0.15.0 2007.09.23 -
eTrust-Vet 31.2.5169 2007.09.27 -
Ewido 4.0 2007.09.28 -
FileAdvisor 1 2007.09.28 -
Fortinet 3.11.0.0 2007.09.28 -
F-Prot 4.3.2.48 2007.09.27 -
F-Secure 6.70.13030.0 2007.09.28 -
Ikarus T3.1.1.12 2007.09.28 -
Kaspersky 7.0.0.125 2007.09.28 -
McAfee 5130 2007.09.28 -
Microsoft 1.2803 2007.09.28 -
NOD32v2 2558 2007.09.28 -
Norman 5.80.02 2007.09.28 -
Panda 9.0.0.4 2007.09.28 -
Prevx1 V2 2007.09.28 Trojan.Nudos
Rising 19.42.42.00 2007.09.28 -
Sophos 4.21.0 2007.09.28 -
Sunbelt 2.2.907.0 2007.09.28 -
Symantec 10 2007.09.28 -
TheHacker 6.2.6.073 2007.09.28 -
VBA32 3.12.2.4 2007.09.27 -
VirusBuster 4.3.26:9 2007.09.28 -
Webwasher-Gateway 6.0.1 2007.09.28 Trojan.Dldr.Zlob.NMO

Arki · http://www.freegamespalace.org 2007.09.28. 22:38:26

Teljesen megértem. Egy fertőzött gép próbált meg ma MSN-en keresztül letölttetni velem egy fájlt, a variáns kifejezés alább elégséges vagy adjak konkrét linket? Persze, talán linuxos verzióhoz találni lehet mást is a link mappájánál (bluetooth hack-et olvastam, de nem jártam utána).

AhnLab-V3 2007.9.29.0 2007.09.28 -
AntiVir 7.6.0.18 2007.09.28 -
Authentium 4.93.8 2007.09.28 -
Avast 4.7.1043.0 2007.09.28 Win32:Delf-FND
AVG 7.5.0.488 2007.09.28 Dropper.Generic.QEU
BitDefender 7.2 2007.09.28 -
CAT-QuickHeal 9.00 2007.09.28 -
ClamAV 0.91.2 2007.09.28 -
DrWeb 4.33 2007.09.28 -
eSafe 7.0.15.0 2007.09.23 -
eTrust-Vet 31.2.5169 2007.09.27 -

Ewido 4.0 2007.09.28 -
FileAdvisor 1 2007.09.28 -
Fortinet 3.11.0.0 2007.09.28 -
F-Prot 4.3.2.48 2007.09.27 -
F-Secure 6.70.13030.0 2007.09.28 -
Ikarus T3.1.1.12 2007.09.28 -
Kaspersky 7.0.0.125 2007.09.28 -
McAfee 5129 2007.09.27 -
Microsoft 1.2803 2007.09.28 -
NOD32v2 2558 2007.09.28 a variant of Win32/TrojanDropper.Delf.NFJ
Norman 5.80.02 2007.09.28 -
Panda 9.0.0.4 2007.09.28 Suspicious file
Prevx1 V2 2007.09.28 -
Rising 19.42.42.00 2007.09.28 -
Sophos 4.21.0 2007.09.28 -
Sunbelt 2.2.907.0 2007.09.28 -
Symantec 10 2007.09.28 W32.Spybot.Worm
TheHacker 6.2.6.073 2007.09.28 -
VBA32 3.12.2.4 2007.09.27 -
VirusBuster 4.3.26:9 2007.09.28 -
Webwasher-Gateway 6.0.1 2007.09.28 Win32.Malware.gen (suspicious)
További információ
File size: 46024 bytes
MD5: aff52cc325b0b30f928bef4a94caf1ea
SHA1: 29dbaeb566131cbc4a6910a905043d4d263d52eb

zoloe 2007.09.30. 12:20:07

Szia Arki,

Kérlek küldj linket a support kukac sicontact pont hu cimre, a nevemre. Köszönöm!

A kínaiak már a spájzban vannak

2007.09.24. 21:46 | Csizmazia István [Rambo] | 6 komment

A rejtett kémprogramok mennyisége az utóbbi években hihetetlen módon megnőtt. Majd egy hónappal ezelőtt kaptunk hírt arról, hogy **Angela Merkel kínai látogatása alatt derült ki**, hogy a német kancellária és több más kulcsfontosságú (Külügy, Gazdasági, Kutatási) Minisztérium számítógépei kínai eredetű rejtett kémprogramokat tartalmaztak, amelyek a kikémlelt adatokat rendszeresen házon kívülre továbbították. A beszámolók szerint a támadások a kínai Lanzhouból, Kantonból és Pekingből indultak ki, és az ellopott adatok is ide érkeztek. Kína cáfolta a vádakat.

Valamivel később **a Pentagonban elismerték**, hogy a védelmi miniszter levelezőrendszeréhez hónapokkal ezelőtt idegenek fértek hozzá és itt is kínai elkövetőket sejtettek a háttérben. Szeptember elején a The Guardian oldalán jelent meg egy hír, miszerint a brit kormányzat egyes számítógéphálózataiba, köztük **a parlament és a külügyminisztérium rendszerébe is betörtek** ismeretlenek. Nem bizonyítható, hogy itt is kínai behatolókról van-e szó, bár egyes források tudni vélik, mindenesetre a félelem az biztosan létezik. A cikk szerint Kínában **a világ legfejlettebb internetes szűrő eszközeit fejlesztették ki**, például az úgynevezett Kínai Nagy Tűzfal (Great Firewall of China) segítségével a Dalai lámáról, Taiwanról szóló és más politikai információk elérését korlátozzák igen hatékonyan.

Bő egy hete pedig Franciaországból szólt a tudósítás, majd Francis Delon nyilatkozott arról, hogy számítógépes kalózok támadták meg **a francia kormányzati rendszereket** és szerinte a nyomok Kínába vezetnek. A kínai kormány természetesen cáfolta, hogy hadserege próbált volna beférkőzni ily módon. Ami érdekes, hogy az 1503-ban született francia Nostradamus egyik jóslata szó szerint így szól: **„keletről jő a sárga veszedelem, mely elpusztítja a világot…”** Lehet, hogy ő már sejtett valamit? Egy biztos: a hihetetlen gazdasági fejlődést produkáló ország valószínűleg **még sok meglepetést fog okozni a világnak**.

Erejükre mindenesetre jellemző, hogy az évek óta megoldatlan probléma (ahány mobiltelefon gyártó, annyiféle töltő csatlakozó) egy csapásra elintéződött, miután **a kínaiak állítólag kijelentették, mostantól csak és kizárólag mikro USB-s töltőt hajlandóak gyártani.** Ezek után lássunk csodát: az öt nagy mobilgyártó érdekes módon hirtelen hipp-hopp meg bírt egyezni a korábban kilástalannak látszó ügyben.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- 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

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/176033

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.27. 18:09:10

Ha jó egy post címe, akkor úgy tűnik, előbb-utóbb divatba jön :-)
www.vezess.hu/hirek/kinaiak_mar_spajzban/12264/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.26. 12:36:38

Az idő igazolni látszik a tendenciákat:
hirek.prim.hu/cikk/72182/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.29. 22:08:40

Ez is érdekes, az összeesküvés elméletek kedvelői akár azt is feltételezhetik, hogy először belenéztek minden fontos résztvevő lapjaiba, majd ők okozták a világválságot ;-)
www.hirextra.hu/2009/03/29/felhackeltek-a-dalai-lama-szamitogepet/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.22. 09:37:38

Az ember néha elmélázik, hogy az ilyen elvileg védett helyekről hogy a pitlibe lehet több ezer GB-ot ellopni :-O
index.hu/kulfold/2009/04/21/szupertitkos_adatokat_loptak_a_pentagontol/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.08. 11:15:30

Tényleg "mindenre" képesek ;-)
index.hu/gazdasag/vilag/2009/05/07/eloirtak_volna_a_dohanyzast_kinaban/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.08. 11:46:28

Szóval kihagytam a kommentből, hogy nem akarok általánosítani, de ha így mennek ott a dolgok: kötelező dohányzás a hon üdvére és az adók növelésére, minden lézető dolog hamisítása, köztük a gyógyszereke és az élelmiszereké is, akkor ugye nem nehéz elképzelni, hogy a számítógépes kártevők, kémprogramok területen sem van/volt/lesz sokkal intenzívebb etikai vagy lelkiismereti visszatartó erő.

Keressünk és találjunk

2007.09.25. 08:56 | Csizmazia István [Rambo] | 2 komment

Egy nagyon érdekes blogbejegyzést találtam a VirusKommando lapján, amelyben arról volt szó, hogy a szerző **megpróbál antivírus próbaverziókat gyorsan és könnyen letölteni**, és összehasonlítja a versenytársakat ebből a szempontból, hol mennyire gyors vagy egyáltalán működőképes ez a lehetőség. Emellett a Google keresőbe beírt találati helyezést is vizsgálja, kinek milyen a kereső marketingje. **A két legbarátságosabb oldal** a cikk szerint az AVG és a NOD32 volt :-)

Az "antivirus" szócska beírása után az alábbi kép fogadja netezőt

Amit még hozzátennék, **ha én lennék az a bizonyos tanácstalan és kutakodó Átlagfelhasználó**, az hogy milyen pót lépéseket tennék, ha éppen ingyenes vagy próbaverziós víruskeresőt szeretnék letölteni.

- meghasalnám és **próbaképpen beírnám az elképzelt magyar domain neveket**, hátha szerencsém lesz és valóban létező: pl. f-secure.hu, kaspersky.hu, stb. Az persze már más kérdés, ha vannak ilyen jellegű találatok, mennyire user friendly módon engednek gyorsan közel a letöltésekhez.
- megnézném **ingyenes vagy shareware letöltő oldalakon** is, pl. Honosító Műhely, Szoftver Bázis, Prím Letöltés, stb.
- az eredeti külföldi oldalt keresném fel, hiszen vannak olyan programok, amiknek egyáltalán nem létezik magyar nyelvű változata, ha jól tudom ilyen például a Trend Micro; és persze van, aki jól elboldogul egy angol nyelvű változattal is.

A weboldalak szerkezetén, és a keresőbeli pozíción túl persze az is **jó lenne, ha maguk a AV gyártók valóban nagyobb erőfeszítést tennének a felhasználók felé az ingyenes próbaváltozataik hatékonyabb népszerűsítésével**, hiszen egyértelmű kapcsolat vélelmezhető ezzel kapcsolatosan: aki egy weboldalról (vagy egy számítástechnikai magazin mellékletéről) feltelepíti ezeket és elégedett, az nagyobb eséllyel válik később elégedett vásárlóvá.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Hogyan szúrjuk ki a gyanús Android appokat?
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/176268

Kommentek:

Vidi Rita · http://www.hosnok.hu 2007.10.09. 18:31:17

Szia István!
nahát, micsoda meglepetés:) mondhatnám, a mai nap legkellemesebb meglepetése.
Először is, látogatók egy ismeretlen helyről, aztán meg itt vagy Te, teljes valódban:) Nem hasonlítasz Rambóra:))

kérdezhetek? ezt a blogot a sicontact kft. "szponzorálja"?
elnézést, ha butaságnak tűnik a kérdésem...
úgy látom, lesz mit olvasni a napokban..:)

örültem! Jövök még. És ezt nyugodtan veheted fenyegetésnek:)

Csizmazia István [Rambo] · http://antivirus.blog.hu
2007.10.09. 21:06:09

Szia Minerva :-)
Hát igen, kicsi a világ!
És igen, NOD-os csapattag vagyok, jól látod. Gratulálok a jó témaválasztáshoz, szerintem nagyon fontos dolgokra hívtad fel a figyelmet ebben a postban.
Egyébként időközben még Bumikával is sikerült összeismerkednem :-)
Ha bármiben tudok segíteni, tudod az email címem.

ESET Smart Security

2007.09.26. 09:02 | Csizmazia István [Rambo] | 23 komment

Április óta sorban az egyre komolyabb változatok látnak napvilágot a NOD32 gyártójának, az ESET komplett védelmi csomagjának publikus bétaverzióiból. A vírus és kémprogram elleni alapok mellett spamszűrő és tűzfal is található a Smart Security nevű integrált biztonsági készletben. A mostani ötödik verzió immár a Release Candite 1, amelynél a bétatesztelők véleményét, észrevételeit és javaslatait is figyelembevéve készítettek.

Az ESS csomag az XP és a Vista mellett a 64 bites Windows változatokat is támogatja (XP, Vista, Server 2003). Aki kíváncsi, és szívesen kipróbálná, ingyenesen letöltheti az ESET honlapjáról.

Ajánlott bejegyzések:

- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/177029

Kommentek:

Lali_ · http://magyaropera.hu 2007.10.25. 22:04:01

észrevétel: atom stabil és jó cucc, eggyetlen gondom, hogy néha (eddig kb 3-4-szer több hónap alatt, az uccsó verziónál is) a kérdezgetős ablak (amikor változik egy progi, vagy net elérést szertne)befagy hiába nyomok bármit, nemválaszol és nemlehet eltüntettni

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.25. 22:53:36

Szia opera11!
Május óta tesztelem a különböző változatokat, és már az elég stabil RC1 verziónál járnak. Melyik változattal voltak a fagyások? Ha nem a legújabbal, látogass el a www.eset.eu/download/beta oldalra, és tölts le a legfrissebbet! Ennél éreztem igazán, hogy kezd nagyon stabil és jó lenni. A kérdezgetős ablak szerintem azért volt, mert a tűzfalnál az interaktív szűrési módot választottad, nem az automatikust. Én mondjuk szeretem, ha kérdezget.

Xfaktor 2007.10.26. 16:34:44

Mivel még nem próbáltam ki ezért érdemben nem tudok nyilatkozni, de az ilyen komplex biztonsági csomagokkal kapcsolatban mindig van bennem egy kis félsz. Remélem ez csak egy rossz beidegződés, de mindig attól tartok, hogy ha egy ilyen védelmi rendszer már alapból tartalmaz tűzfalat, vírusirtót, spamszűrőt stb. akkor megoszlik a figyelme és az egyes komponensei nem olyan hatékonysággal fognak működni, illetve nem lehet majd őket részletesen konfigurálni. A nod32-vel kapcsolatban nagyon jó tapasztalataim vannak, a kérdés csak az, hogy a Smart Security többi védelmi modulja is tuja-e majd hozni a vírusirtó által méltán kiharcolt magas színvonalat.
Félreértés ne essék, én nem akarok farkast kiáltani, sőt nagyon remélem, hogy majd maga a program fogja a leírtakat megcáfolni. Minden eset re :) én már nagyon várom a végleges verziót.
u.i.: Kedves Rambó! Gratulálok a bloghoz, már régebb óta olvasom, és nagyon tetszenek a postok, így tovább!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.26. 17:08:29

Kedves Xfaktor!
Üdv a fedélzeten, és köszi kommentet.
Egy komplett programcsomag viselkedés-elemzési technikát hajt végre, és mindeközben támaszkodik a tűzfalas védelemre, ezzel csökkentve a lehetséges belépési pontokat, ezzel is mérsékelve a fertőzést. Ezzel többet képes nyújtani, mint egy szimpla antivírus. Én is az AV + tűzfal + kémirtó trió híve vagyok, és mondjuk a plusz spyware irtóról az ESS végleges változatának megjelenése után sem szándékozom lemondani. Hogy mit teljesít az ESS a biztonsági csomag teszteken, majd kiderül,remélem a legjobbakat. A fejlesztők előtt mindenesetre le a kalappal, nyitottak voltak minden ötletre, javaslatra, kritikára.

Lali_ · http://magyaropera.hu 2007.10.26. 23:52:43

Szia. A stabilitással nekem a legelső óta nemvolt igazán gondom.(Az eset mappa létrehozási dátuma 2007.07.09, szóval azóta :))
Igen, az interaktív módban használom, én is azt szeretem, ha tudom mit csinál :)
Az 32 bites RC1 van fent. Legutóbb a bonjour service-nél(A win-os Safari "kelléke") csinált ilyet, az első alkalomnál, amikor net-et akart a telepítés után és még nemvoltam, vagy taán pont akkor csatlakoztam...Alapból nemlett volna baj csak pont utána tettem fel a béta Operát is(9.5), ami elsőnek futott, tehát utána kérdeznie kellett volna, hogy az opera 9.5-nek adok a netet..csakhát nem kérdezet, így aztán az Opera sem működött....De egy kijelentkezés megoldotta, szóval nemvészes

Xfaktor: Én meg mindenből pont az ilyen, egy progi sok mindent szeretem. Hardveres Pl: mobil+fényképező+gps+wi-fi..., vagy szoftveres példa: böngésző, levelező, jegyzetkezelő, irc chat, torrent kliens..
A biztonságtechnikai szoftvereknél meg pláne jó ha egyben van minden. Ezért is hiányolom egyébként az ESET Smart Securityből az autómatikusan elinduló programok figyelését, valamint főleg a kémprogramok elleni védelmet, vagy az egybe van fűzve az antivirrel? Mert egyszer amikor lefutattam egy próbaverziós Sunbelt CounterSpyt (amiről aztmondják, hogy elég jó), akkor nemtalált semmit....

Lali_ · http://magyaropera.hu 2007.10.28. 15:50:27

Mégegy bug(?)/észrevétel:
Az Opera böngésző levelezőjét pop3-as llevél küldéskor 2-3 másodpercig befagyasztja!!!!!(Aztán elküldi a levelet) Méghozzá a tűzfal modulja, mert amikor kikapcsoltam az antivirust és az antispam modult, akkor ugyanúgy jelentkezett, de amikor kikapcsoltam a tűzfalat(Disable filtering: allow all traffic), akkor már rögtön küldte a levelet.
Aztán kipróbáltam csak a tűzfal letiltással, akkor is rendesen ment a levél. És a proci használat nem ugrott fel, úgyhogy nem is értem...Azért nemhiszem, hogy ennyi idő kéne, ahhoz, hogy a megfelelő szabályt (Opera böngészőnek engedve van a pop3) alkalmazza, pláne, hogy sima txt üzeneteknél van ez, mindenféle csatolmány nélkül...

Az ilyesmiket hol lehet a fejlesztőknek jelezni?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.28. 18:13:13

Szia opera11 :-)
A fejlesztőknek kétféleképp lehet jelezni:
van egy fejlesztői fórum, ezt itt találod:
www.wilderssecurity.com/forumdisplay.php?f=18
és lehet nekik levelet is írni a betasupport KUKAC eset.sk email címre
Nekem olyan van - de ezt még nem írtam meg én se - hogy a VMWare nem tud fellépni a hálóra, csak ha egy pillanatra leveszem a tűzfalat, de az érdekes az, ha utána rögtön visszakapcsolom, utána már átjár rajta, csak elsőre van neki valamilyen gondja. Még turkálok egy kicsit a szabályaim, és a trusted zónáim közt, nehogy végül nálam legyen valami guzmi.

zoloe 2007.10.28. 19:55:41

Sziasztok!
opera11 - Nem sikerült reprodukálni a hibát, de megírtam a fejlesztőknek. A legtöbb tesztelést valószínűleg az interaktív módú működés igényli, dolgoznak rajta. Köszönjük a jelzést!

Lali_ · http://magyaropera.hu 2007.10.28. 21:05:04

zoloe: Mármint melyiket? Az Operás hiba mindig jelentkezik, a Safaris dolog meg szerintem a rosszkor csináltam, vagy nemcsináltam a rosszdolgot, szóval az nemhiszem, hogy reprodukálható lenne.

Ati82 2007.10.30. 08:04:11

Sziasztok!

Azt szeretném megkérdezni, hogy az Eset Smart Security és a Nod32 3.0v magyar nyelven Nov.5.-én jelenik meg?
Illetve a Nod32 2.7 -ről való átállás az Eset Smart Security-re kb. mennyibe fog kerülni, érvényes licensz mellett?
Egyébként én nagyon megvagyok elégedve az ESET termékével és már várom, hogy meglegyen az új termék.
Számtalan forumon a Nod32 mellett voksolok és vétozom meg negativ véleményeket...

Ati82 2007.10.30. 08:09:28

És még egy kérdés: az RC1 nod elég stabil mindennapi használatra(üzleti gép)? Mivel még csak angol nyelven érhető el, ezért, ha megjelenik a magyar nyelvű, az angolt reinstall, vagy a magyar install után magyar nyelvű lesz?
Egyébként én a Nod32 mellett semmi mást nem használok és még soha nemvolt vele problémám...
Pedig néha járok "rossz" honlapokon. És CSAK IE7-et használok...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.30. 08:52:44

Szia Ati82!
Pontos dátumokat én sem ismerek, ebben sajnos nem tudok segíteni, de a magyar változatok általában valamivel később szoktak megjelenni, szerintem ez most is így lesz. Bővebb infokat erről a Sicontact-os srácok tudhatnak. Én május óta tesztelem a bétákat, és csak a legelsőnél kellett kézzel uninstallálni, azóta simán felmegy az újabb változat, illetve amikor szükséges, ő automatikusan elvégzi az uninstall folyamatot. Ilyen esetekben a korábbi saját beállítások természetesen megmaradnak.
A NOD32 és az ESS is jelentős proaktív, heurisztikus és egyéb elemzéseken alapuló képességei vannak, de mivel az én lelkem nagyon paranoid, mindig használok külön kémirtót is, sőt többet is :-)
Az IE7 használatot olyannak tartom, mintha valaki bezárja ugyan a bejárati ajtaját, de a konyhablakot nyitvahagyja. Mivel közismert, milyen sebezhetőségeket okoz, és emiatt ráadásul első számú célpont, én biztos váltanék a helyedben. Az hogy nem volt problémád, két dolgot is jelenhet:
- az is lehet, hogy volt problémád, csak nem vetted észre
- ha eddig megúsztad, nem biztos, hogy így is marad a jövőben, hiszen a rosszfiúk gőzerővel fejlesztenek

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.30. 09:03:15

Na most látom, kimaradt egy-két dolog.
A béta változatok nem véglegesek, ezért éles használatra csak saját felőssséggel használható, a piaci kitesztelt változat a biztos, amelynek a működésére a gyártó garanciát vállal. Ettől függetlenül nekem a betak semmilyen gondot nem okoztak, és jól vizsgáztak.
Árakról nem tudok semmit, nem is az én asztalom, de az biztos, hogy amíg nincs hivatalos bejelentés, addig ez korai lenne.

Ígérem, ha a megjelenésről lesz biztos, hivatalos információm, meg fogom írni itt a blogban.

Ati82 2007.10.30. 09:25:08

Rambo: köszönöm a felvilágositást.
De én akkor is tartom magamat ahhoz, hogy teljesen mindegy, hogy az ember milyen böngészőt használ, ha figyelmetlen netezés közben...Már 4éve használom az IE-t és a 4év alatt csak 2x volt windows reinstall. Az egyiket a Firefox okozta....
+ az én butaságom. De tanultam belőle és majd 3éve (lekopogom) semmi gondom a számitógép biztonságával(lassulás, kérdéses problémák, stb.)

Lali_ · http://magyaropera.hu 2007.10.30. 21:48:02

Hát Ati82, részvétem: secunia.com/advisories/26201/

Na kérem, az alábbi linken olvastgathatsz az IE 7 egyik biztonsági hibájáról. Az 5-ös skálán 4-es súllyosságú. A segítségével az IE7 user rendszeréhez hozzálehet férni.

És ez nemolyan, hogy figyelsz a netezés közben...Mert nem csak a crack és pornóoldalakon, vagy hasonlóakan kaphatsz vírust....Ez nemis vírus, tehát ezellen a nod és más vírusírtó sem tehet sokmindent, ha jóltudom...Miért te talán a magnyított oldalaknak a forráskódjait mind elolvasod, átnyálazod? Végignézed mindegyiket? Én is betehetnék akár a saját oldala(i)mba is ilyen kódokat és az összes IE 7-es usert jól megszívathatnám. Az egy dolog, hogy ezt nemteszem meg(főleg mert nemvagyok hacker és a konkrét kihasználását sem tudom), de szerintem pár óra googlezással magtalálható.
(Ugyanez a hiba volt a FF 2.0.0.5-ben, csak ott már kijavították ezt speciel)

Persze elvileg ezeket a szoftver fejlesztőknek kéne kijvítani, csakhát sokan tojnak rá....

Mellesleg az Operában(ellentétben az IE-vel és a FF-al) nemigen szoktak lenni ilyen kihasználható hibák, MOST sincs!

Ati82 2007.10.31. 09:29:14

opera11: köszönöm a kimeritő felvilágositást.
Lehet, hogy vannak hibái az IE7-nek, a Firefoxnak, az Operának, a Netscapenek, a Windowsnak, stb.
Lesznek is, amig léteznek.
De mégegyszer hangsűlyozom, hogy én speciál még netalálkoztam vele, és remélem nem is fogok.
Szóval bármi komment lesz az IE7-tel szemben, akkor is használni fogom.
"Persze elvileg ezeket a szoftver fejlesztőknek kéne kijvítani, csakhát sokan tojnak rá...."
- ehhez csak annyi a hozzáfűzésem, hogy mig az Opera és a Firefox egy külön szoftver, addig az IE egy rendszerbe integrált kiegészitő, szóval szerintem annak a frissitése, nemolyan egyszerü elkésziteni a frissitést, mert igazodniuk kell a Windows kiadott frissitéseihez IS....
A másik dolog, ha az Opera a világ legbiztonságosabb böngészője, vajon miért csak páran használják????
Talán mert a biztonságon kivül nemsokat nyujt? Lehet...

zoloe 2007.10.31. 11:13:21

Ati82: Magyar nyelvű új termékek legkorábban december elejére várhatók.
Opera11: Légyszi írj nekem a support@sicontact.hu -ra, kérdezni szeretnék a hibával kapcsolatban. Köszönöm!

Ati82 2007.10.31. 13:33:11

zoloe: köszönöm az infót.

Ati82 2007.10.31. 13:36:51

Zoloe: köszönöm az infót.

Lali_ · http://magyaropera.hu 2007.10.31. 17:05:50

zoloe: küldtem levelet

Ati82:

1. Szerintem nemlenne nehezebb kijavítani az IE hibákat, mint az Opráét és a FF-ét. Mert ők elöször is több platformara készítenek böngészőt, másrészről az, hogy az op.rendszerbe nemtudnak úgy beépülni az nemfeltétlenül előny, vannak hátrányai is, pl az IE komponensek elindulnak az op.rendszerrel a FF és Opera nem, mivel nem az op.rendszer része.(Ezért is indul a FF tetű lassan, míg az IE viszonylag rendes tempóban, de ezt a pár s-ot két oldal betöltés után már elveszti)
2. Másrészről minek javítsák ki a hibákat, vagy tartsák be a webes szabványokat. A sok mezei usernek úgyis megteszi ez a rakás sz.. Aztán majd csodálkozol, ha egy idő után minden 2. oldal ilyen lesz, mint ez: blog.kreative-labs.com

3."vajon miért csak páran használják"
Mert sok mezei (l?)user van. (Egyébként a netezők pár%-a azért nemolyan kezés ember) Egyébként, hogy nemnyújt sokat, azért az egy kicsit erős, mondjuk azért mert mellesleg a böngészők közül ez rendereli a leggyorsabban a weboldalakat, nézzél csak meg pár sebességtesztet(javascript, css vagy bármi mást) a saját gépeden, végezd el különböző böngészőkkel. Én már nagyságrendi külömbségekkel is találkoztam (értsd: 10*lassabb az IE). Másrészől az Operában egy csomó olyan funkció van, ami a többiben nem (levlező, torrent letöltés , irc chat, egérmozdulatos böngészés, jegyzetkészítés...)

doki64 2008.02.16. 21:21:56

Tisztelt Csizmazia István!
Egy lehet,hogy mások által butának ítélt kérdéssel fordulok önhöz. A jelenleg általam használt vírusirtóval /Fs.../ megvagyok elégedve. Sajnos azonban az árával és a memória igényével/lassítja a gépet/ nem, mivel a Nod 32 diákkedvezménnyel és több éves előfizetéssel szinte csak 50 % az általam használtnak. A jövőben szeretném megvásárolni az ESET Smart Security 3.0 megjelenő magyar verzióját.
Kérdésem a következő: kell-e illetve szükséges valami más programot is telepíteni az ESET mellé? Ha ajánlott, akkor nagyon szívesen elfogadnám tanácsát mivel nem erősségem a védelmi rendszer felépítésének módja taktikája.Régebben csak Add-awere volt meg egy sima vírusírtó de a most használatos víruskeresőm telepítésénél felhívta a figyelmem ,hogy távolítsak el minden egyebet. Tehát a Nod mellé kell-e még valami vagy elég biztonságot nyújt önmagában.
Üdvözlettel:doki

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.02.17. 12:56:39

Kedves Doki64!
A magyar verzió ante portas, napokon belül várható.
Én az ESS-t nagyon jónak tartom, de személyiségemből adódóan szeretem alaposan felvértezni magam, a Spyware Terminatorral és a SpyBot-tal megtámogattam. Ezek igaziból mást (is) néznek, a bönészés cookie-jait is takarítják, a megváltozott alkalmazások méretváltozására figyelmeztetnek, stb. Ezt ahhoz tudom hasonlítani, mintha lenne Casc és blokkolásgátló a kocsiban, de mégis tennénk bele pluszban sebváltózárat és trükkös gyújtáskapcsolót is. Ha van kocsi a családban, gondolom értehető, miről beszélek, azt túlbiztosítani szinte nem is lehet. Ennek ellenére elvileg azért egy trailerrel esetleg elemelhetik (nagyon kis esély százalék), de elvileg előfordulhat, ahogy 100%-os vírusvédelem sincsen, csak jó meg nagyon jó.

doki64 2008.02.17. 17:44:25

Rambo: Köszönöm a gyors és kielégítő válaszát.
Üdv. doki

Gmail postafiókok veszélyben - frissítve

2007.09.26. 21:22 | Csizmazia István [Rambo] | 15 komment

Címkék: google gmail csrf noscript itbn

Olvasom a Techline beszámolóját a Google Mail-ről. A 26-án keltezett írásból az a riasztó hír derül ki, hogy Petko Petkov hacker (aki korábban például a PDF fájlok sebezhetőségére hívta fel a figyelmet, most **a Gmailben talált kritikus sebezhetőséget**. A hiba egy CSRF (Cross Site Request Forgery) típusú backdoor segítségével használható ki, amelyet Petkov elmondása szerint egyelőre nem hoz nyilvánosságra, hogy **a Google-nak legyen ideje** reagálni, illetve javítani.

Az eredeti Petkov féle 25-én keltezett leírást elolvasva értesülhetünk arról, hogy a Zdnetes blogjában 26-án Ryan Naraine a sérülékenységet igazolta.

Ami további érdekességgel szolgál, az a **Petkov féle blog kommentjei** között olvasható:
egyrészt egy Buherator nicknevű egy másik sérülékenységről szóló blog oldalra hívja fel a figyelmet, ahol 24-i keltezéssel már POC (Proof Of Concept) kód is található. A kommentezők szerint azonban ez állítólag egy másik sebezhetőség, de nagyon hasonlóan ugyancsak a Gmail ellen irányul.

A további **kommentekből** az derül ki, **a hiba javításáig** jót teszünk magunkkal, ha a Mozilla Firefox böngészőben használjuk a NoScript bővítményt, ez alaphelyzetben blokkolni tudja a Cross Site postot. Mindenesetre a Gmailesek tartsák szárazon a puskaport ;-)

Frissítve:
Közben rájöttem, hogy a Buherator egy hazánkfia, és igen remek technikai blogot vezet.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Ez történik a weben egy perc alatt
- 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/178053

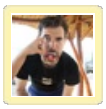
Kommentek:

zoltan galantai phd · http://mono.eik.bme.hu/~galantai 2007.09.27. 12:13:02

jó tudni, mert - szerintem - sokan használnak gmailt a magyarok közül is...
viszont nem teljesenvilágos, hogy az ITBN hogyan kapcsolódik ide: ott is erről volt szó?

Srí 2007.09.27. 12:30:19

Szia rambo! Kérdésem lenne: a NOD32 30 napos próbaverzióját használom. Ha utána megveszem, csak annyi a dolgom, hogy egyszer fizetek és kész? Minden frissítés, egyebek automatikus lesz? Nyilván magától értedődő amit kérdezek - másoknak. De én nem tudom.



Hargita Nándor · http://indafoto.blog.hu 2007.09.27. 12:55:40

&srí ha egy éves licenszt veszel akkor egy évig igen. utána kapsz emilt a sicontacttól, akik a hazai forgalmazók, hogy hamarosan lejár a licenszed.

ha lejárt, utána már nem tudsz frissíteni. De akinek a vírus és kártevőmentesség nem ér meg éves szinten ~6000 forintot az magára vessen :)

ja, és a hosszabbítás már olcsóbb.

Rejtélyes 2007.09.27. 12:58:19

Valamint ha van egy diákod, akkor félárú :) És ha igazán spórolni akar valaki, akkor úgy időzítse, hogy a tanulmányai utolsó évében vegyen 3 éves hosszabbítást :D Lehet :)

Srí 2007.09.27. 13:14:19

Köszi:) Jó hírek:)

satie · http://321.hu/sas 2007.09.27. 14:17:37

1998-ban kényelmetlenné vált nekem az akkori operációs rendszerem és átálltam Linuxra (Debian disztribúció). Azóta követem a konkurrens operációs rendszereket (Open/FreeBSD, Solaris, MacOS, Windows, stb...) de még mindig a Linux a legkényelmesebb. Naponta sok tucat kártevővel találkozom, de még egyik se ártott a rendszeremnek. Miért érné meg még évi 6KHuf-ot is fizetni? :-)

softcore 2007.09.27. 14:29:10

Én is gmail+noscript kombóban levelezek.

Amikor mások ideülnek a gépemhez, akkor bosszantja őket a szkriptek külön-külön engedélyezése az először látogatott lapokon. Tényleg zavaró, amikor egy kitöltött űrlapot azért nem tudsz elküldeni, mert annak a szkriptjét még nem engedéyezted előzőleg. Mi jön ilyenkor: engedélyezés/lapfrissítés/újrakitöltés/küldés. Igaz ami igaz, nem is szenvedek a kémprogramoktól.

Total_KO 2007.09.27. 14:50:44

Vírusvédelmi és tűzfalszoftverre mindig kapok ingyenes vochert. Szerencsés vagyok, vagy akkor most nem értem mi van...

softcore 2007.09.27. 15:02:13

satie: milyen gyakran telepíted újra a Linuxot és ez mennyi időd veszi el? Tényleg érdekel, nem flamelni akarok.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.27. 18:22:44

@galantai:
Szia! Jogos az észrevétel (Gmail vs ITBN), szétválasztottam a postot.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.27. 18:25:04

@Srí:
Szia! Az előttem szólók már megelőztem, és mindent megválaszoltak, köszönet érte :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.27. 18:31:11

@satie:
Szia!
Sok tekintetben igazad van - egyébként én is használok a Windows mellett Ubuntu Linuxot - de azért előfordulnak (persze jóval csekélyebb mértékben) kártevők Linuxra is. A vírusokat általában mindig arra a platformra fejlesztik leginkább, amelyik a legjobban el van terjedve, illetve emellett széleskörben hozzáférhető a dokumentációja. Másrészt sokan vannak, akik kötve vannak a Windows használathoz a munkájuk és a rajta futtatott szoftverek (pl. Exchange, AutoCAD, Macromedia, stb.) miatt. Magyarul van, aki nem választhat, és a Windowsra tényleg élet-halál kérdés a biztonsági program megléte.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.09.27. 18:33:49

@softcore:
Én is így látom, sőt külön öröm, ha pl. egy hírportálon csak a főoldal van engedélyezve, a sok ...ad... hirdető meg nem, a biztonság mellett még erre is jó ez a dolog.

buherator · http://buhera.blog.hu 2007.10.03. 20:27:54

Kicsi a világ :)

@softcore
Én Ubuntuzom, és eddig 1x telepítettem újra 2 év alatt, azt is azért mert lusta voltam utánamenni a hibának

A linux viszont semmit sem ér egy CSRF/XSS ellen (bár az antivírus sem, ha jól emlékszem), NoScriptet minden gépre!

Egyébként ha bejelentkeztek GMailbe, láthatjátok, hogy megváltozott a session ID (az URL végén lévő véletlennek tűnő karaktersorozat) formátuma, szóval lehet hogy ez már a javítás jele...de nem biztos.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.03. 21:00:41

Szia buherator!

Köszi a látogatást :-)

A következő Hacktivityn majd dumálunk, de addig is felvettelek a linkboxba.

ITBN - Az Informatikai Biztonság Napja

2007.09.26. 22:25 | Csizmazia István [Rambo] | Szólj hozzá!

Lezárult a harmadik ITBN, érdemes volt elmenni. Az alaphangulatot megadta a számos előző-előző munkahelyemről (kb. 25 évre visszamenőleg) érkező kollégák jelenléte, és szerencsére a folyosón volt alkalom hosszabb-rövidebb ideig pár szót váltani velük.

Ízelítőnek egy pár fotó a konferenciáról:

Ze'ev Rubinstein az izraeli CERT alapítója beszél

Keleti Arthúr (ICON Zrt) figyeli az elődásokat

John Parker (McAfee) a botnet hálózatokról beszélt

A figyelmes hallgatóság az egyik terem nézőterén

Keleti Arthúr az adatszivárgás kapcsán Rodolfó mestert is megidézte...

Fekete vagy fehér - tette fel a kérdést tiszta fehérben Gombás László (Symantec)

Liam Ryan, a Sophos szakértője

Szigetvári József (IDG) az elnöki pódiumon

Szappanos Gábor (VirusBuster) a víruskeresők jelenéről és jövőjéről beszélt

Ajánlott bejegyzések:

- Ez történik a weben egy perc alatt
- Safe mód a Mechagodzilla ellen
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/178878

Kommentek:

Nincsenek hozzászólások.

Lesben áll egy cáááápa, hajajaj

2007.09.28. 19:15 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: trójai nod32 shark hancu upx

Semmi különös, nem buggyant meg a blog tulajdonos, és egyáltalán nem ezért dudorászik Neoton slágareket :-)

A mai post ugyanis egy érdekes Index cikket szeretne ajánlani, amely tartalmában mintha egy Hacktivity workshop lenne, a Shark nevű trójai készítő programot próbálta ki és mutatta be a szerző a borzongó nagyérdeműnek. A cikk címe is igen kifejező: A hülye is tud vírust írni.

A rettegett vizibestia nyitóképernyője

A történet úgy kerek, ahogy van, én már csak minimális kiegészítést, apró észrevételeket tennék hozzá. Az eszközt sajnos valóban nem túl nagy fáradtsággal meg lehet találni a neten, igaz a készítők weboldalát időközen kivonták a forgalomból. A bemutatott program valóban lenyűgöző, jelszólopástól kezdve a kifényképezett képernyőképeken át a rögzített audio adatfolyamokig UPX csomagolással - van itt minden, mint karácsonykor.

A NOD32 szépen teszi a dolgát, a cápát fel lehet sem telepíteni bekapcsolt antivírus mellett

Azt mindenképpen szerettem volna ellenőrizni, mit jelez a víruskereső egy elkészült kártevőre

Még egy apró érdekesség: az Indexes cikkben említett YouTube videóban egy pillanatra felvillan (direkt vagy véletlenül?) egy IP cím, és amit már az előadó kiejtésből is lehet sejteni, a film készítője nagy valószínűséggel angol (United Kingdom) illetőségű.

Idősebbeknek és katonaviselteknek érdekes lehet a cikkíró személye is, aki nem más, mint Hancu a legendás Commodore Világ csapatból :-)

Ajánlott bejegyzések:

- Gyerek-barát netezés

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/180071

Kommentek:

Nincsenek hozzászólások.

PDF a biztonságos?

2007.10.05. 20:53 | Csizmazia István [Rambo] | 2 komment

Címkék: microsoft adobe pdf iframe exploit sebezhetőség

Sokan úgy tartják, az Adobe Portable Document Format állományai képviselik a megtestesült megbízhatóságot. Formázott, egységes, szabványos, ha kell, hivatalosan kinéző, ezért amikor így kapunk állományt e-mailben, vagy letöltésnél találkozunk vele, biztosak lehetünk abban, hogy semmilyen veszély nem fenyeget minket. Az hogy ez talán mégsincs egészen így, azt megtapasztalhattuk a nyár folyamán, amikor a spamküldők - igaz "csak" ideiglenesen - de átnyergeltek a PDF melléklettel felvértezett kéretlen levél üzenetekre, közben pedig időről időre újabb sebezhetőségekről szóló beszámolók is felkorbácsolták a nyugalmat.

Azt valószínűleg kevesen gondolták még át, hogy egy PDF állomány belsejébe éppolyan könnyedén rejthetők kártékony scriptek, mint azt mostanában egyre jobban tapasztalhatjuk különféle weboldalaknál. Ilyenkor az oldalt feltörik, és egy Iframe exploitot helyeznek el benne észrevétlenül, ami egy kártékony kódot letöltő oldalra juttatja a gyanútlan felhasználót. A tiszta, megbízható oldalak tulajdonosai pedig a nehezen ellenőrizhető reklám bannerek miatt aggódhatnak.

Ezzel az átlag felhasználó máris mattot kapott: hiába nem látogat pornó, warez és egyéb veszélyesnek ítélt szájtokat, elvileg bárhol, bármikor áldozatul eshet egy rosszindulatú linknek.

A Heise.de oldal adott hírt arról, hogy valóban könnyen lehetséges egy olyan preparált PDF dokumentumot előállítani, amely egy beágyazott kártékony linket tartalmaz. A próba kedvéért a számológép (CALC.EXE) alkalmazás elindításával demonstrálták a jelenséget, de viszonylag csekély fantáziával is el lehet képzelni, mekkora a veszély. A Heise felvette a kapcsolatot az MSRT csapattal, hogy értesítsék őket, a Microsoft azonban úgy látszik, nem vette komolyan ezt a feltehetően nulladik napi (zero day) sérülékenységről szóló figyelmeztetést.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- 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

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/187499

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.06. 09:08:42

Egy kis elrettentés: már kattintás nélkül is működik:
buhera.blog.hu/2009/03/05/kodfuttatas_pdf_fel_kattintas_nelkul

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.23. 08:56:06

Mivel az Adobe Reader átvette az Internet Exlorertől a megtisztelő "vírustanya" címet, itt lehet kutakodni alternatív PDF megjelenítők után, mindhárom platformra:
pdfreaders.org/

Netizenek vagyunk-leszünk

2007.10.06. 09:18 | Csizmazia István [Rambo] | 1 komment

Címkék: microsoft google gmail tv calendar stream online password pincode

Fogyasztjuk a médiát, és a hangsúly egyre inkább áttevődik az online tartalmakra. Évek óta várható az a pillanat, amikor az online hirdetési piac a nyomtatott elé vágva beelőz. A gyerekeink már több YouTube, és hasonló online tartalmat fogyasztanak, mint televíziós műsort. Magam is kóstolgatom, fogyasztom az online TV csatornákat, és már szinte csak egy jó filmért vagy DVD-ért kapcsolom be a televíziót.

Pár éve sokan megmosolyogták a bloggereket, de mára az Indexen is külön box és aloldal szolgálja ki az érdeklődök mohó olvasási igényét. Például egy Tóth A. W. blognál nem csak az olvasottság szökik az egekbe, de az olvasókból is komoly reagálásokat vált ki, szinte nincs is olyan postja, amihez ne lenne több száz hozzáfűzött komment pro és kontra. Egyébként ez is jó dolog, hogy a portálok hírei, és a postot író véleménye mellett a hozzászólásokat is böngészhetjük, ezekben gyakran találhatunk érdekes, tartalmas, velős beírásokat (az elkerülhetetlen flamewarokon túl) - ezek nélkül szinte csupasz lenne a blog.

A szemünk előtt nőtt óriássá a Google, és mindenképpen hozzáteszem, nagyon szeretem a keresőjét, jónak tartom hogy nem álltak le, és folyamatosan új dolgokon törik a fejüket, fejlesztgetnek. Viszont a hirtelen növekedésben kicsit a Microsoftnál észlelhető mamut jelenségek is felszínre kerülnek. (Volt egy jó mondás ezzel kapcsolatban: a Microsoft csak a javunkat akarja, ne adjuk oda neki :-D) Emlékezhetünk, ha valamilyen súlyosabb Windows hibára derül fény, először nem kommentálják, majd később jelentéktelennek ítélik, és bejelentik, mérnökeink már vizsgálják a bejelentést, valamint hogy egyetlen ezzel a sérülékenységgel kapcsolatos panasz sem érkezett eddig hozzájuk, de azért addig is csak biztonságos forrásból származó tartalmakat nyissuk.

A múltkori Gmailes hibák napvilágra kerülése után a Pénzkeresők konferencián feltettem a kérdést a Google magyar képviselőjének, hogy mennyire biztonságos a rendszer, és miért nem olvashatunk reagálásokat a hibával kapcsolatban, ígéreteket a javításra, stb. A válasz az volt, hogy aggodalomra semmi ok, mérnökök százai dolgoznak a biztonság érdekében. Nem igazán erre számítottam, hiszen a Microsoftnál mérnökök ezrei dolgoznak szintén a biztonság érdekében, és látjuk mennek vele ;-)

Valahogy az én észjárásommal nem illeszkedik az, ha valaki mint magánember, vagy ne adj' Isten a cége dokumentumait a Google Dokumentumok internetes megoldásával készíti, és ott tárolja. Biztosan megfordulna az összeesküvés elmélet is a fejemben (ha esetleg világuralomra törnének, jól jöhet nekik a sok hozzáférhető információ ;-), de ha az ott tárolt információk biztonságára gondolok, hogy ahhoz külső illetéktelenek esetleg hozzáférhetnek, hát nekem nem lenne bizalmam a könyvelést, és a céges levelezést odatelepíteni - biztosan bennem van a hiba, én egy ilyen bizalmatlan, paranoid kispolgári csökevény vagyok. Tegnap olvastam a Webisztánon, hogy már fél éve ismert az a Google Calendar hiba, ahol más felhasználók naptári bejegyzéseit (köztük bizalmas, nem ritkán jelszavakat is tartalmazó beírásait) bárki szabadon nézegetheti, megborzongtam.

Eddig nem használtam, nem néztem, de tegnap kipróbáltam, és valóban ijesztő, amit látni. Szerencsétlen egyszerű felhasználók, akik megmenekülhettek volna mindettől, ha egy jól látható checkboxban a "Nem Public" lett volna az alapértelmezett érték. Sokan biztosan nem vették volna ki a pipát, hogy most rajtuk nevessen-sírjon a fél a világ. Az igaz, hogy aki mostantól hoz létre naptárt, az végre már a kezdeteknél eldöntheti, hogy publikus akar-e lenni, vagy sem - számomra valahogy a Linuxos megközelítés szimpatikusabb, minden port, lehetőség, stb. zárva van, amíg én magam azt nem engedélyezem - de ez sajnos már nem segít azokak, akik korábban véletlenül, vagy

tévedésből publikussá tették határidőnaptárukat. Azt, hogy a gond nem kicsi, rögtön észrevehetjük, ha nem csak a Webisztánban említett password szót gépeljük be a Search Public Calanders ablakba, hanem például olyanokat, hogy pincode.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- 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/187898

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2007.12.03. 12:03:56

Na csak annyit akartam hozzáfűzni, hogy a dolog sajnos ma is úgyanúgy működik, a csapatban még annyi kezdeményezés sem volt, hogy mondjuk az adatbázisban *.* naptárt priváttá tesznek, aztán elnézést kérnek, és javasolják, hogy akinek tényleg public kell, az most kattintson. Úgy tűnik, az ügyfelek adatai nem érnek meg ennyi kényelmetlenséget :-(

Csak kattint, és kattint, és kattint...

2007.10.08. 16:17 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: blog video youtube orosz török svéd hacker támadás észt

A social engineering szerves része, hogy a figyelmes és leleményes rosszfiúk mindig tudjanak találni olyan **érdekes híreket, címeket, levél subjecteket, csalogató állományneveket, weboldalakat**, amelyek elaltatják az éberségét annak, aki rendelkezik egyáltalán ilyesmivel. Az egyik friss hír szerint egy 20 esztendős trükkös kínai mérnök elkészítette a Being2008 olimpiai honlap tökéletes másolatát, és annak segítségével különböző csalásokat hajtott végre, míg le nem tartoztatták.

De nem csak az a kérdés, hogy milyen érdekes témával lehet próbálkozni, hanem hogy milyen állományokkal kapcsolatban. Persze most nem is a jólismert rejtett, kettős fájlkiterjesztésekre gondolok, hanem valódi, **JPG, AVI, PDF és egyéb állományba csomagolt kártevőkre**. Nem új a téma, hiszen az úgynevezett binder programokkal lehet olyan képeket, vagy moziállományokat készíteni, amelyek a bennük rejlő futtatható kódot észrevétlenül végrehajtják. Egy friss felmérés szerint, amelyben mintegy háromszát biztonsági szakértőt kérdeztek meg, mik lesznek várhatóan 2008 internetes biztonsági fenyegetései. A válaszokból az derül ki, hogy miután a vállalatok komoly erőfeszítéseket tesznek a levélforgalom szűrésére, az emailekről a hangsúly át fog tevődni más területekre. Miután sokan megtanulták, hogy ne nyissanak meg ismeretlen, és gyanús leveleket, hogyan kezeljék a phishing gyanús emaileket, ezért **most a médialejátszók ideje látszik felvirágozni**.

Zuhanórepülés lehet a vége a meggondolatlan letöltésnek

Már magyar producer is fenyegetődzött azzal, hogy szándékosan megfertőzött kópiákat fog feltölteni az internetre. A sláger **a YouTube videomegosztó oldal és annak filmjei**. Ezek linkjei jönnek mindenhonnan: idegenektől és ismerősöktől érkező levelekben, honlapok cikkjeiben, stb. Az emberek hozzászoktak, hogy ne kattintsanak a banktól érkező linkre, de a videókat látni akarják, és a dolog működik. Fokozott veszélynek lesznek még kitéve a felmérés szerint a közművi hálózatok, a blogok és a wiki oldalak. Ezeknél igyekeznek majd olyan programokat elrejteni, amelyek a háttérben észrevétlenül igyekeznek kódjukat lefuttatva kémkedni, weboldalakat eltéríteni, bizalmas adatokat eltulajdonítani.

Nem lehet minden videofájl mellé egy forgalmi rendőrt állítani ;-)

Ha a szakmai tudás és a rosszindulat megvan, nem állhat semmi az elektronikus támadások útjába, elég ha csak a tavaszi észt-orosz konfliktusra gondolunk - igaz ez csak találgatás, bizonyítani nem lehet semmit. Egy hadüzenet nélküli háború, ahol orosz kormányzati IP címekről is indultak támadások? Volt-e tényleges állami közreműködés? Vagy csupán elszigetelt csoportok harca volt? A választ nem ismerjük, és talán soha nem is fogjuk megtudni.

Hasonlóan feszült a helyzet mostanában a svéd-török relációban is, ahol **török hackerek mintegy ötezer svéd honlapot támadtak meg**, miután a muszlimokat sértő karikatúra jelent meg egy svéd újságban. Az újságíró fejére 100 ezer dolláros **vérdíjat is kitűztek**, és az indulatok igencsak magasra korbácsolódnak, mert a svéd nyilatkozatokban a török fél által remélt bocsánatkérés helyett inkább azt kommunikálják, hogy nem éreznek semmiféle bűntudatot a történtek miatt, valamint arra hívják fel a figyelmet, mindenkinek hozzá kell szoknia ahhoz a tényhez, hogy nyugaton egyáltalán nem szokatlan az effajta élcelődés. Úgy tűnik nem csak az egyéni felhasználóknak, de az országoknak is fel kell készülniük egy esetleges hadüzenet nélküli elektronikus támadás elleni védelemre.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Majdnem mindenki átverhető adathalászattal
- 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/190247

Kommentek:

Nincsenek hozzászólások.

Halló, itt a bank ügyintézője! Vagy mégsem?

2007.10.09. 09:33 | Csizmazia István [Rambo] | 1 komment

Címkék: voip hacktivity bank korea csalás phising vishing

Ha most azzal kezdem, hogy megfelelő szakértelem és programok birtokában a Voip alapú beszélgetéseket is le lehet hallgatni, ezzel nem mondok semmi újat, ennek látványos demonstrációjához volt szerencsénk a legutóbbi Hacktivity konferencián is.

Ami viszont újszerű megoldás a csalás bizniszben, hogy a trükkös elkövetők a bank ügyfélszolgálata nevében jelentkeznek.

Koreában mindenesetre lecsaptak az ottani legnagyobb jelszóvadász csoportra, az akcióban kínai szál is szerepelt egy illegális bevándorló bandatag személyében. Az elkövetők a telefonban magukat a Pénzügyi Ellenőrzési Hivatal (Financial Supervisory Service) munkatársainak beállítva azzal a mesével próbálkoztak, hogy az ügyfél számlázási adatai kiszivárogtak, ezért haladéktalanul másik számlára kell átmozgatni a pénzt. Általában valamilyen bank, hitelkártya cég, vagy pénzügyi kormányzati szervezet nevében jelentkeztek, és ezzel a trükkel 25 embertől 350 millió wont (mintegy 270 ezer EUR) sikerült kicsalniuk.

Ha pénzügyekről van szó, megszívlelhetjük Virág elvtárs szavait "Az a gyanús, ami nem gyanús". Vagyis inkább legyünk a szokottnál is óvatosabbak, gyanakvóbbak. Egy idevágó idézet szerint "Jobb egy percig gyávának lenni, mint halottnak életünk végéig..." Magyar esetről nincs tudomásunk, de amint az közismert, a tavalyi év végén már magyar nyelvű levelekkel is elérte hazánkat a banki phishing, ezért nem kizárható, hogy idővel itt is próbálkozhatnak majd hasonló telefonos módszerekkel.

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- 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/190972

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.03.03. 18:13:10

Itt egy jó kis story, választ ad arra, hogy kell-e vigyázni Magyarországon, vagy sem:
index.hu/bulvar/2009/03/03/trukkos_csalok_vadasznak_idos_bankszamla-tulajdonosokra/

Citrixed van? Tudok egy jó YouTube mozit...

2007.10.10. 17:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google youtube rejtő citrix petko petkov

Petko Petkov úgy látszik megint jól belenyúlt, ezúttal a Citrix gateway eszközök sebezhetőségét vette észre és demonstrálta. Az élet újabb bizonyítéka, hogy játékos és kísérletező kedvű emberek teszik a legérdekesebb felfedezéseket. Az írás címe is figyelemfelkeltő: "Citrix: birtokolni a legális hátsóajtót".

Beszámolója szerint az érintett, támadásra nyitott oldalak között vannak kormányzati (.gov) és a hadügyi (.mil) helyek is.

Ime a bemutató Hacking Citrix video:

Amúgy a Google, és a többi kereső is érdekes eszköz, sok olyasmit is beindexel, ami aztán meglepetést okoz, persze ehhez hozzájárul a szervereken nem megfelelően alkalmazott jogosultság, és a webszerverek hiányos konfigurálása is. A bemutatóban az .ICA kiterjesztés szerepelt, mi kísérleteztünk egyet, és megnéztük, mit találunk, ha például logokat keresünk a Google-ban:

ext:log

Jönnek a találatok, persze van, ami több éves állomány, de **sok IRC csevegést**, FTP szerver használat naplózást, IP címet tartalmazó frissebb állományt találhatunk.

Hadd forduljak most a marginális irodalom általam nagyon kedvelt Rejtő mesteréhez:
"D'Artagnan, aki tőrrel és karddal szemben már annyiszor megállta a helyét, nem tudom, hogy védte volna meg lovagi nimbuszát zsebkések és szódásüvegek ellen. Általában, aki itt nem vési jól fejébe a kikötőnegyed alaptörvényeit: 'Semmi közöd ahhoz, ami nem tartozik rád' - az nagyon rövid életű lesz ezen a földön, ahol még a rendőrposztok is lehetőleg kerülik az olyan helyeket, ahol nézeteltérés van."

Az alapelv persze szép, azonban a neten lakók már jól tudhatják, hogy igencsak sokan vannak, akik nagyon is fürkészik azt, amihez ugyan

semmi közük, de valamiért könnyen vagy nehezen, de hozzáférnek, és pénzt lehet vele keresni. Mindenestre azok a szervezetek, akik Citrixet használnak, most kaptak egy komoly, jóindulatú figyelmeztetést.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Android kémprogram persze csak a mi érdekünkben
- Tízből öt kártevő hátsóajtót nyit
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/192480

Kommentek:

Nincsenek hozzászólások.

Norton, a gyors-lassú...

2007.10.11. 10:31 | Csizmazia István [Rambo] | 3 komment

Címkék: norton gyors lassú sebesség itbn víruskeresés

Még a látszatát is szeretném elkerülni, hogy Norton ellenes lennék. Peter remek könyvein nevelkedtem, abból (is) tanultam a programozói szakmát, sőt a családban is van, aki még a mai napig is a sárga dobozos programokra esküszik, és teljesen elégedett velük. Szóval az úgy volt - tisztelt Bíróság ;-) - hogy volt szerencsém végigülni az **Informatikai Biztonság Napján** megtartott szakmai előadásokat, benne az új Norton Security 2008 csomagról szóló bejelentéssel. Az előadást hallgatva először akkor lettem egy kicsit szkeptikus, amikor azt hallottam, a rengeteg új és javított funkcionalitáshoz állítólag 24 MB memória foglalás elegendő. Szerepelt azonban **egy olyan kocka is a slideban**, ami a túl magas víruskeresési sebesség káros voltát ecsetelte (szegény AVIRA, és NOD32 itt lesunyhatta volna a fejét, amiért oly gyorsan teszik ezt;-).

Erre mit látok egy tegnapi Számítástechnika cikkben :-O Még a szalagcíme is formaegyes filmeket idéző: "Norton Security: felpörgetve".

Benne pedig az alábbi idézet szerepel:

"Emellett a Norton Internet Security 2007-hez viszonyítva a 2008-as termék felhasználói felülete 22 százalékkal gyorsabban reagál, és a gyors-szkennelést 39 százalékkal gyorsabban hajtja végre. Volt szerencsénk kipróbálni a termékeket, így meg tudjuk erősíteni a fentieket, valóban kevésbé fogják meg a gépet a korábban próbált biztonsági alkalmazásoknál - gyakorlatilag nem tapasztalható semmiféle zavaró lassulás."

Eddig az idézet. Kezdek akkor végképp semmit nem érteni. Lehet, hogy a sebesség csak addig átok, amíg másé, ha már a miénk, akkor már áldás?

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
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/193133

Kommentek:

Ati82 2007.10.30. 11:07:36

Tényleg elég furcsa meghatározások.
De ez csak irigység...
Én szerintem, amit régen el...tak a nortonék, azt a nod32 teljesiti folyamatosan és most már szeretné visszaszerezni a régi kuncsaftokat, amit elvesztett a Norton a Nod32 előnyéből származóan....

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.30. 11:28:08

Szia :-)
Tényleg nem bántani akartam őket, de valahogy van egy olyan érzésem, hogy a technikai szakemberek a háttérben megfelelően tudnak beszélgetni, együttműködni, közben pedig a kereskedelmi és a marketing fronton meg sok a valós vagy vélt sértés, konfliktus, különösen itt Magyarországon.
Azt pedig már nem is mertem odaírni az eredeti cikkben, hogy Peter Norton a vírus korszak hajnalán nonszensznek és nem létező problémának titulálta a dolgokat, azt mondta: ez csak egy városi legenda, és annyi alapja van, mint hogy krokodilok úszkálnak a New Yorki csatornákban. Aztán csak később ébredt rá, hogy muszáj felkapaszkodnia a szekérre, ha nem akar lemaradni.
Azért azóta jól belehúztak, és nyugaton nem lehet úgy bemenni egy számítástechnikai üzletbe, hogy plafonig érő sárgadobozos polcokkal ne találkozzunk ;-)

Ati82 2007.10.30. 12:02:44

Lehet.De ez nem nyugat. A Kereslet és Kinálat nem úgyanaz...
Igaz, függ egyik a másiktól, de attól , hogy a "polcokon" tömve van a Norton termékekkel, az nembiztos, hogy keresik is olyan arányban...
Egyébként itthon is bárhova bemegyek(számtech bolt vagy bevásárló központ, stb) a polcokon csak a Kaspersky és Norton termékeit látom kirakva kinálatban, pedig Keresettebb "itthon" a Nod32 ;)

Foltozó kedd - Exploit szerda

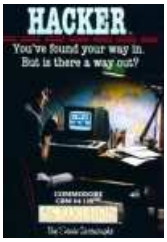
2007.10.12. 16:42 | Csizmazia István [Rambo] | 4 komment

Címkék: microsoft hiba kedd szerda hacker word exploit sebezhetőség

A világ már csak ilyen, logikus szabályokra épül, ahol **minden szereplőnek megvan a maga érdeke**. Vagy másképpen: érdek a világ ura a Zero Day esetekben is. A Microsofté az, hogy ilyenkor kijelentse, a hiba nem új, már kihasználták ezt megelőzően is, vagy a másik verzió szerint nincs tudomásuk a sérülékenységet konkrétan kihasználó eseteről. A támadók pedig sokszor egy egész hónapot nyernek az exploit kódok kihasználására, és ezt a laza időszakot csak egy esetleges gyorsan kiadott, rendkívüli frissítés veszélyeztethetné. Persze konkrét igény és érdeklődés jelentkezik az ilyen nulladik napi kihasználható kódokra, még árverési portál is létezik hozzá.

Kritikus hiba a Wordben - akad-e valaki, akinek ez a szalagcím egy sosem hallott mondatként hangzik? Talán arra már felkapnánk a fejünket, hogy "ma egy hibát sem találtak az x termékben". A Word alkalmazásban olyan kiemelten kritikus minősítésű hibát fedeztek fel, melyet **egy speciálisan megformázott Microsoft Word állománnyal** lehet kihasználni, és ha ezt a gyanútlan áldozat megnyitja, távoli kód végrehajtása válik lehetségessé - ami ugye nem hangzik túl jól, és ráadásul a felhasználók zöme adminisztrátori jogokkal rendelkezik.

Szerepe szerint a **Microsoft ilyenkor azt tanácsolja**, a hiba kijavításáig (hányadik ilyen is ez?) csak megbízható forrásból származó dokumentumokat nyissunk meg. Jó hír lehet az Office 2007 és az Office 2003+Service Pack 3. felhasználóknak, hogy őket nem érinti az említett veszély.



Nem szabad igazságtalannak lennem, fizikailag gyakorlatilag **elképzelhetetlen, hogy egy ekkora kódban sose fedezzenek** fel újabb, és újabb sebezhetőséget. Úgy rémlik, ez a kiszámítható havi patch rendszer nem váltja be a korábban hozzáfűzött reményeket.

Azért egyszer szeretném megélni, hogy valaki már nem csak pusztítatni, hibát kihasználni, hanem mondjuk javítani, a rászorulókon segíteni, vagy netán építeni akarjon. Például egy olyan találmány, amit ha eldobok, a helyén rögtön lakóház nőne ki a földből, vagy egy nagy terített asztal keletkezne az éhezőknek, éppenséggel tetszene. Na jó, tudom, ábrándozás az élet megrontója, na meg a számítógép is utasításaink szerint, és nem kívánságaink szerint működik, továbbá az élet nem habostorta. Kár...

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Elégedetlenek vagyunk a Facebook biztonságával
- 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/194506

Kommentek:

buherator · http://buhera.blog.hu 2007.10.12. 21:14:48

"Azért egyszer szeretném megélni, hogy valaki már nem csak pusztítatni, hibát kihasználni, hanem mondjuk javítani, a rászorulókon segíteni, vagy netán építeni akarjon."

Az igazi hackerek pont ezt teszik, csak ők ugye kevesebb sajtóvisszhangot kapnak...

Ezt a frissítőkedd dolgot egyébként nem értem. Az MS elvileg azért találta ki, hogy időzíthetőek legyenek az upgrade-ek, de ez miért zárja ki, hogy a frissítéseket azonnal kézhez kapjuk?

Egy Debianon nincs ilyen probléma, és ha akarok, két sorból csinálhatok magamnak frissítőkeddet, -szerdát, vagy amit akarok.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.12. 21:31:39

Szia :-)

Minden elismerésem a hackereké, főképp, ha fehér sityka van rajtuk, földig emelem a kalapom a tudásuk, a leleményességük előtt. Igyekszem a szemléletből én is inhalálni egy picit...

A frissítő keddel szerintem az a probléma, hogy:
- a Windows nem nyílt forráskodú
- kénytelen vagyok kivárni, amíg a javítás megérkezik

Én egyébként Ubuntuzom (ami nagyban Debian kompatible) és nagyon szeretem. Egy rendszergazdi ismerősöm muterjának először XP volt telepítve, és nem igazodott ki rajta, mindig volt valami baja. Utána kapott Ubuntut, és ezzel teljesen elégedett :-)

buherator · http://buhera.blog.hu 2007.10.13. 10:00:01

A zárt forrás még nem szabadna, hogy problémát jelentsen, van sok ügyes programozó a MS-nál, írjanak egy GUI-t, mint az update-manager+cron, pakolják be a beállításokat a registrybe, és meg van oldava a probléma.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.13. 10:48:42

Jogos a két pont. Lehet, hogy lemaradt a problémalistámról a harmadik szepont ;-)
- valószínűleg egyelőre nincs rá hajlandóságuk, hiszen így is dől a lé. Talán a jövőben, ha majd üzletileg megszorongatják őket a versenytársak, akkor jobban fogják keresni, mi is a felhasználók érdeke.

Amikor a fagylalt visszanyal - Frissítve²

2007.10.13. 08:22 | Csizmazia István [Rambo] | 4 komment

Címkék: spam médiahack orosz gyilkosság viagra botnet szemétlevél alexey tolstokozhev murdered

Vannak határai az emberi béketűrésnek, amikor úgy érezzük: eddig, és ne tovább. Ez a limit persze esetenként és egyénileg változó, én arra emlékszem, amit anyám mesélt mindig: arra még rávehető az ember, hogy hagyja, hogy eltapossák és tönkretegyék, de hogy még meg is tapsolja, azt aki tönkretette, hát azt már nem! **Úgy tűnik, vannak akiknek megint megtelt a hócipőjük a kéretlen levélszeméttel**: Moszkvában egy nagyban játszó spammert, Alexey Tolstokozhevet állítólag meggyilkolták. Érdekes az észrevétel, hogy ha a nevét megpróbáljuk lefordítani, az 'ThickSkin', vagyis vastagbőrű, érzéketlent jelent.

Tolstokozhevet a híradás szerint luxuslakásában találták meg, aki korábban millió számra küldözgette a Viagra, Cialis, pénisz növelő (hahó, és nem növesztő ;-) tablettákat és egyéb gyógyszereket ajánlgató emailjeit, és szolgálatait is közismerten különféle gyógyszergyárak honorálták. A Viagrával kapcsolatos levélszemét forgalom 30%-át neki tulajdonítják, ehhez **gyaníthatóan a hackerektől bérelt botnet hálózatot**. 2007-ben megszerzett jövedelmét 2 milliós amerikai dollárra becsülik, ebből nyilvánvaló, hogy az efféle tevékenység igen jól jövedelmező. Csak összehasonlításképpen, egy orosz átlagfizetés körülbelül 400 dollárnak felel meg.

Tolstokozhev nem az első orosz spammer áldozat lenne, mint közismert, 2005-ben Vardan Kushnirt gyilkolták meg valószínűleg hasonló indíttatásból. A kérdések kérdése azonban csak most következik. **Vajon igaz-e ez a mostani hír?** Ha körülnézünk a ROKSO-n, **nem találjuk**, és ez azért érdekes, hiszen a **SpamHouse Toplistája** alapos szokott lenni. A névre rákeresve túl sok érdemi találattal a Google sem kényeztet el bennünket, egy Sunbeltes blogban meg egyenesen beugratásnak tartják a hírt.

Lehet, hogy tényleg csak mediahack az egész? Oroszország messze van, nehéz a hírek valóságtartalmát ellenőrizni, a sok hírportál pedig bambán átveszi, aztán jön az Igazi Mao, meg a Magyarabok Afrikában, és hasonló agyament, de roppant szórakoztató történetek.

Ha a spamellenes törvényi szabályozás nem éri el a célját, talán a szelíd rábeszélés használ ;-)

Hogy a hír valós-e, nem vennék rá mérget. Az azonban bizonyos, hogy a gyilkosság valóban durva válasz lenne, ennek ellenére a környezetemben **sok olyat ismerek, akik szíves-örömest eltöltenének** néhány percet egy ilyen spamküldővel egy zárt, sötét helyiségben :-)

FRISSÍTÉS +++ FRISSÍTÉS +++ FRISSÍTÉS

Buherator kolléga jó érzékkel jelezte, az eredeti hírt megjelentető oldal elég érdekes körülmények között jött létre, a Domaintools bejegyzése szerint két napja, 2007.10.11.-én foglalták egy kétes hírű webhosting cégnél. További **"feltételezések szerint elképzelhető, hogy a hír elterjedése után kártékony kódot installálnak rá, hogy a nagy hírportálokról érkezők tömegeit fertőzzék meg!"** Köszönöm a kommentet :-)

Ha valaki most próbálja megnyitni az oldalt, akkor ez a kép fogadja

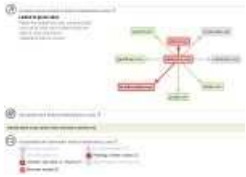
Az oldal forrásában pedig ezt látni:

* because of a huge amount of traffic this post received, I had to temporarily shutdown the blog leaving only the cache version
*
<!--LiveInternet counter--><script type="text/javascript"><!--
document.write("<a href='http://www.liveinternet.ru/click' "+
"target=_blank><img src='http://counter.yadro.ru/hit?t44.6;r"+
escape(document.referrer)+((typeof(screen)=="undefined")?"":
";s"+screen.width+""+screen.height+"*"+(screen.colorDepth?*
screen.colorDepth:screen.pixelDepth))+";u"+escape(document.URL)+
";"+Math.random()+
"' alt=" title='LiveInternet' "+
"border=0 width=31 height=31><\/a>")//--></script><!--/LiveInternet-->

Ami végül kétségtelenné teszi, hogy hülyének lettünk nézve, az kiderül a következő képből. Ha rá kattintunk a "this post" linkre, akkor láss csodát: a 2007.10.11-én bejegyzett domain blogja azt mutatja, mintha már februárban is lettek volna bejegyzések, kóbor apácák megtévesztésére. Mi most ez nem ettük meg, a világvége elmaradt.

FRISSÍTÉS2 +++ FRISSÍTÉS2 +++ FRISSÍTÉS2

Ha a Googleban rákeresünk a "estdomains.com malware" szavakra, meglepősen sok találat bukkan fel, szinte szinonim szavakként látjuk a riportokban. Úgy tűnik, sok korábbi gyanús esetben bukkant fel az Estmedia.com neve.



Voltak, akik komolyan vették

Sorry vagyok a hegyről, véletlenül minden linkem ide mutat...

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- 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/194822

Kommentek:

buherator · http://buhera.blog.hu 2007.10.13. 09:53:04

Szakértők szerint átverés az egész:

www.securityfocus.com/brief/606

Ahírt közzétevő domaint csütörtökön regisztrálták az egyik nem túl jó hírnévvel rendelkező hosting cégnél. Elképzelhető, hogy a hír elterjedése után kártékony kódot installálnak rá, hogy a nagy hírportálokról érkezők tömegeit fertőzzék meg!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.13. 10:42:17

Szia :-)

Nagyon is elképzelhetőnek tűnik a hozzászólásod, köszi a kiegészítést, én is frissítettem a postot.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.31. 12:46:17

Nem tudom ellenőrizni, de reméljük igaz a hír. Sajnos, amikor nem működik a jogállam (lásd felvett, de a munkásoknak ki nem fizetett pénzek a Megyeri hídnál. hozzá el nem rendelt nyomozással fél éve után), ne csodálkozzon senki, ha ököllel, Krav-Magával, viperával tesz igazságot a becsapott állampolgár a sorozatcsalóval szemben.
www.zoom.hu/szirena/internetes-csalo-44033.html?ref=hk

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.05.08. 12:48:10

Újabb újságíró "nevelési" média hack a kopi-pészt bajnokainak :-)
index.hu/kultur/media/2009/05/07/meghackeltek_a_maurice_jarre_halalhiret/

Kattintsunk-e Psycho macskára?

2007.10.15. 16:02 | Csizmazia István [Rambo] | 1 komment

Címkék: vírus macska cat psycho képeslap trójai nod32 greetingscard nuwar virustotal

Legalábbis erre biztat minket az a kéretlen email üzenet, mely a postafiókunkban landolt. Életünk része, hogy a **papíralapú üdvözlőlapok helyett egyre inkább SMS-t vagy internetes képeslapot kapunk és küldünk**. Tudva tudjuk, hogy piros betűs ünnepeken ezt a kártevők terjesztői is igyekeznek kihasználni, de ne gondoljuk azt, hogy az ünnepek közti időszakban nem történhet semmi baj. Általában igyekszünk mindenkit figyelmeztetni, hogy **levélben kapott linkre NE kattintson rá**, mi viszont tegyük éppen ezt, nézzük meg és próbáljuk ki, mi történik, ha mégis!

Amint a megadott linkre kattintunk, egy hamisított Greetings Card küldő oldalra jutunk, amit nemcsak a fura "76.221.199.10" címsorból vehetünk észre, hanem abból is, hogy bárhova kattintunk, a " SuperLaugh.exe" nevű trójai próbál meg letöltődni a gépünkre.

A legtöbb vírusirtó szerencsére képes felismerni, így a NOD32 is fityiszt mutatott a kártevő letöltési kísérletének.

Ideiglenesen kikapcsoltuk a víruskereső aktív védelmét, és letöltöttünk a trójait, hogy aztán megvizsgálhassuk a VirusTotal oldalon is.

A NOD32 Win32/Nuwar.Gen néven azonosította.

Természetesen, **az eredeti képeslapküldő szolgáltatás ártalmatlan**, nem terjeszt vírust. És íme az eredeti nevető psycho macsek, innen lopta a víruskészítő a képet. Azért az eredeti lapon is van mire vigyázni, ha a beígért két hetes ingyenes account készítésénél óvatlanul megadjuk a valódi telefonszámunkat is, akkor a meglehetősen drága prémium VIP szolgáltatásra fizetünk elő automatikusan.

Úgy tűnik, túl lassan írtam ezt a postot, mert most ellenőrizve a kártékony oldalt, már szerencsére elérhetetlenné tették azt. A tanulság miatt gondolom azért mégis megérte elolvasni.

jánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- 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/197018

Kommentek:

mCucc 2012.04.01. 20:46:28

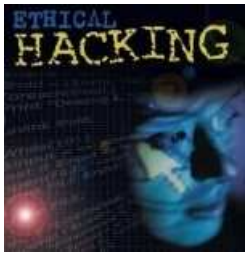
Jha, ez kb olyan mint az express-files.com ahol a virustotal szerint (úr isten! -.-) 3/41 írtó ismerte fel, és a hotmediasearch és tsa-i az adware-jükkel, de a fájlméretek is gyanúsak. Nem szaporítva a szót, ne töltsünk le nevesincs húúú de jó (kamu) hozzászólásos "szolgáltatással"! UI: mindjárt felteszem a képeket wp-re, ott meg lehet nézni
Remélem lehetett érteni amit írtam :-)
Link: mcucc.wp.com/

Etikus hackelés

2007.10.17. 11:19 | Csizmazia István [Rambo] | 4 komment

Címkék: voip sql wifi tanfolyam hacker etikus rootkit audit netacadémia mitnick

Igen, valóban létezik ilyesmi, ez nem fából vaskarika. Komoly cégek dolgoznak ezen a területen, és ajánlják a **biztonsági audit nevű szolgáltatásukat** mindazon piaci szereplőknek, akik a biztonságot mindenek felett fontosnak tartják. Persze ez nem egy statikus dolog, inkább ahhoz hasonló, ahogy a Zen buddhizmusban is a tökéletességet elérni ugyan sohasem lehet, de azért **állandóan törekedni kell rá**.



A Netacadémia egyik legújabb, Etikus Hackelés nevű tanfolyamán jártunk, ez volt az első (publikus) kurzus. Korábban már jártam itt egy Windows 2003 Server tanfolyamon - akkor személyes Fóti Marcell volt az oktató :-) - és most is a szokásos, magasszínvonalú, gyakorlatias előadást vártam, és ebben nem is csalódtam. Egy hetes volt a tanfolyam, ami tulajdonképpen inkább rövid ízelítő vagy összefoglaló, pedig **hétfőtől péntekig egésznapos, és roppant érdekes elfoglaltságról** volt szó. A téma viszont annyira bőséges, hogy aki teljesen járatlan ebben, fogalma sincs a TCP/IP protokollról, sosem programozott még semmilyen nyelven sem, nem találkozott még SQL adatbázisokkal, nem próbált meg saját erőből valamilyen problémájára megkerülő trükköt (workaround) kitalálni, az inkább csak lexikonszerű összefoglalásnak érezhette. A lényeg - mint mindenhol - itt is a részletekben lakozik, és abban ha teljesen új dolgokat nem is, de sok apró trükköt, alternatív megoldást hallhattunk, láthattunk, próbálhattunk ki a gyakorlatban.

Aki érdeklődik vagy érintett a számítógépes biztonság témakörében, annak mindenképpen javasolt, sok esetben a rózsaszín ködöt is képes megszűntetni a hallgatóban, **aki eddig bambán megbízott olyan dolgokban, mint Windows vagy Linux belépési jelszó biztonsága**, Wifi használat titkosítás nélkül, vagy WEP kódolással, de a weboldalak, SQL adatbázisok, sőt a napjainkban egyre népszerűbb VOIP kapcsolatok leggyakoribb gyenge pontjaira is fény derült, de volt szó rootkitekről, szteganográfiáról is.

Sok olyan muníciót adott, amin továbbhaladva, nyomozva, próbálgatva, kíserletezve bővíthető az ezzel kapcsolatos ismeret. Valószínűleg a vérbeli hackereknek nem kell propagálni az élethosszig tanulás nevű programot, van arra belülről fakadó igény bőségesen :-D

Éppen a második Kevin Mitnick könyvet olvasom, a Behatolás művészetét és tényleg csak az érdesség kedvéért **egy-két mondatot** idézek belőle.

A 4. fejezet elején olvasható a következő mondat: **"Costa Katsaniotis 11 éves korában kezdett el ismerkedni a számítógépekkel, amikor kapott egy Commodore Vic-20, és nekilátott, hogy programozással fokozza a gép teljesítményét. Már ilyen zsenge korában írt egy szoftvert, amely lehetővé tette, hogy barátja betárcsázással lássa az ő merevlemezének tartalmát."** Na ez LOL - pláne hogy

én is Commodore-ral kezdtem, ha ez VIC-20-ra vonatkozik, akkor szerintem kicsit kamuizű volt. Ez persze az egyébként nagyszerű és érdekes könyv értékét nem csökkenti. A szerzőpáros komoly erőfeszítéseket tett a kényes témák miatt, hogy vezérfonalukban csak abszolút hihető, sokszorosan megerősített, illetve valószínűsített történetek szerepelhessenek a kötetben.

A másik érdekesség inkább csak a magyarországi börtönviszonyokhoz képest lehet érdekes, az egyik leleplezett hacker interjújából való: **oron volt az utolsó szövetségi intézmény, amelyben volt úszómedence, és Costa később hallotta, hogy Barbara Walters televíziós riportja eredményeképpen a medencét nem sokkal szabadulása után betemették. Személy szerint én megértem, hogy egy új börtön építésénél nem költik az adófizetők pénzét úszómedencére, de azt nem értem, hogy egy létezőt miért kell lerombolni."** Úgy tűnik, a hogyan mennek a dolgok kérdésre minden országban vannak ilyen "mérd mikrométerrel, jelöld krétával, vágd baltával" típusú intézkedések.

Ajánlott bejegyzések:

- Safe mód a Mechagodzilla ellen
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok
- Nyári tanácsok utazáshoz
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/198975

Kommentek:

bxh · http://www.mediaart.hu 2007.12.22. 07:29:43

Nekem is volt egy-két kamu szagú elem a második Mitnick "bibliában", de ez nem sokat csökkent az értékéből. Mondjuk az első közelébe sem ér. :)

bxh · http://www.mediaart.hu 2007.12.22. 07:32:25

Ja és tök durva, hogy egy csomó könyvtárban láttam már mindkét kötetet. Tök pozitív.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.22. 22:26:01

Szia Bxh!
Az első inkább technikai kötet mellett azért a második is adott érdekességeket: kedvencem az a vállalat volt, aki előtte fel akart vásárolni egy kis biztonsági céget, és el is kezdtek egyezkedni, majd ezek után megbízták őket egy teljes biztonsági audittal! A hacker srácok meg jókat röhögtek, mikor a velük kapcsolatos vezetői iratokat olvasgatták, mert persze hogy sikeresen bejutottak, és mindenhez hozzáfértek. LOL :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.04.22. 13:57:15

Megy a toborzás az USA-ban:
index.hu/tech/biztonsag/2009/04/22/hackereket_toboroz_a_pentagon/

Üdv, itt a Skype jelszólopó...

2007.10.18. 14:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: skype jelszó veszély malware trójai defender alert

Egy hírben olvastam egy olyan új kártevőről, amely a Skype felhasználóinak bejelentkezési információit és egyéb bizalmas adatait veszélyezteti. A vírus spam levelekben, fertőzött weboldalakon és azonnali üzenetküldőkön (Yahoo, MSN, ICQ, Skype) terjed. A lényeg, hogy az üzenetben szerepel egy link, amely a "65404-SkypeDefenderSetup.exe" nevű kártékony program állományra mutat.

Ha a felhasználó elindítja ezt, akkor a számítógépén egy olyan ablak jelenik meg, amely kísértetiesen **hasonlít a Skype eredeti belépési felületére**. Az egyetlen látható különbség a bejelentkezésre szolgáló gombnál észlelhető - és persze, hogy nem a saját tálcánkon, vagy start menünkben szereplő megbízható hivatkozást indítottuk el.

Ha valaki megadja a Skype-os belépési adatait, akkor a trójai az Internet Explorerből megszerzett egyéb **bizalmas adataival együtt elküldi ezeket a támadók számára**. A hamis program nem képes bejelentkezni a Skype szolgáltatásaiba, a jelszó megadása után ezért csak egy hibaüzenetet láthatunk.

A Skype biztonsági blogjában teljes részletességgel le van írva az eset, kimentett képernyőképekkel illusztrálva. Ha valaki véletlenül áldozatul esett volna, haladéktalanul cseréljen jelszót.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/200219

Kommentek:

Nincsenek hozzászólások.

Van új a spam alatt - Frissítve

2007.10.18. 11:23 | Csizmazia István [Rambo] | 3 komment

Címkék: spam mp3 commodore hang c64 sound spamszűrés

Mi jöhet még spam fronton? Bármi - jósolhatjuk bátran, megerősítve Rejtő Jenő azon gondolatát, hogy csak az fél, akinek van fantáziája. Ebből az árucikkből pedig szemlátomást nem szorulnak importra a leleményes rosszfiúk, gondoljunk csak a **képalapú, Excel és Word dokumentumokban érkező, vagy a legutóbbi PDF állományok formájában** megtestesülő kéretlen szemétlevelekre. A mostani újítás inkább vicces tűnik, **immár MP3 melléklettel is érkezhet spam**.

Erről számolt be az MPP blogja, úgy véljük, jogos a két pont, megint lehetett csavarni egyet a dolgokon, **kíváncsian várjuk a szűréssel foglalkozó szakemberek reakcióit**.

A levélben érkezett "snoring.mp3' fájlt meghallgatva volt **némi retro C64** érzésünk, a szűrőkkel agyontorzított hang a felejthetelen Sam & Reciter programot idézte fel jóemlékezetünkben, amelyben a híres Kennedy beszédet is előadta a jó öreg Commodore 64...

A nagy különbség, hogy a Sam-es beszéd így 23 év után is érthetőbb :-) C64 for President! :-)

FRISSÍTÉS +++ FRISSÍTÉS +++ FRISSÍTÉS +++

Közen egyre érkeznek az újabb levél változatok.

Ebben a másikban - a neve ezúttal "sayyousayme.mp3" - egy néhány bájttal nagyobb méretű MP3 található, a TAG mezők itt sincsenek kitöltve. Ami közös a másikkal hangfájllal, hogy mindkét állomány a Lame 3.97 verzióval készült, legalábbis a bejegyzés erről tanúskodik.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- 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/200022

Kommentek:

ihatethisindapassthingy 2007.10.18. 13:10:52

Azért nem kell kétségbeesni :) Az átlagos céges hálózaton semmi szükség nincs MP3 file-ok fogadására ismeretlen küldőktől. Ha szofisztikáltabbá akarunk válni, akkor jöhet egy összetett szabály:

- A levél bizonyos tulajdonságai (szöveg jelenléte/hiánya, max. tapasztalt hossza)

- Az MP3 file kisebb, mint a mintában legnagyobb tapasztalt. A spammernek az éri meg, ha kis file-okat kell küldenie, ezért nincs szinte 60-80K-nál nagyobb spam. A gyakorlat azt mutatja, hogy az MP3 file-ok ennél tipikusan jóval nagyobbak.

- A formátum MPEG 2.5 Layer III, Single Channel, perverz bitrate, nincs az informális hossz megadva a fejlécben (00:00), stb. az MP3-ból hiányzik az ID3 tag és pár fejlécelem, ami klasszikusan előfordul.

A három fenti fő feltételcsoport és annak alszabályai már meglehetős biztonságot nyújtanak az "MP3 spam" azonosításában. A spammerek természetesen bármikor megváltoztathatják a paramétereket, ilyenkor a szabályokat utánuk kell igazítani. Általában nem nagyon törik magukat.

A PDF spamet sem úgy érdemes megfogni, hogy megpróbáljuk belőle kinyerni a szöveget (ami adott esetben OCR nélkül nem is lehetséges, lévén a PDF elsősorban nem szöveget tárol és ha van is benne, akkor sem biztos, hogy a jó sorrendben), hanem úgy, hogy ellenőrizzük a PDF és a hordozó levél karakterisztikáit.

Just my two cents.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.18. 13:22:22

Hello ihate...!

Köszi a kommentet :-)

Rendszergizda barátom mondja, hogy náluk az MP3 melléklet alapból ki van zárva, jöhet az akár ismerős küldő nevében is.

Közben még egy olyan módszer is felmerült a repertoárban, hogy a szűrőmotorok azt is tudják figyelni, hogy egy adott levélnél megmondják, hogy nagyon hasonló levelet hány példányban küldek ki már az interneten. Ha egy levelet például milliószor kiküldtek már, akkor joggal feltételezhetően spam volt.
Én valahogy azt tippelem, ez egy POC próba, és talán nem lesz tartós a dolog.

ihatethisindapassthingy 2007.10.18. 14:30:30

Rambo, igen, sok szűrő egyfajta szignatúrát készít a levelekről és ezek felbukkanási tulajdonságait nézi, ilyen pl. a Commtouch engine-je, amit több üzleti spamszűrő is licenszel, adott esetben saját név alatt.

Mostanában sok ilyen proof of concept próbálkozás volt, de többnyire elhaltak (ZIP spam, XLS/DOC spam, a PDF is visszaesett) és szerintem az MP3 is halálra van ítélve, ami tartja magát az "egzotikus" technikák között, az az image spam. Érdekes viszont, az nem nagyon akar fejlődni. Az idézett kolléga blogjában most láttam 3D-s elforgatott image spam-et, de ez sem terjedt még el.

Szerintem a spammerek egyszerűen nem fordítanak komoly figyelmet a spam célbajuttatására. Ha ez nem így lenne, akkor a pl. Greylisting nem lehetne hatékony (bár nagyon aggresszív) technológia. Sok kicsi sokra megy alapon megszórnak bármit és csak moderált erőfeszítéseket tesznek azért, hogy átjussanak a szűrőkön. Ha túl sok levél bukik el a spamszűrőkön, akkor vesznek még pár tíz dollárért néhány millió címet. A lényeg, hogy jöjjön a commission és a kisebb ellenállás irányába haladnak inkább.

A nagy Krackin Networks átverés

2007.10.19. 18:13 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: p2p vírus vihar worm csalás hamis storm fájlmegosztó krackin netcraft cisrt networks

Szép dolog a P2P, bár a lelkesedést valószínűleg nem minden piaci szereplő osztja. Az bizonyos, hogy valamilyen formában mindenki hallott róla, találkozott vele, alkalmi vagy akár rendszeres fogyasztóként. Vagyis tökéletes csali lehet egy új fájlmegosztó lehetőség, könnyű keresés és telepítés, azonnali élvezet ígérete csábítóan hangzik. Pontosan ezért lendültek akcióba a rosszfiúk a Vihar Vírus (StormWorm) új változataival **"Krackin - The Global Sharing Network"** néven. A képen gondtalan fiatalok, csinos lányok önfeledten zenét hallgatnak, táncolnak; a feltűnő lila hátterű reklám pedig az sugallja felénk: Gyere és fogyassz, van itt minden: zene, tánc, képek, video, chat és blog. Ugorjunk hát fejest és nézzük meg közelről!

Az oldal **már a legelső pillanatban próbálkozik** - ha nem védjük magunkat például Firefox alatt NoScripttel - és automatikusan lefuttat egy XOR és unescape segítségével kódolt JavaScript programot, egy olyan preparált médiaállományra mutat, amivel QuickTime és más sebezhetőségeket igyekeznek távolról kihasználni.

Az XOR kódot szépen vissza is fordítottam, de az unescape-pel kevesebb szerencsém volt, ez valószínűleg a speciális kínai karakterek miatt lehetett.

Ez akkor is igyekszik fogást találni a gépünkön, ha magát a "krackin.exe" fájlt nem is próbáljuk meg letölteni vagy futtatni.

Mi a Google segítségével tíz ilyen URL címet találtunk, ezek **főleg Egyesült Államokbeli gépek voltak**, de volt közte már lekapcsolt marókkoi és spanyol országi oldal is. Érdekes megemlíteni, hogy a Netcraft Toolbar már most egy nap után szépen jelezte néhány oldalnál, hogy **csaló siteról van szó**.

Maga kártevő egy WIN32 PE típus exefájl, **többféle mérettel is előfordul**, nekünk egy 85,804 bájt méretű példányhoz volt szerencsénk. Megvizsgálva a VirusTotal oldallal, az alábbi értékelést kaptuk.

Matematika órán egyik kedvenc mondatom az volt "Vegyük észre, hogy...". (A másik kedvenc amikor egy lány felelt a táblánál, és elhangzott: és most a logaritmussal egyszerűsítünk az egyenlet mindkét oldalán... bűvös mondat :-) Vegyük észre mi is, hogy az is a megtévesztést szolgálja, ha valami már nem 1.0, nem 1.1, hanem szépen kiforrott 1.2 verzió, az már biztos jó lehet. Ha netán paranoiás egyedek begépelik a korábbi verziókat a keresőbe, tisztán látszik, nem volt itt semmiféle előző változat.

Mielőtt lecserélnénk korábbi jól bevált torrent vagy egyéb (tűzfal, stb.) alkalmazásainkat, **legyen bennünk némi kétkedés**, ha a semmiből egyszercsak egy varázsprogram reklámablaka jelenik meg, ami jobbnak, szebbnek, használhatóbbnak **állítja be magát, és csak a kattintásunkra vár**.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Dropbox csalival terjedtek a kémprogramok
- Küldj pénzt! - Az elveszett poggyász sztori

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/201427

Kommentek:

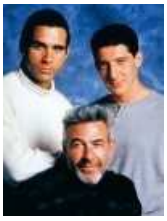
Nincsenek hozzászólások.

És ki figyeli a figyelőket?

2007.10.20. 17:07 | Csizmazia István [Rambo] | 6 komment

Címkék: kormányzat ausztria spyware megfigyelés trójai kémkedés legális kémprogram

Ha emlékezetem nem csal, úgy jó 5-6 éve volt ez téma, vajon a vírusvédelmi programok átengednék-e a kormányzati, titkosszolgálati trójai programokat, volt szó Echelon tervről, Magic Lantern kódról, és onnan lehet gyanítani, melyik gyártó működhet esetleg együtt, hogy azok nem azt mondják, hogy "nem", hanem csak simán nem kívánnak válaszolni a feltett kényes természetű kérdésre. Idén júliusban volt egy érdekes és terjedelmes írás, amelyben különböző biztonságtechnikai cégeket faggattak arról, **milyen az együttműködésük a titkosszolgálatokkal**, volt-e olyan **megkeresés vagy egyezségük állami szervekkel, hogy engedjenek át trójai vagy kémprogramokat**, és hasonló érzékeny témák - szerintem kötelező olvasmány kategória.



Jelenleg **Ausztriában kavarognak az indulatok**, miután az ottani kormány előzetesen egyet értett azzal, hogy a gyanúsítottak számítógépeit ilyen módon is ellenőrizhessék, lehallgathassák. A tervezet szerint csak megalapozott gyanú vagy terrorizmus esetén történne ilyen megfigyelés, és **kizárólag bírói meghatalmazással**. A tervezet részleteiről jövő februárig kellene megállapodni, és **2008 nyarán tervezik** azt hatályba léptetni.

Az internet ellenőrzése Magyarországon is megtörténik, azt a Nemzetbiztonsági Hivatal végzi - gondolom ezzel semmi nagy újdonságot nem mondtam. Nyilván minden országban kétoldalú a dolog: a netezők jogosan a privátszférájukat féltik, míg **a hatóságok pedig hatékony eszközt akarnak birtokolni** a tartalmak és forgalmak ellenőrzéséhez, hiszen állításuk szerint csak ilyen módon nyílik lehetőségük a terrorista, a pedofil, és egyéb számítógépes bűnözéssel kapcsolatos esetek ellen érdemben fellépni.

Egy ilyen rendszer elvben sok mindenre használható, s csak remélhetjük, senki nem lépi túl a maga kereteit, és nem egy totális ellenőrzés fog így kialakulni, melyben például a szerzői jogi oldal megpróbálja a maga pecsenyéjét sütögetni, közben pedig közönséges hétköznapi állampolgárokból bűnözöt igyekszik kreálni. A biztonsághoz, a számítógépet használók táborának megnyugtató biztonságához ennek **világos, átlátható, meghatározott keretek közt zajló és minden szereplő számára egyértelmű szabályozása** is hozzá tartozna.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Hogyan szúrjuk ki a gyanús Android appokat?

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/202200

Kommentek:

buherator · http://buhera.blog.hu 2007.10.21. 11:01:01

Szerencsére a nyíltforrású szoftverek és a különösen nehéz matematikai problémák megkerülhetetlen védelmet nyújtanak magánszféránk számára. Szóval gyakorlatilag csak azokat nem lehet egy ilyen határozaton keresztül fülön csípni, akit kellene...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.24. 21:33:21

Igen, és valahogy csak a Windowsra van kihegyezve ez az akció. Mitagadás nem értem. Attól is tartok, hogy amilént a Sony rootkit mögé is bújtattak vírust, mi lesz ha valaki majd ezt is kihasználja valami trükkös célra?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.01.26. 09:32:29

Az amcsik nem cicóztak, minden újságíró teljes adatforgalmát: fax, telefon, email, netes tenykedes lehallgatták. Kíváncsi vagyok, lesz-e belőle valami új Watergate ügy:
blog.wired.com/27bstroke6/2009/01/nsa-whistleblow.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.06. 09:05:59

A Blackberrynél minden egyes alkalmazott minden forgalmát ellenőrzik:
www.zdnet.com.au/news/communications/soa/RIM-records-all-employee-calls/0,130061791,339295260,00.htm

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.28. 09:09:24

Lassan, de biztosan haladunk a sötét balkáni középkor felé :-(
nonstopuzlet.hu/kemkedo-internetszolgaltatok-vege-az-ingyenessegnek-20090327.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.03.31. 09:24:06

Tanulságos olvasmányok rovatunkban a kínai kémkedésről:

Drive-by download közelről

2007.10.24. 19:06 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: download malware spyware adware stevens rambo noscript kártevő drive by

Nagy forgalmú és biztonságosnak vélt portálok, hirdetési oldalak éppúgy veszélyben vannak, akárcsak az alacsonyabb látogatottságú weblapok: egyszercsak valaki észrevétlenül belehackel egy JavaScript kódot. Jó ha nem Internet Explorert használunk, de korántsem jelenti azt, hogy egy Operával vagy Firefox-szal máris megnyugodva hanyattdőlhetünk a fotelünkben. Nem csak emiatt a Drive-by download kód miatt, hanem egyébként is erősen ajánlott a böngészőbeli "biztonsági rendszerváltást" mielőbb megtenni.

Mi érkezhet így hivatlanul? Bármi. Spyware, Adware és egyéb kártevők. Ha megnézzük a cikkbeli első példát, és a Googleban rákeresünk az érdemi script elejére **'ext:html "60!105!102!114!97!"'**, hamar kapunk olyan találatot, amiben a teljes kód szerepel. Mi lehet ez valójában? Nézzünk bele!

Nosza, egy kis pofozgatás után felveszi a VírusHíradós cikk képernyőjén levő kinézetet, már csak a ", " stringet kell "!" jelekre cserélni. Most, hogy megvan a teljes kód, elmentjük egy helyi mappába akármi.html néven, és akár már indíthatnánk is a böngészőt, hogy kipróbáljuk. Viszont **van egy nagy gond: a JavaScriptes Document.Write azonnal kiírja és végre is hajtódik** a kártékony kód. Ez így nem lenne túl szerencsés!

Mi most csak vizsgálni akarjuk a dolgokat, mit tegyünk hát, hogy **csak lássuk**, mire megy itt a játék a while ciklusban, de ne kapjunk be rögtön valamit? Cseréljük ki a "document.write(out)" részt "alert(out)" paranccsal. Ez ugye egy tetszőleges szöveget jelenít meg a üzenet boxban. Vagyis a kód nem lefut (pontosan ezt akarjuk), hanem csak a változó tartalma jelenik meg már kikódolva. Tadaaaaam, itt a csúnya Iframe!

Egy <IFRAME...> URL hivatkozást látunk, amely anélkül fut le, hogy azt bárki észrevenné. Nem kell zseninek lenni hozzá, hogy azt gyanítsuk, ez nekünk nem szerencsés. És akkor lássuk a mostani linket, ez a www.cracklab.info. Lehet megtenni a fogadásokat tétre, helyre, befutóra, vajon milyen országban hosztolták az oldalt? Akik zsetonjaikat Oroszországra tették, azok nyertek. Szerencsére azt látjuk, az említett oldal már üzemen kívül lett helyezve, lekapcsolták. Persze ilyen kártékony kódok még ezerszám találhatóak. A módszert talán nem is meglepő, hogy sok esetben például warez oldalakon is használják.

Jó, ha az antivírus és tűzfal program mellett van kéznél kémirtó is - az ingyenes és jól használható kategóriában az Adaware, a Spybot

Search & Destroy, és a Spyware Terminator is jó szívvel ajánlható. Nem butaság a használt operációs rendszer és a használt alkalmazói programok frissítéseinek naprakészen tartása. Ehhez jó segítség lehet a Secunia Inspector, a Microsoft Baseline Security Analyzer, vagy akár a Sunbelt Network Security Inspector. Az említett eszközök hatásosan és alaposan feltárják a gyenge, elavult komponenseket, és a frissítéshez is konkrét linkkel, útmutatóval szolgálnak. Az alternatív böngészőhez a **Finjan Secure Browsing, a NoScript, a Netcraft Toolbar, Crawler Toolbar és a RobotGenius Guard** pluginek lehetnek hasznosak. Az én kedvencem, hogy a NoScript alapból tilt mindent, és csak azon az oldalon, ahol én akarom, és csak azok a scriptek, amit én akarok, kapnak lehetőséget a futásra. Elismerem, ez néha kényelmetlen, macerás, ha valami nem működik, nem jelenik meg egyből az űrlap, engedélyezni kell, de hát valamit valamiért. Különben is tetszik az elv, csak az fusson, amit én engedélyezek. A fordítottja egy nagy zsákutca.

Nem lehet elégszer leírni, hogy ne kattintsunk bármire ész nélkül, ezt Didier Stevens híres kísérlete is igazolta. **"Az Ön gépe vírusmentes? Kattintson ide ingyenes fertőzésért!"** szövegű hirdetést hozta létre és naplózta a kattintásokat. Hogy Kournikovára miért kíváncsi valaki, azt még valahogy el tudjuk képzelni, de **mi járhat annak a fejében, aki ingyen fertőzést szeretne**?

Azt hiszem, idebiggyeszthetünk egy jó kis idezétet a tárgykörből, nevezetesen a Rambo II. című filmből. Murdock tábornok a bevetés előtt éppen a technikát isteníti: "Tökéletesen nyugodt lehet Rambo, a világ legtökéletesebb fegyverei állnak a rendelkezésünkre", mire hősünk **"Én úgy tanultam, hogy az ész a legjobb fegyver"**. Mitagadás, a technika lenézése nélkül mi is osztjuk e nézetet...

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/206309

Kommentek:

Nincsenek hozzászólások.

Smaller, shorter, smarter

2007.10.25. 13:30 | Csizmazia István [Rambo] | 6 komment

Címkék: firefox hiba explorer internet reader adobe pdf foxit calc.exe cyanid e

A sok kisebb South Park epizód után egyszercsak megjelent a Bigger, longer, uncut egész estét betöltő moziként. Aki bírja ezt a stílust, az örült ennek a növekedésnek. Nézzük meg mi most ebből a szempontból **az Adobe ingyenes PDF olvasóját**, vajon egy átlagos teljesítményű gépen mi vár ránk verzióról verzióra, örülünk-e a plusz megáknak és jó dolog-e alternatív böngészőt, alternatív PDF olvasót használni? Kísérletezünk, és jól nekieresztjük a **0day PDF próbakódot** (PoC) a programoknak.

Hogy az **Internet Explorer monnyon le**, használjunk helyette például pluginekkel ékesített Firefoxot, arról már korábban értekeztünk. Az Adobe Readert vizsgálva azt láthatjuk, verzióról verzióra hízik a telepítőcsomag méret, és az egyre lassuló működési sebesség azt is lehetővé teszi, hogy egy-egy terjedelmesebb dokumentum megnyitása után ne csak türelmetlenül doboljunk az asztalunkon, hanem **még kávézni is elmehessünk**.

A kávéfüggők emiatt múlhatatlanul hálásak lehetnek, de mit tehetünk mi belgák? Nézzünk valami más lehetőséget! A **Foxit Reader egy szintén ingyenes alternatíva**, háztáji használatra - ha nem nyomdába dolgozunk - tökéletesen megteszi, és a megjelenítés tökéletes, a betöltés sebessége pedig nagyságrendekkel alázza le a nagy testvért. Hogy ezenkívül még mit tesz és mit nem tesz, arra mindjárt visszatérünk pár sorral lejjebb.

Az Index írásában arról olvashatunk, elindultak a PDF hibát kihasználó valódi kártevők, most éppen valamilyen számlázással kapcsolatos levélmellékletként érkeznek az áldozatokhoz. A PDF hibáról szóló leírás több verziót is érint, Krisztustól napjainkig egy **hosszú lista foglalja össze** a sebezhető alkalmazásokat: "az Adobe Reader 8.1, az Adobe Reader 7.0.9, az Adobe Acrobat Professional 8.1, az Adobe Acrobat Professional 7.0.9 vagy az ezeknél régebbi verziók esetében jelentenek veszélyt. Továbbá csak akkor használhatók fel kártékony célokra, ha a felhasználó Windows XP vagy Windows Server 2003 operációs rendszert és **Internet Explorer 7 webböngészőt futtat** a számítógépén." Itt máris kaján vigyor jelenhet meg az orcánkon - úgy kell annak, aki még mindig ezzel böngészik ;-) A kísérletünkhöz kiválasztunk egy korábbi Adobe csomagot, és a 7.0-ás angol Reader változatot gyorsan feltelepítjük.

A teszthez cyanid-E próbakódját használjuk fel (lásd a kommentelők közt), ami **a "mailto" mezőbe írt, speciális formátumú karakterlánc segítségével** a Windows számológépét (calc.exe) fogja magától elindítani a pdf_poc.pdf megnyitása után a sebezhető környezetekben. Nézzük mi vár ránk: **a dokumentumot megnyitva nyomban előtűnik a számológép**, vagyis bármilyen kódot le lehetett volna futtatni ezzel a trükkel.

Miután már benyeltük, halvány vigasz lehet, hogy az elavult PDF olvasó Dugovics Tituszként legalább feldob egy frissítésre buzdító ablakot is.

A vitorlából a szelet **a 8.11-es javított változat** fogja ki, ha ez a frissítés megtörtént, akkor már nem futtatható tetszőleges kód, hanem valóban az alapértelmezett levelező tűnik elő, és afelől érdeklődik, jól vagyunk-e, nem szédülünk-e, és biztos-e, hogy a címzett mezőbe szánjuk a calc.exe programot hívogató zavaros programsort?

Ha ugyanezt a dorbézolást lejátsszuk a Foxit Readerrel is, úgy rezignáltan nyugtázhatjuk, hogy ezzel a programmal ettől az egész hajcihőtől már eleve megkímélt volna minket a sors.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- 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/206943

Kommentek:

buherator · http://buhera.blog.hu 2007.10.25. 14:01:34

Öőö...lehet hogy én vagyok a vak, de pdp féle PoC-tel nem találkoztam. cyanid-E néven posztolt valaki egy saját megoldást a kommenteknél (a filenév ugyanaz mint nálad).

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.10.25. 14:33:26

Öööö..., igen..., öööö...hát...izé...nem...vagyis... teljesen igazad van, köszi, javítottam :-)

Vidi Rita · http://www.hosnok.hu 2007.11.04. 21:25:24

Szia István!
Mostantól ezt a pdf olvasót preferálom, és adom tovább az infót.
Köszi a tippet!
Örülök a blogodnak, mert nem 86 helyen kell utánajárnom az infónak:))

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.05. 19:18:54

Szia Rita!
Nekem egy 1400 Mhz-es notebookom van és az Adobe Reader, amíg egyaltálan feléled, csinálok száz fekvőtámaszt.
A Foxitnál pedig 3-ig számolok, és már olvasom is a doksit, nekem ennyit jelent.
Aki nyomdába termel, vagy spéci táblázatos tartalmakkal dolgozik ütközhet vele apróbb-nagyobb kompatibilitási problémákba.
Azt azért tudni kell, minden szoftver támadható:
antivirus.blog.hu/2007/10/31/minden_es_mindenki_tamadhato

Vidi Rita · http://www.hosnok.hu 2007.11.06. 14:49:53

István!
Akkor azért az a beceneved, hogy Rambo?:))))
ne tagadd, külön vadászod a lassan induló progikat;))

hát én termelek nyomdába (is), igaz, egy ingyenes progival, és most megnéztem az instrukcióid hatására, simán olvassa azt a .pdf-et is.. és már készültem fekvőtámaszozni, de teljesen igaz: még a székből sem volt időm felemelkedni, azonnal megnyílt A Foxit-al!:)

hát igen, logikusan végiggondolva minden támadható sajnos... de ezért vagyunk, hogy segítsünk:) és ez jó:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.06. 15:23:30

Hehe :-)
> Akkor azért az a beceneved, hogy Rambo?:))))
> ne tagadd, külön vadászod a lassan induló progikat;))
Így igaz, mindent bevallok, sőt igazából szándékosan több példányban is el szoktam indítani az ilyen lassú progikat...
Próbálok találni egy ilyen furmányos PDF doksit, és akkor talán abból is lesz majd egy post... Mindenesetre a Foxit "kicsi, sárga, savanyú, de a miénk" :-D

Michelle Wild köszöni jól van

2007.10.26. 09:45 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam brigi wild michelle lexi wagner

A szokatlanság néha lehet jópofa, de úgy néhány szánalmas próbálkozás után szívesen lepofoznánk már a baráti levélnek álcázott spamet küldő illetőket. Igaz, nekünk most nem Brigi küldi a puszit, hanem "csak" Lexi érdeklődik alázatos tisztelettel, hogy "Amúgy miújság", pedig **nem is Wagner úr a nevünk**.

A levél feladója állítólag Kocsis Alexa, legalábbis ezt a nevet használta a levél írója. Maga a levél az alábbi:

A levél részletes adatai pedig így néznek ki, lásd lent. Az IP Address Locatorral és a RIPE oldallal sem lettem sokkal okosabb. Az utcai illegális plakátoknál - ha épp nem érik tetten a kiragasztót - a reklámozott termékek gyártóit, forgalmazóit szokták megkeresni. A beharangozott oldalak adatai jelen esetben valóban több konkrét fogodzóval szolgálhatnak: látszik ki jegyezte be, mikor, hogyan, miért és egyáltalán. Persze ez nem lehet bizonyíték a felelősségre, mert a konkurencia vagy egy rosszakaró is küldhette a levelet, hogy befeketítse őket.

Gondolom senki nem lepődik meg, a Velvet portálon található Impresszumban nyoma sincs ilyen nevű munkatársnak. Ez nem is lehet komoly, hiszen nem valószínű, hogy az Indexesek illegális fizetős warez oldalt üzemeltetnének.

"Ha férfi vagy, légy férfi, ne hitvány gyönge báb" - tanultuk még anno decibel az iskolában Petőfi versét. A spam áradat korábbi egyenes, nyíltsisakos szamuráj virtusát, amelyben face to face közlik velünk: "Jó napot kívánok, én vagyok a spam, tessék vegyél Rolexet és Viagrát, kitűnő minőség, olcsó az ára" - így szemtől szembe, már megszoktuk;-) Amúgy pedig semmi újság, csak **szívből utáljuk a kéretlen leveleket, így burkolt, jópofizós formában meg kétszeresen is.**

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- 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/207087

Kommentek:

Nincsenek hozzászólások.

Kattintsunk-e egyáltalán bármilyen macskára?

2007.10.27. 18:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: macska worm security smart psycho kitty storm eset virustotal avg avast! ess

Múltkori psycho macskás történetünk úgy látszik nem akar véget érni, egyre **újabb levelek érkeznek** állítólagos internetes képeslapküldőktől. Rambo kattint, megnéz, VírusTotálozik, majd tanulságokat próbál meg levonni.

A levél szinte már szokásosnak mondható, **egy IP címmel megjelölt helyre invitál**, hogy majd ott megszemlélhetem a rettentően vicces Kitty képeslapot.

A weboldal Deja Vue érzést gerjeszthet azokban, akik az előző postot is olvasták, annyira hasonlít, hogy pontosan ugyanaz.

Az ember nevethetnékje azonban valamilyen rejtélyes ok folytán bennszorul, ha **a beígért vicessképeslap helyett egy "SuperLaugh.exe" állomány** tolakszik minduntalan letöltődni. A vicceskedvű weboldal készítőjéről gondoltakat most intelligensen magunkbafojtjuk, és maradunk ember.

Ha megnézzük a VirusTotal segítségével, mit is rejt a program - gondolom már mindenki sejti, hogy valamilyen **Storm Worm változatról van szó**.

Ami rém vicces, hogy a kártevő nem egy állandó fájl, vagy valamilyen random módon, vagy IP cím figyeléssel szabályozva változik, mindenesetre pár óra múlva, mikor ismét próbálkozunk, **már egy teljesen más méretű és nevű exe állomány**, ezúttal "KittyCard.exe" álnéven kopogtat nálunk.

Nekünk szerencsénk van, a NOD32 szépen megfogja, és ahhoz, hogy egyáltalán próbaképpen letölthessük, átmenetileg ki is kellett kapcsolnunk a valós idejű védelmet. A mellékelt kép az **ESET Smart Security** RC1 betaváltozatával készült.

Feltöltjük a fájlt a VirusTotal-ra:

Az eredménylistákat vizslatva az az érdekes felfedezés adódik, hogy a sokak által kedvelt, ingyenes Avast! egyik kártevő verziót sem ismerte fel, a másik népszerű ingyenes program, az AVG pedig csak a korábbi változatot jelezte ki. Nekik valószínűleg érdemes még **nagyobb gondossággal és figyelemmel internetezni**. A levélben jelzett oldalt időközben szerencsére már lekapcsolták, de a trükk még tucatnyi helyen bukkanhat fel a jövőben. Úgy tűnik mindig csak egy rövid ideig üzemelnek ezek az új oldalak, aztán pedig rendre tovább és tovább költöznek.

Addig is a fertőzések elkerülése okán inkább száguldozzunk Hello Kittys Ferrarival legott :-)

A felgyülemlett stresszt pedig vezessük le egy jó kis Pantera számmal, melyet mi máson is játszanának, mint egy Hello Kittys gitáron :-)

· 1 trackback

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- 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/209983

Trackbackek, pingbackek:

Trackback: Hogyan? 2008.09.14. 14:47:03

AVG Free telepítése és használataAz AVG egy otthoni célra ingyenes (ámbár létezik fizetős verziója is), Windowsra és Linuxra is elérhető, viszonylag egyszerűen kezelhető vírus és kémprogramirtó. Az ingyenes verziót egy, a háztartásunkban található, üzleti…

Kommentek:

Nincsenek hozzászólások.

A német trójai faló ügy

2007.10.29. 14:38 | Csizmazia István [Rambo] | Szólj hozzá!

A múltkori, Ausztria állami trójai programjával kapcsolatos cikk után egy barátunk küldött egy linket, melyen a felirat szerint a német állami trójai program béta változatát tölthetjük le. Kaptunk az alkalmon, letöltöttük, kipróbáltuk, és hogy amit láttunk, attól vajon arcunkra fagyott-e a mosoly, azt a folytatásban megtudhatják.

Nosza, gyorsan letöltöttük, beizzított ProjectMonitorral felvértezett seregünk bátran a telepítésre kattintott és vártuk, hogy a rettegett trójai bemutassa a kémkedés magasiskoláját.

Az tetszetős intro képek alatt arra gondoltunk, hogy talán pont ilyenkor, a "parasztvakítás" alatt pakolja tele a gépet a sok trójaival, de a logelemzések semmilyen új process, semmilyen új fájl keletkezését, semmilyen Registry machinációt vagy hálózati forgalom létrejöttét nem mutatta ki.

Kicsit furcsa volt látni egy free trial verzió használatát egy ilyen Bundes Trojanerben - nem futja a kapitalistáknak regisztrálni egy 18 EUR értékű szoftvert, hát ez LOL :-) Úgy tűnik, ez egy nagy átverés, az egész csak egy képekből álló slideshow. Talán itt is azt vizsgálják, hányan kattintanak egy ilyen linkre?

Próbaképp azért feltöltöttük a VirusTotalra, minden csendes, ketten gyanúsnak gondolták, amit nagy valószínűséggel az alkalmazott PE vagy ASPACK exetömörítés okozott.

Megkerestük az AL-Software Team weboldalát és letöltöttünk egy próbaverziót a Slideshow Stúdióból, majd gyorsan összeütöttünk egy néhány képkockából álló demót, és heves izgalmi állapotban EXE fájlt generáltunk. A még meleg PROBA.EXE állomány szinte kísértetiesen hasonló VirusTotal eredményt hozott.

Hogy ez az egész mire jó, az nem teljesen világos, talán a Lajtán túl túlságosan ráérnek az emberek - rejtély. Mindenesetre rákukkantottunk, ki jegyezte be az oldalt, és nem a Német Belügyminisztériumot találtuk ott, sem Andrea Merkelt, hanem egy Kai Blitz nevű brück-i illetőt.

Ha mindez április elsején történik, talán még hahotázunk is egyet, mint a Furkó kamu vírusirtó érdekes történetén. Mivel azonban nincs elseje, sőt április se nagyon, így bezárjuk az aktát és a bejegyzést is.

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/211905

Kommentek:

Nincsenek hozzászólások.

Üdít, frissít, formában tart

2007.10.31. 19:51 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: frissítés pdf exploit foxit milw0rm

A múltkori PDF hibáról szóló postban azt ecseteltük, hogy olykor, sőt többnyire jobban járunk, ha a közismerten hibás mammut alkalmazások helyett **kicsi, okos alternatív megoldást** használunk. Természetesen ezzel nem váltunk jegyet az örök hibamentes vadászmezőkre, de gondjainkat valamelyest csökkenthetjük. A szakmai körökben csak "vírustanyaként" aposztrofált Outlook Express helyett **jó választás lehet** a ThunderBird vagy a TheBat!, az ActiveX és még sok egyéb sebből vérző Internet Explorer helyett pedig nagyságrendekkel biztonságosabb egy Firefox vagy egy Opera. Ezzel azonban nem megszüntetjük, csupán csökkentjük a várható támadások számát: **100%-ig biztonságos, teljesen hibamentes és támadhatatlan alkalmazás ugyanis nem létezik**. Hiába, az élet kegyetlen.

Ha már itt tartunk, a statisztikák szerint a blog olvasói ilyen böngészőket használnak, 53%-os indexxel a tűzrókás csapat vezeti a mezőnyt. Sajnos a Linux userek száma csekély, bár igaz, itt nem nagyon tudunk nekik friss információval szolgálni.

Visszatérve főtémánkra a FoxitReader valóban megóvhat minket a mostanában dúló PDF sebezhetőségtől, de leleményes emberek tudták-tudják-tudni fogják, hogyan oldják meg ezt a problémát is. Valamelyik ökölvívós fimben szerepelt egy plakát az edzőteremben az alábbi felirattal: **"Amíg te pihensz, valahol a világ másik végén valaki keményen edz, hogy szétrúgja a ..."**

Mi is biztosak lehetünk abban, hogy valahol, egy boszorkány konyhában **már reszelik a biteket a Foxithez is**. Körbenéztünk a híres-hirhedt Milw0rm oldalon, és csak pár másodperc kellett, és sikerült egy idevágó exploit kódot találni.

A POC kódot betöltöttük kedvenc Dev-Cpp ingyenes C fordítónkba, és már kész is lett a FoxitReadert összeomlasztó minta PDF állomány. (Mindössze a kód végén található dátumos copyright sort kellett kitörölni, vagy kikommentezni.)

Belecsapunk a lecsóba és megnyitjuk kedvenc FoxitReaderünkkel, ami most éppen a 2.0-ás verzió. Mondjuk ez a kód **csak összeomlasztani fogja** az alkalmazást, nem pedig tetszőleges programot futtat le alattomban, de azért kíváncsian várjuk a hatást, ami ne marad el.

Hát igen, valóban fejre állt. Igaz, a forráskódban szerepelt a **"The vender has been notified"**, azaz a gyártók értesítve lettek a hibáról, előbb-utóbb kijavítják. Gyors kutakodás után észrevesszük, hogy már elérhető a 2.2-es változat, ezért villámgyorsan letöltjük, és frissítünk. Most kiderül majd, megszívlelték-e a figyelmeztetést.

A 2.2-esnak már vág az esze, mint az intelligens mosópornak, és mosolyogva közli, az iménti PDF egy hibás, sérült állomány, amely nem nyitható meg. A kísérlet végén nem is maradt más hátra, mint a tanulság levonása: **érdemes gyorsan és rendszeresen frissíteni nem csak az operációs rendszerünket, de a használt alkalmazásainkat is**.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Tízből öt kártevő hátsóajtót nyit
- Safe mód a Mechagodzilla ellen
- Nyári tanácsok utazáshoz

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/214543

Kommentek:

Nincsenek hozzászólások.

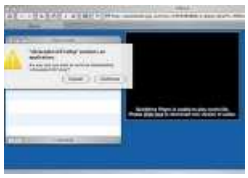
Trójai a Macintoshon

2007.11.05. 21:49 | Csizmazia István [Rambo] | 5 komment

Címkék: mac video macintosh trójai kártevő kodek osx.rspluga

Egy régi tétel szerint vírusok **mindig arra az operációs rendszerre íródnak**, amely széleskörben elterjedt és hozzáférhető a részletes dokumentációja. Ez alapján ha nem is várjuk, de sejtjük, a háttérben zajlanak már az erőfeszítések **a Macintosh platform** elleni kártevők fejlesztésére. Ennek egy jelét láthattuk a napokban: alighogy megjelent az OS X Leopard, máris arról szóltak a hírek, igazi kártevő jelent meg a Mac-es gépekre.

Egy Windows környezetben már bevált program átiratáról van szó, amely **egy video kodek csomagban** található. Erotikus tartalmakat kínáló oldalakon bukkant fel, ahol a látogató egy üzenetet kap, hogy **a film megnézéséhez egy új verziójú kodeket** kell letöltenie. Ha a kártékony oldalon valaki a linkre kattint, akkor a számítógépére letöltődik a kártevő. A lényeg még mindig ott van, hogy ehhez a felhasználó aktív közreműködésére van szükség, ezért sokan nem is tartják veszélyesnek az esetet.



A témára hamarosan visszatérünk, addig igyekszünk beszerezni egy működő példányt az OSX.RSPlug.A trójaiból.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- 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/219663

Kommentek:

Gazs · http://bergengocia.net 2007.11.06. 11:20:18

Szia,
a screenshot alapján sikerült letöltenem a trójait, éppen vivacodec1000.dmg néven jött le. Csatolok egy screenshotot a telepítőjéből a fájllistával együtt. Nem telepítettem fel, mert nem vagyok tisztában a letakarításának módjával, de ha gondolod, együtt kipróbálhatjuk.

myskitch.com/gazs/dock-20071106-111914/

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.06. 16:35:21

Szia Gazs :-)
Köszi a jelentkezést és a segítséget, keresni foglak emailben.
A linket viszont gyorsan kitakartam a képből, mert panaszkodtak az olvasók, hogy a Windowsos gépekre Zlob trójait töltöget az oldal :-(

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.24. 09:13:11

Egy újabb csapás az imperializmusra:
www.enterprise-security-today.com/story.xhtml?story_id=120000A1JFXC

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.06.26. 10:07:10

Úgy tűnik, kezd beindulni a biznic, szemlátomást növekszik a Mac népszerűsége:
www.informationweek.com/news/security/client/showArticle.jhtml?articleID=208800731

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.12.03. 10:25:05

Új fejlemény: az Apple saját oldalán ajánlja, hogy mindenki használjon valamiféle vírusirtót:
appleblog.blog.hu/2008/12/02/itt_a_veg_az_apple_virusirtot_ajanl_a_macreű

És ami még érdekes:
support.apple.com/kb/HT2550?viewlocale=en_US
Ez a link tegnap még tartalmazta a hírt, mára eltűnődött :-O

A digitális jogkezelés vadhajtásai

2007.11.06. 18:18 | Csizmazia István [Rambo] | 1 komment

Címkék: commodore digitális év c64 70 idsa jogkezelés dohi

A PCWorld online oldalain már olvasható a cikk előzetese, ebben néhány elrettentő eset kerül említésre: hogyan próbálkoznak a gyártók ellenőrzést gyakorolni a felhasználók felett, olykor kétes technikai eszközökkel is. Kicsit ehhez kapcsolódva a szerzői jogról ötlöttek fel bennem kételyek, ennek időtartama ugye elvileg 70 év, amit kissé sokallunk. Vajon **milyen értéket képviselne ma már egy Windows 3.0**? Gyaníthatóan alig valamicskét, mégis az 1990-ben kiadott szoftver esetén még hátra van ebből 52 év :-O

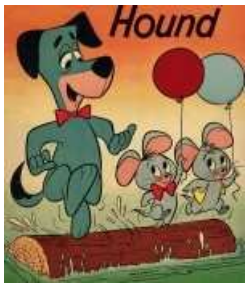
Nagy Feró énekelte egykor, hogy "Operett ország, operett nép..." **Dohi barátom** hozzájárulásával mutatom a Magyar Commodore 64 H.Q. weboldalát. Éppen pár hete, hogy Sam.Joe tisztességben megemlékezett a Commodore64 25-ik születésnapjáról. Sokan vannak, akik még nosztalgiából az emulátorokkal játszanak. Nos, nem teljesen tisztázott minden esetben a letöltött játékok jogi helyzete, van amikor minden egyértelmű és világos, és van, amikor találgatásokra vagyunk kényszerítve, illetve tisztán vélelmezhető a jogi helyzet megsértése. Teljesen egyértelmű a szituáció, ha ingyenes vagy ingyenessé tett játékokról van szó. A Llama Soft például ingyen letöltetővé tette minden Commodore 64-re készült játékát. Egy másik szimpatikus kezdeményezésre láthattunk példát a www.worldofspectrum.org weboldalon, ahol csokorba szedve egy hosszú listán olvashattuk azoknak a fejlesztőknek a neveit, akik **lemondtak a jogaikról és szabaddá tették műveiket a nagyközönség számára**.

A következő kategória a magárahagyott, abandonware névvel aposztrofált programok. Ekkor – mivel a jogtulajdonos másként nem rendelkezett – vagyis nem is tiltotta a későbbi felhasználást, logikusan vélhetnénk szabadon letölthetőnek ezeket az alkotásokat is, de ez nem feltétlenül helytálló. Vannak olyan cégek is, akik e régi, retro hőskor óta a páston vannak, és töretlenül fejlődnek, ontják azóta is jobbnál jobb játékaikat – hogy erre is mondjunk példát: az EOA, vagyis ElectrOnic Arts. Ezek a cégek abban gondolkodnak, hogy a virágkorukat élő színes kijelzős mobiltelefonok, kéziszámítógépek új lehetőséget jelenthetnek korábbi licenceiknek, és emiatt nem engedélyezik a szabad felhasználást.

Azt azért mindenképpen fel kell hoznunk érvként, hogy aki ZX 81, Spectrum, C64, +4 vagy hasonlóan 20-25 éves korú géphez gyűjtögeti a programokat, az a cikk szerzője szerint **nem bitorló, hanem valójában múltmentő** – hiszen a mai legfiatalabb generáció már nem is emlékszik olyan számítógépre, amelyben ne lett volna már beépítve CD olvasó. Úgy tűnik, ezen ereklyék, régi szellemi alkotások csak lelkes megszállottak segítségével menthetők meg az utókornak. A jogszabály szó szerint vett **70 éves szerzői jogi elévülés ebből a szempontból nonszensz**, fizikailag kivárhatatlan és nagyon is vitatható.

A képeket azért mutatom, hogy mindenki kedvére borzonghasson... Az IDSA (Interactive Digital Software Association) töröltette a magyar weboldalról a 25 éves játékokat! Ezek ugye 320x200-as felbontásban működő, több évtizedes programok.

Még nagyon régen (2002-2003 tájékán) rajzfilm kedvelőként csináltam egy internetes galériát, melyben kb. 300 rajzfilm vagy 4000 képét tettem fel azoknak, akik még tudják ki volt Magilla Gorilla, Viziló Vili, Balu Kapitány és Johnny Quest. Pár hónap után kaptam egy baráti figyelmeztetést, hogy vigyázzak, mert a rajzfilmfigurák is szellemi oltalom alá esnek. Egy pillanatra eltűnődtem, hogy **az "illegális" Foxi Maxi használatért vajon érdemes-e vállalni a börtönt?** ;-)



Visszatérve a C64-s oldalhoz, az a horror, hogy nem csak a játékokat, de a hozzáuk tartozó egyéb dolgokat is **töröltették a weboldalról**. A hivatalos kézikönyvek esetén talán még érthető, de hogy az újsagból scannelt, **játékosok által rajzolt térképeket is**? Vicc az egész :-(

Ajánlott bejegyzések:

- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Akiknek a Captcha kínszenvedés
- 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/219702

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.06. 09:11:02

Amikor maga a szerző szív a jogvédők miatt.
itcafe.hu/hir/szerzoi_jog_abszurd.html

Trójai a Macintoshon II.

2007.11.07. 12:43 | Csizmazia István [Rambo] | 2 komment

Címkék: macintosh trójai kodek estdomains zlob

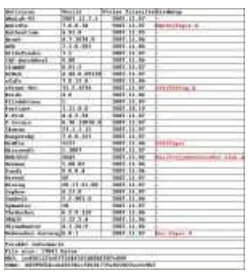
A múltkori postban ígértem, hogy erre a témára még visszatérünk. Közben diskuráltam Mac-es barátaimmal, és nagyjából az jött le nekik, hogy **amíg a juzernek magának kell kattintania, addig komolytalannak** tartják a trójai veszélyt. A cikkben aztán a látható **URL címet kitöröltem**, mert igaz hogy a Mac kártevőt így le lehetett róla tölteni, viszont a **Windows felhasználók panaszkodtak**, hogy hozzájuk pedig EXE formátumú Zlob trójai töltődik le onnan.

A weboldal regisztrációjánál - talán nem meglepetés - itt is a **kétes hírű Estdomains** tűnik fel.

Már egy korábbi cikkben, az Alexey Tolstokozhev állítólagos halálhírét hírül adó hamis webhelynél is az Estdomainsnél történt a bejegyzés.

Közben **Gazs volt olyan kedves**, és küldött a Macintosh gépéről egy szép screenshotot, amelyen éppen sikerült letölteni a trójait, ez akkor vivacodec1000.dmg néven jött le. A képen a **trójai kodekcsomag telepítőt látni a fájllistával** együtt.

A letöltött trójai egy **DMG, azaz Disk iMaGe típusú állomány**, és a VirusTotallal vizsgálva, az alábbi eredményt kaptuk:



A konklúzió lehet az is, hogy ne látogassunk az Estdomains felségterületéhez tartozó oldalakat, vagy az, hogy ne nézegessünk XXX tartalmakat, esetleg csak annyi, hogy ne kattintgassunk ész nélkül, különösen **kodekcsomag telepítési ajánlatoknál**.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/221178

Kommentek:

Gazs · http://bergengocia.net 2007.11.07. 13:53:59

Az ijesztő az, hogy alapbeállítások mellett -- eddig kényelmes voltam megváltoztatni a gyári viselkedését a Safarinak -- a "biztonságosnak" ítélt fájlformátumokat -- képek, pdf-ek, sőt, a disk image-et is automatikusan elindítja. A rajta levő installerrel együtt. A download gombra kattintás után automatikusan lehúzta, felmountolta és elindította a telepítőt, bár ha jól tudom, később kér adminisztrátor jelszót. Ettől függetlenül a legtöbb maces nem fog gyanút. Egyetlen szerencse, hogy nagyobb a füstje a trójainak, hátha jobban odafigyelnek ezután a felhasználók

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.14. 11:03:54

Úgy tűnik, nem ülnek a babérjaikon a rosszfiúk :-O
www.f-secure.com/weblog/archives/00001312.html
Futószalagon készülnek a variánsok...

A ninjától az androidig

2007.11.08. 14:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: security új smart verzió android arculat nod32 eset ess sicontact

A frissen megjelenő új termékekkel (ESET Smart Security biztonsági csomag, ESET NOD32 Antivírus 3.0) új arculatot is bevezet az ESET, egy **gondolkodó androiddal** próbálja a termékekbe épített, **a proaktív védelemhez szükséges mesterséges intelligencia fontosságára** felhívni a figyelmet.

Az android sem akármilyen, ugyanis azt a magyar Digic Pictures tervezte.
A **Digic Pictures** a magyar származású hollywoodi producer, Andy Vajna **tulajdonában lévő** Cinergi Interactive cégcsoport tagja és számítógép-animációs filmek, trükkök készítésével foglalkozik. A magas szintű, **igényes munkákra specializálódott műhely a Terminator 3 forgatásában** is résztvett.

Mostanában divatos lett az android, lásd a Google projektjét, de találkoztunk Johnnie Walker Androiddal és Philips Shavers Robottal is a YouTube oldalán.

A jelenlegi plakátokon, reklámokon látható kardos hölgy Michelle Lee, feketeöves kaszkadőr és színésznő, aki az ESET számára exkluzív fotósorozatot készített.

A kizárólagosság egyébként valóban fontos, mert ezzel el lehet kerülni az olyan vicces, véletlen eseteket, amikor két antivírus gyártó is, ESET és a Panda egyazon grafikai elemet vásárol meg az interneten: példánkban az ESET partner oldalán és a Panda nyitólapján ugyan a kép van, csak tükrözve :-)

Az új termékekkel kapcsolatos arculatváltás Magyarországon várhatóan decemberben/januárban zajlik le.

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/222232

Kommentek:

Nincsenek hozzászólások.

Balekvadászat

2007.11.09. 11:10 | Csizmazia István [Rambo] | 5 komment

Címkék: torrent balek gorilla swishmax fullversion mybittorrent

Aki olvasta Mitnick valamelyik könyvét, vagy figyelemmel kíséri a spam háborút, tudja miről beszélek. **Mindig kell valami érdekesség**: Kournikova meztelen fotói, gyors haszon a tőzsdén, különleges gyógyszer akció, azonnali adóvisszatérítés, Vista crack, kiemelkedő jövedelem napi egy óra otthoni munkával, univerzális szériaszám generátor minden víruskeresőhöz, férfiasság növelő, ingyen diploma, csodás fogyókúra recept, keresik a balesetben elhunyt milliomos örökösét - az ismeretlenektől kapható levelek tárgya még hosszan folytatható. Rafinéria felső fokon. **Ma torrentezni indulunk**, és ígérem, ez a kirándulás sem lesz unalmas, előbukkanak az összefüggések, és megpróbálunk majd valamiféle tanulságot is leszűrni.

Bemelegítésnek keressünk rá a **Swishmax kulcsszóra**, és használjuk ehhez a Torrent Search Engine Searcher oldalt, ami egy jópofa kereső, a baloldali panelben beírt kulcsszóra végig lépkedhetünk több gyűjteményen is. Van is sok találat, de az egyik oldalon, a MyBitTorrent-ben kissé elképesztő a mérete, többszáz megabájt. Mivel jól ismerjük a szoftvert, ez teljességgel nonszensznek tűnik, és a SwishZone oldalán jól látszik, a 2-es változat telepítőcsomagja sem lépi túl a 23 MB-ot. Nosza, éles elmével gyorsan rákeresünk a **"barmit keresek, mai feltoltes, 201 es 659 mega"** nevű tételre, és minő meglepetés, találat erre is van :-)

A Web Security Guard hűséges házőrzőként megmorogja a gyanús Fullreleases oldalt, ami a **warez oldalaknál nem meglepő**.

Most már vérszemet kapunk, és nagy furmányosan a **"te egy hulye gorilla vagy" című szoftvert keressük** heves izgalmi állapotban. Gondolom, senkit nem ér meglepetésként, ebből is van raktáron, még pedig **a megszokott 201 és 659 MB méretű** óriás csomag.

Továbblépve a részletekre - már alig tudjuk visszatartani magunkat, hiszen a világhírű "te egy hulye gorilla vagy" program teljes verziója fog perceken belül az ölünkbe hullani - örömmel konstatáljuk, hogy nem csak **Full release, de ISO, Crack, Keygen és FULL-CD** változat is elérhető belőle.

Legott a Download feliratú gombra bökünk, és várjuk az igazság pillanatát.

Ez olybá tűnik, kissé késedelmet szenved, ugyanis **azzal szembesülünk, hogy csak a regisztráltak töltögethetnek**.

Kesernyés és kissé csalódott mosollyal orcánkon belevetjük magunkat a regisztrációba.

Újra reménykedünk, megvan a beszédes nevű accountunk, akkor hát hajrá előre! Éles szeműeknek esetleg feltűnhet a láblécben az alábbi apróbetűs kitétel: "Best viewed in MS Internet Explorer..."

Bízunk benne, hogy most más semmi nem ronthatja el az örömünket, kíváncsian várjuk a gorillát, hátha mégis létezik, csak mi nem tudtunk róla.

Krisztus koporsóját se őrizték ingyen, no meg ingyen ebédet még senki nem evett - a stuffok **letöltéséért itt fizetni is kell**, a regisztráció önmagában sajna nem elég. Ezt persze nem kötik az orrunkra, **előtte adjuk csak meg jól az adatainkat.**

Gorilla végül mégsem jön, helyette ismét a járuljunk a kasszához kezdetű ablak tűnik fel, valamilyen rejtélyes okból mégsem kotorászunk a pénztárca után. Ha még hozzávesszük azt, hogy a MyBitTorrent oldal Privacy Policy menüpontjában "We are a leading Torrent Website" mondatot izlelgetjük, hát komolyan felötlik bennünk, vajh miért nem veszik észre az ilyen minőségű linkeket?

Tanulság? Nos több is lehet: "A hülye is tud fake letöltési oldalt fenntartani", vagy "Hogyan gyűjtsünk be e-mail címeket, néha még pénzt is semmiért", esetleg "mit tehetünk, ha éppen nem azzal játszunk, ami velünk egyidős"? Kártevők terjesztésére hiszékenyeknek mindenesetre alkalmas lehet az ilyen oldal.

Sajnos végtére nem sikerült megtudnunk, mit tartalmaz a "Te egy hulye gorilla vagy" Full Release version, lemaradtunk, mint a borravaló.

Pedig még keygen is volt hozzá :-D

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/223216

Kommentek:

feriboy 2007.11.09. 18:54:12

torrent kereséshez ajánlom a mininova.org-ot, illetve a torrentz.com-ot :)

cworm (törölt) 2007.11.10. 01:31:14

lol! :D
feriboy te meg hülye vagy:D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.02.23. 14:33:39

Az írás természetesen NEM a torrent ellen készült, hanem az ilyen csalárd csomagok ellen.
Közben zajlik a Pirate Bay per, és legálissá tenné a fájlcserét a norvég kultuszminiszter :
www.hwsw.hu/hirek/38162/pirate_bay_torrent_fajlcsere_kiado_zene_legalis_ifpi_norveg_magancelu.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.13. 10:43:30

Nem számítógépes téma ugyan, nem is klasszikus computer kalózokról szól, de a balekvadászat címszó alá, mint jól tejelő balekekokat megfejő, zseniális ötleman, korunk Osztap Bendere, pont beleillik:
www.deluxe.hu/cikk/20090707/kalozvadaszat_az_uj_szorakozas_a_gazdagok_koreben_akiket_az_adeni-obol_vizeire_visznek

titan 2010.04.26. 15:31:23

vaze, pedig már olyan kíváncsi voltam... szerintetek Tescoban meg lehet már kapni ó'csóér'? :D

Hamis kémirtók

2007.11.12. 16:53 | Csizmazia István [Rambo] | 8 komment

Címkék: fake spyware terminator warrior kémirtó

Számos vírusirtó (például az ESET, az F-Secure, a Norton, a Panda, a Trend Micro) **rendelkezik kémprogramok elleni védelemmel**, de azért óvatosságból sokan használnak külön kémirtót is - a paranoiásabbja akár többet is. Nagy népszerűségnek örvend **az ingyenes eszközök mezőnyében** például a SpyBot SD, a LavaSoft Adaware és a Spyware Terminator. Azonban vannak érdekes esetek, **amikor jobb, ha távoltartjuk magunkat az ingyenes programoktól**, sőt előfordul, hogy **egy Terminator nem "az a" Terminator**.

A kémprogram mind a magánemberek, mind a cégek számára igen veszélyes. A magánemberek bizalmas adatai zsarolásra lehetnek alkalmasak, illetve nevükben, **adataikkal visszaélve különféle bűncselekményeket követhetnek el**, illetve **jelszavaikat és a banki adataikat eltulajdonítva anyagilag is megkárosíthatják őket**. Cégek esetében az eddig felsoroltak mellett a szellemi tulajdont, szabadalmakat, technológiákat és a konkurencia számára hasznos üzleti titkokat veszélyeztetik a kémprogramok.

Ha ellenszert keresünk, nem minden kémirtóként megjelölt program fog megvédeni minket, hiszen **ezek között is akad megtévesztő alkalmazás szép számmal: például a SpyFalcon, a SpyAxe vagy a SpySheriff**. Bár egy ilyen csalárd program azt állítja magáról, hogy eltávolítja a kémprogramokat, azonban ez nem igaz. Jobb esetben csak hatástalan, rosszabb esetben **hamis riasztásokat produkál, hogy az ijesztgetéssel a szoftver fizetős verziójának megvételére bírja rá** a szerencsétlen próbaváltozatot használó áldozatot. A legrosszabb esetben pedig **a hamis kémirtó maga a kémprogram**, és pontosan ő lopja el az adatainkat.

Nemrég olvastam egy fórumon, hogy a Spyware Terminator nem jó, csaló program, vigyázni kell vele. Eléggé meglepett a dolog, ezért haladéktalanul a Spywarrior weblapra siettem, ahol **egy óriási lista található a csalárd, álkémirtókról**. Jé, a listában tényleg ott a Spyware Terminator, hmm - egy pillanatnyi tanácstalanság érződik, de aztán jön megvilágosodás. A gyártó honlapja nem a jól ismert www.spywareterminator.com, hanem egy holland oldalra mutat. A táblázat kommentjében pedig egyértelműen leszögezik, ez program valóban nem az a bizonyos program, csupán névazonosságról van szó.

Jótanácsként érdemes megjegyezni, hogy **a névtelen, újonnan megjelent védelmi csodaprogramokat ne a saját bőrünkön próbáljuk ki**. Használjunk inkább neves, a teszteken jól teljesítő, a szakmai fórumokon széles körben elismert, illetve megbízható és elérhető hivatalos gyártótól származó biztonsági programokat, akik magas színvonalú teméktámogatást is nyújtanak.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Küldj pénzt! - Az elveszett poggyász sztori
- Nyári tanácsok utazáshoz
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/226563

Kommentek:

zvaragabor 2007.11.12. 20:10:08

Nekem van egy hobbivinyóm, amire egy XP SP2-t tettem föl, frissítéseket nem telepítettem, IE6-ot legsebezhetőbbre állítottam be, és elkezdtem netezni. Crack/serial, pornóoldalak, majd néhány popup, rájuk is kattintottam, és jöttek szép sorjában az álirtók. :) Összeszedtem vagy 5-6-ot, többek között a PcSecure Systemet, de egy utólagos antispyware futtatás után előkerült egy SpySheriff, és még más hasonló tipusú programok is. Karanténba zártam mindent, majd visszahelyeztem őket egy átmeneti mappába, hogy egy béta antivírus laborjának elküldjem őket. Küzben az ESET NOD32 Antivirust ki kellett kapcsoljam, mert szinte mindegyik fájlra riasztott. Egyébként az az antispyware az a-squared Free volt. Nagyon jó, szerintem még jobb is, mint amiket felsoroltál a blogban. Realtime védelme nincsen, automatikusan sem frissít, de szép nagy adatbázisa van. Másik nagyon jó még az AVG AntiSpyware Free. Enneksincs valós idejű védelme, frissíteni is csak kézileg tud, de az első 30 napig teljes értékű, a próbaidő leteltével butul csak le. Ezek vannak a gépemen, semmi más. Illetve van DropMyRights, SpywareBlaster, Foxhoz NoScript, és AdBlock Plus, és egy Nod szigorúra állítva.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.13. 10:44:38

Szia Gábor!
Köszi az észrevételeket, legjobban a "az ESET NOD32 Antivirust ki kellett kapcsoljam, mert szinte mindegyik fájlra riasztott" mondat tetszett :-D
Munkahelyi környezetben, illetve érzékeny (banki, kormányzati, stb.) adatok esetén biztos, hogy nem ingyenes, hanem csak és kizárólag fizetetős kémprogram ellenes alkalmazásokat kell választani, ilyen például a SpySweeper és a CounterSpy.

zvaragabor 2007.11.13. 15:05:02

Igen, fontos adatokat tartalmazó környezetben fontos a jó antispyware, nem hiányzik egy adatlopás. És hát a fizetős termékeknek vagy jobb a realtime védelme az ingyenesekéhez képest, vagy ha az a bizonyos ingyenes antispy egy jobb féle, akkor meg nincs valós idejű védelme. Fene egye meg a kompromisszumokat. :)

zvaragabor 2007.11.13. 15:34:54

Ami az ominózus mondatomat illeti, szándékosan írtam. :)
Végülis a nodnak ez a dolga, riasszon a módosult/létrhozott/végrehajott kártékony fájlokra.
Csak megjegyeztem, mert elég zavaró volt, hogy visszaállítottam a fájlt a karanténból, nod meg belekontárkodott a dolgaimba. :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.13. 15:40:02

Szia!
Értem én, tökéletesen értem :-))))

lacibacsi153 2008.11.07. 15:54:18

Rambónak:

Találtam egy kisméretű antispyware progit.
Hamis-e?
PC Tools Spyware Doctor 6.0

Köszönettel: Lacibácsi

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.11.08. 10:56:36

Szia Lacibácsi!

A PC Tools SD egy valódi cég valódi terméke :-)
Használhatod bátran, itt van egy kis info róla:
www.pcworld.hu/forum/index.php?showtopic=11953
reviews.cnet.com/security-and-encryption/pc-tools-spyware-doctor/4505-3688_7-32305499.html

lacibacsi153 2008.11.09. 11:29:15

Köszönöm!

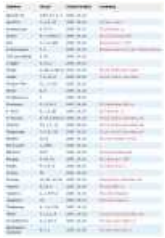
Maxtor és a trójaiak

2007.11.13. 09:28 | Csizmazia István [Rambo] | 2 komment

Címkék: taiwan merevlemez maxtor trójai fertőzött

Úgy látszik, **lassan érdemes lesz külön rovatot nyitni az újonnan vett és vírussal fertőzött számítástechnikai eszközöknek** - a szeptemberi Stoned Angelinával fertőzött Meidon notebookok után most a **Maxtor Basics 500G külsős merevlemezeiről** derültek ki kevéssé szívderítő dolgok.

Az esetről részletes beszámolót találtunk a Taipei Times anyagai között, és ebből az derült ki, hogy **a fertőzött számítógépek minden mentett adatot megkíséreltek feltölteni weboldalakra**. A Thaiföldön gyártott külsős merevlemez széria két trójai állományt tartalmazott autorun.inf és ghost.pif néven.



A termékeket azóta visszavonták az üzletekből. A támadás módja újszerű, és sokan ismét kínai szálakat sejtenek a kémkedési ügyben. Az eset pikantériája, hogy **ilyen típusú eszközöket különféle kormányzati ügynökségek is vásárolnak**, és könnyen elképzelhető, hogy amíg az esetet észlelték, már kikerülhettek bizalmas adatok is.

Nem elképzelhetetlen ilyenkor a célzott támadás sem, pl. tudtak egy nagy volumenű kormányzati megrendelésről, és megiratták a kártevőt pontosan ebből a célból, és a többi áldozat csak véletlenül került bele. Az adatvédelemnél a cég vezetőinek, kulcsembereinek azt is **meg szokták tanítani, hogy legyenek gyanakvóak, ha az utcán, parkolóban USB kulcsot, iPodot találnak**, hiszen sokszor nem véletlenről van szó, hanem pontosan nekik helyezték oda, egy kémprogrammal ellátva.

A két weblap közül a www.we168.org egy Amerikában hosztolt, és úgy tűnik, még működik, de már törölték a tartalmát.

A másik a www.nice8.org pedig egy korai weblap, amelyet időközben lekapcsoltak.

Annyi azért látszik, hogy a **domain bejegyzés rendje túl laza**, Yon ge nevű egyén a yongge cégtől a yongge utcából igazán fantázia dús alkotás, persze **a ga ga által regisztrált gaga cég is teljesen hihető, a megjelölt gagaga utca** pedig a turisták kedvelt célpontja ;-) Tényleg már csak azt várná az ember, hogy az amerikai filmekből ismert 555-tel kezdődő telefonszám is ott sorjázzon.

Nem azt mondom, hogy személyit, útlevelet és a kutya oltási bizonyítványát is be kellene kérni, de hogy ezt nem ellenőrizte senki, az tuti. Kíváncsi lennék, ha Magyarországon valaki Majomváry Armandó, Zomba, Ló utca 23/b címről kérelmezne egy új bejegyzést, vajon átmenne-e a szűrőn.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Majdnem mindenki átverhető adathalászattal
- Hogyan szúrjuk ki a gyanús Android appokat?
- 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/227428

Kommentek:

titan 2010.04.26. 17:10:27

Bizonyos esetekben szerintem simán átmenne (bár amikor a poszt íródott, lehet még nem ment volna át)
Viszont GoDaddy segítségével hasonlóan ellenőrizetlenül lehet vásárolgatni a domain-eket

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.04.27. 12:52:46

Most szigorítottak valamelyest Kínában is a doménregisztrációban, mostantól már név, cím és személyazonosító irat is kell hozzá. Hogy ezeket mennyire ellenőrzik, nem tudom. Az embert azt sem érti, hogy korábban miért nem így volt.

Azt viszont nem szabad elfelejteni, hogy Magyarországon a nagy köztartozást felhalmozó cégeket ukrán, szerb vagy hajléktalan strómanok nevére milyen simán és könnyedén lehetett átjátszani, pedig az kicsit komolyabb adminisztrációjú műfaj.

Eladó az e-mailcím gyűjteményem

2007.11.14. 16:28 | Csizmazia István [Rambo] | 29 komment

Címkék: spam yahoo levél nhh címlista kéretlen

Sokféle spamet kaptunk már, tele velük a padlás. Ami most érkezett, az **egy kicsit különbözik a többitől**, bár azt azért nem állíthatnánk, hogy kiemelkedik közülük, mint gladiátor az eunuchok táborából. Emberünk - a tücsök és hangya nyomdokain járva - **szorgos nyári munkáját kívánja aprópénzre váltani**. Vajon az NHH mit szólna mindehhez?

A levél maga a következő:

Nagy Sándor vagyok, és szeretném eladásra ajánlani a nyár folyamán
összegyujtött email címeket tartalmazó listámat - változások miatt ezeknek
nem tudom hasznát venni.

A címlisták a következo tételekbol állnak:
- 200.000 magyarországi vállalkozás email címe
- 400.000 vegyes email cím, mely foként magáncímeket tartalmaz

A fenti címeket, mint jeleztem, az interneten idén nyáron gyujtöttem,
nyilvános forrásból, a hibaszázalék mindössze tíz százalék. Ugyanakkor
mellékük adom a Worldcast kiküldo programot, ezzel bárhonnan óránként több tízezer email sebességgel küldheti ki leveleit, valamint az Atomic Email
Hunter programmal további címeket tud gyujteni.

Amennyiben az ajánlatom érdekli Önt, kérem, jelezzen, küldök részletesebb
tájékoztatót. Ugyanakkor kérem, ne erre a címre válaszoljon, hanem a
mailto:sandor_nagy2006@yahoo.com címre, mert azt gyakrabban olvasom.

Üdvözlettel,
Nagy Sándor

Hát, köszönjük a megtisztelő ajánlatot, de nem élünk vele.

- 1 trackback

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/229039

Trackbackek, pingbackek:

Trackback: Worldshots 2007.11.15. 15:14:29

Re: Eladó az e-mailcím gyűjteményemCsizmazia István nem dobta fel Random Sándort, aki időnként megpróbálja eladni hatszázezer darabos email cím listáját, barátunkat a Nemzeti Hírközlési Hatóságnak. Én viszont egy dupla teszt keretében megtettem. Egyr…

Kommentek:

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.14. 18:04:22

Kedves KopaszMercis!
Bár magam osztom a felháborodásodat :-), annyit szeretnék kérni tőled nagy tisztelettel, hogy szalonképes kommentek szülessenek.
Mivel szerkeszteni nem tudom a kommenteket - nem tudok kipontozni dolgokat ;-) - ezert most visszaírom a bejegyzésedet - sorry, de módosított formában. A lényeg azért nem fog elveszni.
Az ilyet b.....m s.....be egy arab terroristaval.. szarazon.
Azt hogy egy ilyen címárus honnan veszi a bátorságot ehhez a házaláshoz, azt én sem értem.

Darth Revan 2007.11.14. 18:12:40

az ilyenek e-mail cimet kitakarni? minek? ok talan tiszteletben tartjak masok jogait?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.14. 18:25:04

Kedves Darth Revan!
Jogos a felvetés, de maradtam ember :-) Küldhettem volna tovább az NHH-nak, de ettől nem állt volna meg a spamáradat.
Illegális ötleteim persze lehetnének (feliratni az ürgét egy rakat homoerotikus hírlevélre, stb.:-) de maradok a tiszta ösvényen.
Bemutattam a pofátlanságot, ennyit tehetek.

buherator · http://buhera.blog.hu 2007.11.14. 19:05:20

NHH-nak elküldeni pedig nem lenne rossz ötlet, elvégre az a dolguk, hogy az ilyeneknek a körmére nézzenek! E-mail harvestingre amúgy nem hiszem hogy van törvény sajnos...
Azt kéne hogy az ilyenek vállalkozásainak címét nyilvánosságra hozni, aztán megnézni milyen fejet vág, amikor "óránként több tízezer" viagrareklám fut be a mailszerverére...

Ja, egyébként a 20y.hu-n azt hiszem kinnt van a csávó címe, ha valaki szeretné próbára tenni a Yahoo spamszűrőjét :P

20y.hu/20071026/enni-ehetsz-csak-24-oraig-ne-a-szaddal.html

OkoskaTo:rp 2007.11.14. 19:06:03

Kedves Rambo! Az illegális megoldások a tettlegesség különböző vállfajait jelentik. Buzihírlevélre felírni teljesen legális, ámde nem elég alapos. Sokkal inkább buzi _társkeresőbe_ kell feladni bevállalós hirdetéseket a nevében.

hematite · http://standby.blog.hu 2007.11.14. 20:20:22

Minden heten jon egy ilyen email a freemailes fiokomba, a sok mas mellett...

stringer 2007.11.14. 20:25:27

október 26-án küldtem el ezt az nhh-nak állásfoglalásra, azzal a megjegyzéssel, hogy ne indítsanak eljárást, mert annak a költségét nekem kellene fizetnem (naná, ki más, mint akit spammelnek, nehogy már a spammer fizesse meg).

azóta válaszra sem méltattak.

bizonyára sok dolguk van.

Daniel W. Mcload 2007.11.14. 20:40:19

Én is elküldtem az NHH-nak, mint ahogy stringer kolléga, és engem sem méltattak válaszra....

Tehát ennyit az NHH-ról.

buherator · http://buhera.blog.hu 2007.11.14. 20:52:55

Ugyan nem ebben az ügyben, de nekem már válaszoltak, igaz beletelt pár hónapba. Úgyhogy csak türelem :) Egyébként szerintem minél több helyről kapnak visszajelzést, annál jobb, szóvalne fogjátok vissza magatokat!

dark future · http://www.andocsek.hu 2007.11.14. 21:35:55

Az igazi probléma nem is ezekkel a spamlistás köcsögökkel van, hanem az ISP-kel. A spam-ek ellen igazán hatékonyan ők tudnának védekezni központilag, de általában szarnak rá, sőt valószínűleg nem is érdekük csökkenteni az áradatot, hátha a jónép emiatt is motivációt érez, hogy modemről szélessávra váltson...

0xFFFF 2007.11.14. 21:46:16

Kedves dark future !

Az isp-k védekeznek, ahogy tudnak. Éppen a közelmúltban hallhattuk, hogy a T-nemtudomki :) automatikusan és alapértelmezetten tiltja a 25-ös portot az dsl végpontok felől....de ha kéri a végpont, feloldja, mert teljes szolgáltatást ad el, amivel igenis élhetek, ha akarok. Erről hát ennyit.

A spam ellen egy hatékony védekezés van, de az nem életképes, mert senki nem akarja menedzselnia saját levelezését, ez pedig az ún. fehér lista. Csak attól jön meg a levél, akinek a címét a listára felteszem. Az összes többi /dev/null-ra megy. Ez egyébként analógiája a telefonszámnak. Csak az tud híni, akinek megadod, mert a telefonkönyvből tiltod magadat. Érdekes, hogy a telefonnál törődnek ezzel az emberek, míg a mail fiókjuknál nem.

Listák. A tag, aki kínálgatja a listát, nem fogható meg. Senki nem tiltja, nem is lehet tiltani, hogy a weboldalakon szereplő mailcímeket gyűjtsed, ha megtiltanák, gyakorlatilag a böngészést tiltanák :) Okos ember nem teszi ki a mail címét weboldalra. Aki meg iwiw rajongó, az szokja a gyűrődést. :)

államcsőd · http://www.allamcsod.hu 2007.11.14. 21:58:56

spam :(

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.14. 22:28:36

@buherator:
Szia. NHH-ban úgy látom, igazad van.
@Okoska To:rp:
Hát igen, ez sem rossz ;-)
@Stinger:
Hello! Te az a bizonyos Stingr vagy ala PCW?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.14. 22:33:04

Daniel W Mcload!
Lehet, hogy ők is aszerint foglalkoznak az ügyekkel, hogy vagyunk-e valakik, vagy sem. Lásd igen érdekes cikket a VirusHiradón www.virushirado.hu/hirek_tart.php?id=1227 ahol Alicia Keys MySpace fiókját még aznap rendbetették, míg a kevésbbé híres előadókkal meg nem törödtek :-O

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.14. 22:39:21

0xFFFF:
Kedves 65535 ;-)
Sok mindennel egyetértek, de az "okos ember nem teszi ki az email címét" módszer nem mindig járható. Ha van valami vállalkozásod, és azt akarod, hogy megtaláljanak, kell az elérhetőség. Ha pedig cégnél dolgozol, egy pávián is kitalálja előbb-utóbb a cégpolicyt, keresztnév.vezeteknév@cégnév.hu és küldi sok spamet, na meg akármilyen domain elé beírt "support", "info", "sales" is ad terepet a kísérletezésnek. Szóval marad a szűrés, nincs mit tenni.

andreiground (törölt) · http://www.andreiground.com/ 2007.11.15. 00:13:01

Az ilyen embernek bitenként 40 millió levél járna, de akkor meg a yahooval cseszne ki az ember. Vajon mennyit érhet potom 400000 e-mail cím?

attreides 2007.11.15. 00:13:24

"azzal a megjegyzéssel, hogy ne indítsanak eljárást, mert annak a költségét nekem kellene fizetnem"

nem úgy van az, minden egyes eljárás költségét ők maguk vállalják... Hivatalból kötelesek eljárni.

Rwindx 2007.11.15. 01:14:12

Kedves 0xFFFF !

A védekező ISP-k azaz a T- ...cik akiket említesz, inkább a kisebb szolgáltató cégeknek tettek alá mint a spammereknek. Ugyanis így a 25-ös porton azok mailszerverét sem lehet elérni a T-...ci hálózatából. Ez ellen gyakorlatilag a 25-ös port átirányításával lehet védekezni (a feloldás macerás), de mire minden user átállítja az kínszenvedés. Ja és az átlag user rögtön a mailszolgáltatót szidja nem az ISP-t.

Arról nem is beszélve, hogy azóta semmivel sem csökkent a magyar címtartományokból érkező spamáradat (saját tapasztalat). Múlt héten én is küldtem egy delikvenst az NHH-nak, de választ én sem kaptam eddig. A hirdető cégek pedig elég egyértelműen beazonosíthatóak voltak.

A whitelist szintén problémás, mert egy cég esetében nem tudhatod hogy ki akar majd írni neked, és milyen emailcímről. Ez nem menedzselés, hanem elérhetőség kérdése. Véleményem szerint használhatóbb módszer egy szerver oldali spamszűrő, szigorú beállításokkal. Ezen is át fog jönni sajnos valamennyi, de pl.: napi kb 8-10000db spam, vírusos levél így is visszapattan

a mi szerverünkről. Ezt közel 300 felhasználó kapná meg minden nap. Ennyivel könnyebb az életük.

0xFFFF 2007.11.15. 04:56:00

Kedves Rwindx !

Egy cégnél sem probléma ez a dolog. A weboldalra egy form captcha-val felszerelve és az ír, aki akar. Miért kéne kirakni mail címet ?

A szerveroldali szűréssel az a baj, már a hagyományos értelemben vett szűréssel, hogy a szervert dolgoztatja. Nekünk napi 100000 spam lepattintása az átlagérték és igenis bosszant, hogy a szerva a spamfilter miatt izzad.

A végső megoldás egyébként törvényi szabályozás lenne, ami kimondaná, hogy ha forintosítom a kárt a spammer köteles a cehhet fizetni. Lenne egy két érdekesség.

Addig azonban jól jövedelmez például a webfocusnak a www.koremail.hu oldal, ami nem más, mint spammer site, hiába írkálják tele olyan dolgokkal, hogy ügyfeleink nyilatkoztak, stb.

0xFFFF 2007.11.15. 04:58:40

Ja igen ! Aki az NHH-ra vár, az naív ember. Az is csak egy hivatal, öncélú, nem a fogyasztó érdekvédelmi szervezete. A nevükben sincs ilyesmi, ők a hírközlést felügyelik, a hírközlők parazitái.

Terveüdekszi 2007.11.15. 09:07:49

"Bemutattam a pofátlanságot, ennyit tehetek."

Nobel békedíjat neked! Én meg tudok olyat, hogy yyyyy yyyyyyy ellopja az emberek pénzét. zzzzzzzz zzzzzz pedig államellenes bűncselekményeket készít elő. Én is bemutattam ezt a pofátlanságot, én mit kapok?

Amúgy az ilyen ember elmegy a picsába. Remélhetőleg kicsiny hazánkban nem talál vevőkörre.

Blany 2007.11.15. 09:39:47

Október 26-án kaptam az összes saját domainemhez tartozó (nem publikus!) mailcímemre ezt a spamet. Továbbküldtem internetes jogásznak, hogy lépjünk. Ő konzultált az NHH-val, pontosabban ott dolgozó illetékessel, _gyakorlatilag_ semmit nem tudnak tenni, és bőven kaptak jelzéseket erről a spammerről.

A weboldalakon megtalálható mailcímek gyűjtése _illegális_, erre van törvény, csak szeretik "nem érteni" az emberek. (Reklámjellegű mailt csak a címzett előzetes beleegyezésével lehet küldeni.) Az én privát, tehát honlapokról nem elérhető mailcímemhez meg "duplán" illegális módon juthatott csak ez a fickó.
És lehet hőbörögni, hogy az NHH vagy akárki "állambácsi" miért nem lép, de ne felejtsük el, hogy még az USA-ban se egyszerű az ilyen ügy. Az államtól várt megoldás helyett pofonegyszerű lenne, ha senki nem venne ilyen listákat, nem lenne piaca, és megszűnne (magyar vonatkozásban).

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.15. 16:25:05

@Terveüdekszi:
Nobel díjat nem, de egy korsó sört mindenképpen megérdemel az érdekes információd.
Meglepett hogy ez az yyyyyy ilyen elvetemült, a zzzzzzz arcátlanságáról pedig már nem is szólva, mélyen csalódtam bennük :-O
Most már az sem lepne meg, ha képük megjelent volna a Kretén magazin "Kevésbbé foglalkoztatott bébiszitterek" rovatában ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.15. 22:57:52

Akit érdekel, egy további adalék lehet a témához a Kékfény múltkori adása, bővebben az alábbi linken:
spamblog.hu/2007/11/14/millios-atveres-a-kekfenyben/
Én sajna nem láttam, és utólag most néztem meg, az eladó emailcímes levél is szerepelt benne.

f.zsolti 2007.11.20. 19:02:02

Nos, én rákérdeztem a palira és az alábbi anyagot kaptam:

Üdvözlöm,

és köszönöm az érdeklődését.

Tehát az általam eladásra ajánlott anyag:
- Atomic Email Hunter címgyűjtő program - további címeket lehet küldeni bármilyen nyilvános forrásból,
- Worldcast kiküldő program - ezzel nagyon könnyen lehet bárhonnan hírleveleket kiküldeni, szöveges, vagy html formátumban is
- 200.000 magyarországi cég email címe
- 450.000 vegyes, főleg magán email cím

A címeknél, mint írtam, 10 százalék a hibaszázalék, másnak még nem adtam el, csak email címek, txt formátumban, ezt kezeli a kiküldő program, de átmásolható Word dokumentumba, Excellbe is.

A lebonyolítás: Budapest, és környéke esetén el tudom küldeni futárral, vagy átvehető a belvárosban is, más esetben postai út. Fizetés előtt be lehet nézni, tehát lehet ellenőrízni, ilyesmi.

Az ár: az egész csomag együtt, programokkal: 30.000 HUF.

Bármilyne kérdésre szívesen válaszolok, és örülnék, ha arról is tájékoztatna, hogy ha nem aktuális (válaszig nem ajánlom másnak).

Tisztelettel: Nagy Sándor

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.20. 21:09:12

Szia Zsolti!
Köszi szépen a kiegészítést, érdekes volt. Számomra a fő meglepetést az okozta, amikor azt mondja az emberünk, hogy vár a válaszodra, és addig nagy gálánsan nem ajánlja másnak :-) Hát ez LOL :-D

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.09. 15:00:34

Emberünk úgy tűnik nem nyugszik, ma 14.59-kor ismét beborította szokásos levelét...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.29. 17:54:32

És ime a végkifejlet Abszurdisztánban, nem történt bűncselekmény:
www.origo.hu/techbazis/internet/20080916-nincs-a-spammerek-ellen-betarthato-torveny.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.04.16. 13:57:26

Talán-talán elkenik végre a szájukat:
www.mfor.hu/cikkek/Buntetne_az_e_mail_cimek_adas_vetelet_az_ombudsman.html

Érdemes-e kémkedni a feleségünk után?

2007.11.15. 14:00 | Csizmazia István [Rambo] | 8 komment

Címkék: spyware bűncselekmény nod32 kémprogram házastárs eblaster spyrecon

Egy frissen megjelent cikkben két ilyen ügy is terítékre került - mondhatnánk: **két férfi, két eset.** A számítógépes kémkedéssel, illegális megfigyeléssel vádolt uraknak néhány éves börtönbüntetéssel kell szembesülniük. Az ítéletek már csak azért is érdekesek, mert a **programok hivatalos, legális, megvásárolható termékek**. Persze a korrektség, az őszinteség és a becsület nem találhatók az üzletek polcain. Gondolom védekezésül hasonlókat mondhatnak, mint a Bárányok hallgatnak című filmben Hannibal Lecter: "**ez akkor és ott jó ötletnek tűnt.**"

Az egyik esetben a SpyRecon kémprogrammal történt **az elhidegült feleség számítógépes kikémlelése**. Ennek az esetnek **4 év börtönbüntetés lett vége**. A másik történetben a **SpectorSoft eBlaster kémprogramja** játszotta a főszerepet, amit egy exbarátnő gépére telepített az illető úriember, bár tetténk fényében ez a szó talán erősen kétségbevonható. Itt kicsit már **durvoidba ment át a kukkolás: meg is változtatta a volt szerető jelszavait**, és belepiszkált az eHarmony társkereső oldalán található adataiba is.

Letöltöttük hát az eBlaster programot, **hogy lássuk, hogyan, miért és egyáltalán**. A nagy telepítő csomag ártalmatlan, ezt egy gyors VirusTotal vizsgálattal megnéztük. Induljon hát a telepítés.

Az mondjuk kissé átlátszó púder, hogy kiírja, **úttörő becsszó, hogy csak a saját gépeden használod, és közlöd az illetővel, ha netán más gépére telepíted**. De ha szólsz, akkor minek az egész? :-O Kicsit olyan, mint viccben: "Julcsa, hadd menjek fel hozzád a szénaboglya tetejére, ne félj, nem szerelmeskedni akarok. Hát ha nem, akkor meg minek jönnél fel?" Itt még az lehet egy érdekes momentum, hogy **a munkaadók akár a Bibliára is őszintén megesküdhetnek hazugságvizsgálóval ékesítve, hiszen valóban a SAJÁT gépükre telepítik** :-D

Meg kell adni egy jelszót, amire a titkos billentyű kombináció lenyomása után kinyílik majd az admin varázsszelencéje.

Az alapos fejlesztők még arra is gondoltak, hogy a nyomokat, értsd a telepítő csomagot is el kell tüntetni a színről. Ez **annyira jól működik**, hogy még a másik \TARTALEK nevű mappából is kitakarította az install pack másolatát.

A kémprogram maga egy 3 megabájtos exe, amit a Windows/System32 könyvtárba helyez el, és ennek **a neve** - ugyanis két külön telepítést is csináltam - **mindig más lett**: egyszer maxibser.exe, másodjára kerorfax.exe lett. Ügyes, látszólag közömbös, semmitmondó nevek, akár rendszerfájlnak is nézhetnénk, és persze mondanom sem kell, sem a futó processzek, sem a futó programok közt nem látni - ez egy kémprogramtól evidencia.

Jó hír, hogy **a NOD32-vel simán megtalálható és irtható**, erre még később visszatérünk. Most nézzük, mennyire részletes képet láthattak a férjek. Ehhez az Alt-Ctrl-Shft-S billentyűket kell lenyomni, és a telepítéskor megadott jelszót begépelni. Belépünk hát a csodák palotájába, Szezám, tárulj!

Lépkedjünk a felső menüben: első helyen az e-mail üzenetek állnak, majd **a meglátogatott weboldalak listája**.

Az összes megfigyelt billentyűleütésünk, időponttal.

Az elindított programok listája.

S hogy mozi is legyen (bár a tömörség miatt fekete-fehér), a **rendszeres képernyőképek** között tetszés szerint lépkedhetünk. Így **az egérrel betűnként copy-paste módszerrel bemásolt banki jelszavak sem menekülhetnek** a leleplezéstől.

A NOD32 jól vizsgázott, az effektív, futtatható főprogramot bedobva a VirusTotalba láthatjuk, **név szerint szépen detektálja azt**.

Jó pár éve még PC Worldos újságíróként kaptam egy ilyen kérdést, hogy **elfogadható-e, ha a szülő ilyen, és ehhez hasonló programokkal vizsgálja gyermeke internetezési szokásait**. Elismerem, hogy pokolian nehéz dolog ez. Én úgy vélem és akkor is azt írtam - bár sok veszélyes vonatkozása van az internetnek, és sok kiskorúból kisebb-nagyobb mértékben, de hiányzik az egészséges veszélyérzet, mégsem használnék erre ilyen módszert. Ha pedig gyerek lennék, és észrevenném, hogy a szüleim orvul kukkolnak, bekameráztak, kémprogrammal figyelnének, őszintén csalódnék bennük, amiért nem beszélnek, beszélgetnének inkább nyíltan velem.

Azért egy kellemes tanulságot még levonnék gyorsan: aki ilyen kémprogrammal ügyködne, az ne NOD32 mellett próbálkozzon ;-) Ennyi volt.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Gyerek-barát netezés
- 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/229767

Kommentek:

zvaragabor 2007.11.15. 18:07:18

Gépelési hiba a 8. (Jó hír...kezdetű) bekezdés 3. sorában:
"lenyomnni".

Ezt a féle virustotal eredménytáblázatot te mivel éred el?

Most nézem csak, hogy te magyarítottad az oldalt. :) Grat hozzá.;)

zvaragabor 2007.11.15. 18:35:56

Nem szóltam, megvan...kompakt nézet.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.15. 20:29:39

Kedves zvaragabor!
Köszi :-) Július 26-án lett kész a magyar változat, de azóta is bővül egyre újabb nyelvekkel.

Koronix · http://otletlada.blog.hu/ 2007.11.16. 11:49:45

Szuperjó a post! De azért egy szerencsésebb nősüléssel még több hely marad a HDDn. ;)

A gyerekekről: szerintem ártani nem árt ha így is figyelsz rá, ahogy te el tudsz vele beszélgetni úgy egy rossz szándékú is...és félelelmből sem fogja elárulni a skac. Nem is a gyereket kell így figyelni, hanem azt h egy ilyenbe ne bonyolódhasson bele.

GeraldB 2007.11.16. 11:49:56

Ha én pakolnék ilyet valaki gépére, valószínüleg betenném a nod-nál a kivételek közé ;-) (persze abszolút feltételes módban)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.16. 15:11:53

@zvaragabor:
Koszi a jelzest, javítottam a hibát :-)

@Koronix:
Kicsit teoretikus a dolog, mert nincs gyerekem, és ezzel kapcsolatos közvetlen tapasztalatom, ezért köszi a hozzászólást.

@GeraldB:
Jó a tipp, ha valaki nagyon nem ért a géphez, abszolút feltételes módban így benézheti a dolgot ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.29. 12:54:52

Új lehetőség, mobiltelefon útvonalának megfigyelése - mint a Tűzfal című filmben a kutya fülébe épített chipnél - weboldalon keresztül, jutányos áron:
www.origo.hu/techbazis/mobil/20080929-oroszorszagban-mobilon-figyelik-hol-jar-a-gyerkoc.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2009.07.13. 10:25:05

Egy kis adalék, mitől is lesz jólértesült egy bulvárlap?
Persze szigorúan csak a briteknél, máshol biztosan nincs ám ilyen ;-)
www.origo.hu/nagyvilag/20090710-lehallgatasi-botrany-andy-coulsonnal-a-news-of-the-worldnel.html

Virtuális tolvajok, valódi letartóztatás

2007.11.19. 11:19 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: frei hotel lopás life csalás bútor tér virtuális játékosok gamer habbo second

A Frei dosszié műsorok közül egy igen emlékezetes volt számomra. A 4. dimenzió című adás - bár a fél életemet a számítógép mellett élem, mégis tudott újat és érdekeset mutatni. Aki lemaradt volna, **az online archívumban megnézheti**. Az epizódban többek közt a Second Life játék részleteire derült fény, és az ott látottak fényében földig emelem a kalapom az olyan über-kreatív emberek előtt, aki virtuális aranyat ásnak és online lovakat tenyésztenek. Hogy mi köze ennek a biztonsághoz? Több mint, hinnénk, pedig első hallásra mindenki talán csak a név-jelszó biztonságára gondolna.

Az online játékosok az utóbbi években jelentős mértékben célpontjaivá váltak a különféle csalásoknak, jelszó lopásoknak, még külön tanulmányt is megjelentettek a témáról. Talán meg sem lepődünk, hogy a különféle jelszó lopó trójaiak különösen a Kínát és Dél-Koreát érintik a legerőteljesebben.

Az, hogy a virtuális bútor lopás igazi letartóztatást is okozhat, nos ezt új fejleménynek tekinthetjük. Azért kíváncsiak lennénk, milyen arcot vágnának nálunk egy magyarországi rendőrőrszobán, ha valaki panaszra menne, hogy az orkjának ellopták a virtuális fejszéjét ;-) Szóval a példa természetesen nem magyar, a BBC-News hírei között jelent meg, és a Habbo Hotel virtuális játéktéren történt lopások ügyével foglalkozik.

A Habbo Hotelben mintegy **30 országból hatmillió ember játszik havonta**. A fiatalkorú gyanúsítottakat azzal kapcsoltban hallgatták ki, hogy mások lakásaiból **mintegy 4000 EUR értékű bútort tulajdnonítottak el**. A Second Life-hoz hasonlatosan, i**tt is kifejezhető a játékosok által birtokolt javak igazi pénzbeli értéke**, éppen ez adhatja a jogalapot az eljáráshoz.

A virtuális javak feletti civakodás **alkalmanként valódi gyilkossághoz is vezethet**, 2005-ben egy kínai játékos megölte barátját, aki egy kölcsönkapott kardot a játékon belül eladott. Az eset kicsit hasonlít ahhoz, amikor egy 419-es nigériai csalás kapcsán egy cseh nyugdíjas végső elkeseredésében igaziból agyonlőtte a nigériai nagykövetség – pénze visszaszerzésében egyre csak tehetetlenségét hajtogató – konzulját. Az biztos, hogy egy esetleges **virtuális börtönbüntetés a virtuális csalók és tolvajok számára nem rendelkezik elegendő elrettentő erővel**, muszáj valódival előrukkolni :-)

Mi mást tehetnénk hozzá a fentiekhez, mint hogy az Elátkozott partból idézünk egy rövidet, mintegy lezárásként. Nagy **kár, hogy a mai elektronikus és igazi tolvajoknak látszólag már ilyen ici-pici erkölcsi érzéke sem maradt** :-(

"Jámbor ember vagyok, talán azért, mert anyai ágon egy nagybátyám kántor volt, és már kora ifjúságomban magamba szívtam a jó erkölcs törvényeinek tiszteletét. Ezért csak a legritkább esetben szánom rá magamat arra, hogy Márta napján lopjak."

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/233852

Kommentek:

Nincsenek hozzászólások.

Amikor a telefon hazatelefonál - Frissítve

2007.11.20. 21:01 | Csizmazia István [Rambo] | 1 komment

Címkék: apple iphone et kémkedés abrams imei randy stocks weather

Van amikor ET telefonál haza, de úgy látszik, nem csak vele fordul elő ez a szerfelett érdekes mozzanat. Egy nemrég megjelent hír szerint az Apple figyeli az iPhone készülék használói szokásait, **és továbbítja az Apple szervereire a látogatott weboldalak, emailcímek, hívások adatait**. A cikk szerint a Tőzsdehírek (Stocks) és az Időjárásjelentés (Wheather) kódja rejtett módon a telefon IMEI címével együtt kéretlenül és titokban továbbítja ezeket az információkat.

Az eseményekről a Hackintosh fórumon is beindult az eszmecsere. Egy magyar oldalon is olvashattunk már a dologról, a Mobil Portál cikke szerint megkérdezték az Apple hazai képviseletét, akik **cáfolták az üggyel kapcsolatban** megjelent információkat. Kíváncsian várjuk a további fejleményeket.

Randy Abrams, a NOD32 antivírus alkalmazást fejlesztő ESET oktatási igazgatója az eseményeket kommentálva **rámutatott a helyzet egy másik fonokságára is**, miszerint az így begyűjtött adatok elvileg alkalmasak arra, hogy adatbázisból bárki **csekély erőfeszítéssel kimutatásokat készítsen arról, hogy (az egyes) felhasználók milyen részvények után érdeklődnek leginkább**.

FRISSÍTÉS - FRISSÍTÉS - FRISSÍTÉS - FRISSÍTÉS

Közben több forrásból is - kommentezőktől, levélíróktól - kaptunk jelzést, hogy a valódi IMEI szám nem kerül elküldésre.

A cáfolatról **Arilius** küldte Gizmodo linkjét, a Heise.de oldal pedig beszámol a még így is ellentmondásos helyzetről. Mindenkinek köszönjük!

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- Elégedetlenek vagyunk a Facebook biztonságával
- "Szósölmédia" és nyaralás
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/236186

Kommentek:

Arilius (törölt) 2007.11.21. 09:31:34

izé...azóta van update. az az imei amit küld nem az az imei, sőt nem is telefon, hanem alkalmazás függő. tehát az összes Stocks program ugyanazt a kódot küldi el.

forrás: gizmodo.com/gadgets/iphone-doesnt-send-imei-information-to-apple-324640.php

Fertőző banner hirdetések

2007.11.20. 12:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hirdetés banner csalás hamis antivirus

Sokféle ember van, és bizonnyal akad köztük olyan is, **aki tényleg szereti a reklámokat**, netán még éjszaka is bezabál belőle - én azonban nem tartozom közéjük. Bár **állítólag el kell fogadjuk, hogy ez életünk része, mégis, akit eléggé zavar, és utána néz, tudja mit kell tennie**, felveszi a tvfilmeket videora, hogy át tudja tekerni a reklámot; az internetes böngészésnél meg AdBlock Plus plugint használ, és itt gyorsan le is állok az ötletbörzével, mielőtt még nekem is levelet írnak a jogászok, mint Ajnásznak. A friss hír a következő: a napokban **nagy látogatottságú amerikai sport portálokon több fertőzött hirdetést is találtak**.

A cikk szerint az MLB (Major League Baseball) és az NHL (National Hockey Legaue) oldalain **olyan kártékony hirdetések jelentek meg a DoubleClick rendszerén belül, amelyek átirányították a felhasználók gépeit**. Az ottani szakértők szerint kivédhetetlen volt a trükk, amellyel flash állományba ágyazott kód segítségével térítették el az internetes forgalmat. A machináció révén felbukkanó trükkös hirdetés pedig **egy csalárd antivírus programot próbált letöltetni a gyanútlan felhasználókkkal**.

A basebell és hoki rajongók tömegei valószínűleg valóban meg is ijedhettek a hamis reklám üzenettől, amely szerint a gépük fertőzött. Egy korábbi postban már írtunk azokról a kétes és **hamis vírus- és kémirtókról, amelyek a gép állapotától függetlenül hibaüzeneteket jelenítenek meg és közben agresszíven igyekeznek rábírni az áldozatot a termék teljesértékű változatának megvásárlására**. A Hamis kémirtók cikkben egy hosszú listát találhatunk az ilyen csaló kém- és vírusirtó programokról.

A cikk írásakor az NHL honlapján **már nem éltek a DoubleClick reklám bannerek**, pedig többször is igyekeztünk előcsalogatni őket. Mindenesetre a jövőben a reklámokkal sem árt elővigyázatosnak lenni és továbbra se fogadjunk el sütit idegentől ;-)

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- 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/235493

Kommentek:

Nincsenek hozzászólások.

Legyen Ön is milliomos!

2007.11.21. 09:24 | Csizmazia István [Rambo] | 1 komment

Címkék: spam levél kéretlen

Ha eddig valamilyen ok miatt rejtve maradt volna előttünk a titokzatos módszer, mellyel az aranykarkötős, Longines órás, Ferraris **milliomosok táborához egyszerűen és könnyedén csatlakozhatunk**, úgy most lehull a lepel, és kitárhatjunk elménket. Így kell a 100 leggazdagabb magyar következő kiadványába bekerülni.

A kényesebb izlésűeknek talán ellenükre lehet, hogy **a csodarecept egy kéretlen levélben érkezik, nem fizettünk elő, és nem is iratkoztunk fel álomvalóra-váltó hírlevélre**. Talán a sors vagy egy titkos jóakarónk irathatott fel a listára - legalábbis ezt mormogjuk magunk elé a bajszunk alatt. Bár eddigi tapasztalatunk alapján a milliomosok közül még a legperverzebb **sem ingyenes webtárhelyen** osztotta az észt, azt már végképp nem értjük, **mi viszi rá, hogy másokkal is megossza a titkot, ha ő maga már kőgazdag**, és a varázsmódszerrel kereshetne még többet is? Talán csak nem új balekokra van szükség a rendszerben? Irány pénzkeresés, megyünk a http://penz.freebase.hu/ weboldalra.

Induljon a banzáj, épüljön a piramis, ami persze az oldal készítője szerint nem az, hanem teljesen legális. **Mi szánalmas átlagemberek viszont úgy szeretünk pénzt keresni, hogy ne azzal kezdődjön a dolog, hogy még mi fizessünk**.

Az instrukciók olvasása közben reveláció erejű felismerés hasít belénk: egy régóta kínzó kérdésre - Ki küldözgeti ezt nekem? - hirtelen ölünkbe hull, megkapjuk a választ. **Többezer kiküldött levél, hát "Nem nagyszerű ez?"** teszi fel a kérdést a weboldal készítője? De, rettentően pazar, teljességgel el vagyunk alélva a gyönyörűségtől.

Ejnye no, hát szabad itten kérem kishitűen kételkedni, mikor H. J. Moines, Mitchel Wolf és Charles Morris szerint is ez volt életük legjobb befektetése?

A megtévesztésekkel kapcsolatban, azok gyökerével, a **csalók gondolkodásmódjával igen színvonalasan foglalkozik** Nemere István: Szélhámosok könyve. Aki elolvassa, nem csalódik, remekül szórakozik, és az olyan levente trükköket sem fogja bevenni, mint az áldetektívek áljelentései.

Most befejezem a cikket, mennem kell, ugyanis egy kedves nigériai ismeretlen emailben ajánlott egy nagyobb összeget, ha én előtte küldök neki pénzt, **ezért most szaladok a postára** ;-)

Ajánlott bejegyzések:

- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/236565

Kommentek:

Bobek i Lolek 2007.11.21. 12:44:20

Az ilyen gyökereket kéne a rendőrség-bsa és hasonló ingyenélőknek baszogatnia, nem azokat akik letöltötték a terminátor 43-at valamelyik fáljcserélőn keresztül.

Tudom mit adtál meg jelszónak tavaly

2007.11.22. 10:10 | Csizmazia István [Rambo] | 6 komment

Címkék: firefox javascript jelszó crack tábla rainbow table szivárvány pasword ophcrack md5 hash masterpassword

Semmi új nem lesz ebben a mai cikkben - hehe, ez aztán a remek kedvcsináló - legalábbis annak, aki benne él a számítógépes biztonságban. **Két aprócska módszert mutatunk be** jelszó fronton - az újszülöttnek minden vicc új alapon - aztán lehet hüledezni annak, aki esetleg nem ismerte. Csak egyet nem mondhat majd senki, hogy a látottnak fényében neki aztán nincs semmi vesztenivalója, neki nem kell vigyáznia.

Biztos emlékeznek az Index olvasók a rainbow táblákról szóló cikkre, már a címe is impozáns volt: Percek alatt fejti meg jelszavainkat az új hackerszerszám. Ebben sok minden igaz volt, **de hogy ez új lenne**? Szerencsére akkor Buhera kolléga történelmileg helyretette a dolgokat.

Az hogy **az MD5 titkosító algoritmussal is lehet bűvészkedni**, nem újdonság, ennyit az egyirányúságról. Egy tegnapi érdekes HVG cikk után játszogattunk el három ilyen oldallal (http://md5.rednoize.com , a http://www.md5oogle.com és a http://md5.cryptobitch.de), és igen, szépen működik a dolog. Az, hogy a Google segítségével pedig keresni is lehet ilyesmikre, jól felhívja a figyelmet arra, **ne ringassuk magunkat hamis illúziókba vélt fórumos vagy egyéb biztonságunkat illetően**.

A másik érdekesség **egy aprócska JavaScript kód.** A szkripteket sokan hajlamosak lebecsülni, pedig segítségükkel sok hasznos és sajnos sok kártékony dolgot is lehet művelni. Egy nyár derekán született blogbejegyzésben egy jó kis jelszóvisszafejtő készséget találtunk, ez kísérletünkben FireFox alatt még úgy is simán megmutatta a jelszavakat, hogy közben egy masterpassword védte azokat. Illetve legyünk jóhiszeműek, úgy is lehet fogalmazni, mit tegyünk, ha esetleg elveszítettük a mesterjelszavunkat? A mindössze 327 karakter hosszú - ebben már a kiiratások is benne vannak - **szkriptet bemásolva Firefox címsorába** egy ablakban egy könnyed laza csuklómozdulattal **felkínálja a hiányzó, az aktuális laphoz tartozó jelszót** az elmentett adatbázisból. Bár a cikk azt állítja, Opera és IE alatt is megy, nekünk ez sajna nem működött, ha valakinek mégis sikerült, kérjük írjon egy kommentet!

Sokszor teszik fel a kérdést a barátok, ismerősök, miért kell ennyire paranoiásnak lenni, miért kéne vigyázni egy átlagembernek ennyire? Pont belefutottam egy jó kis Öveges professzor szintű felvilágosító anyagba, **minden szónál többet ér egy megfelelő YouTube videó**,ez következik most.

A tanulság mindenképpen az, hogy jobban kell óvni a jelszavakat, ha pedig mi írunk programot, **az MD5 hash függvény bamba alkalmazása helyett** vigyünk további csavarokat, **saját változókat és XOR-olásokat is az MD5 használatába**, hiszen a számítógépek teljesítménye évről évre növekszik. Ezzel kapcsolatban érdemes az MD5 történetben hivatkozott eredeti blogbejegyzés kommentjeit is átböngészni. **A jelszavakat pedig közösen használt gép esetében SOHA ne mentsük el a böngészővel.**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Tízből öt kártevő hátsóajtót nyit
- Ez történik a weben egy perc alatt
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/237821

Kommentek:

buherator · http://buhera.blog.hu 2007.11.22. 15:02:40

A kriptográfiai algoritmusok esetében abból kell kiindulni, hogy a támadó ismeri azt, ezért a legjobb amit a programozó tehet az, hogy megköveteli az erős jelszavak használatát.
Persze hangos káromkodásokra bírja ösztönözni a támadókat, ha pl. a jelszavakat a felhasználónevekkel konkatenálva hashelik (saját tapasztalat ;)), de egy megfelelően eltökélt hackernek nem jelent akadályt egy, az új "igényekhez" igazított jelszótörő program megírása.

Egyébként jó kis poszt lett, gratula!

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.22. 23:07:16

Szia Buherator :-)
Az említett extra konkatenálásról jutott eszembe, hogy pár éve csináltam egy admin felületes PHP-s cuccot egy cégnek, és most mint akit a tatár kerget, gyorsan megnéztem, nem szúrtam-e el, mi a helyzet ott. Hála Istennek, már benne vannak a rambo-állandók meg az XOR a kutya oltási bizonyítványával plusz a dátum...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.30. 18:11:18

Közben láttam egy ilyet is:
computerworld.co.nz/news.nsf/scrt/C50D36EFEC2B482ACC2573A00070EF83
Hehe, ez már december elsejei cikk :-)
Egy újzélandi biztonsági szakértõ az aucklandi kiwicon rendezvényen olyan Sony PlayStation 3 alkalmazást mutatott be, mellyel nagyon gyorsan lehet készíteni MD5 szignatúrákat. Nick Breese másodpercenként 1,4 milliárd hash-lenyomatot képes elõállítani tetszõleges - akár szótárból vett - karaktersorozatokhoz, stb...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.30. 19:17:34

Mea Culpa, közben láttam a mai bejegyzésedet :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.02.25. 11:26:57

Most látom, hogy az md5oogle oldalt legyakták, és eladó... Az md5crack viszont azóta is él és virul.

titan 2010.04.26. 17:32:22

@Csizmazia István [Rambo]: nem kell félteni azokat, könnyedén fel lehet építeni md5- és egyéb táblákat... azért a hosszú karaktersorozatokkal konkatenált jelszavak már nem annyira könnyen visszafejthetők, hiszen exponenciálisan növelik a kellő tábla méretét. Vagy tévedek tán?

SMS Spam, arghhhh

2007.11.23. 10:41 | Csizmazia István [Rambo] | 3 komment

Címkék: spam sms bank üzenet biztosító kéretlen

A kéretlen email üzenetekre már szinte mindenki kialakított valamiféle stratégiát a Del gomb nyomogatástól kezdve a szofisztikált szűrő alkalmazásokig, és akkor **szépen és lassan kezdenek jönni az SMS spamek**. Most már csak az a kérdés, hogy mi belgák hová álljunk?, de Henry is érdeklődhetne nagy tisztelettel: Hová vezet ez?

Egyszer olvastam egy fórumot, melyben az aluljáróban való nyugalmas és békességes közlekedésről, a kéretlen szórólaposztásról folyt az elmélkedés - köztük a már öt éve végkiárusító cipőbolt a legviccesebb - és az egyik hozzászóló írta, csináltatott egy polót az alábbi felirattal: **"Nem állok meg, nincs egy percem, nem írom alá, nem térek meg, nem veszem meg"**. Ez jutott eszembe, mikor már a második SMS spam bírt beszédelegni a telefonomba. Az elsőnél (*Vásárolja meg a hosszú hétvégére autópálya-matricáját az OTPdirect szolgáltatásokon keresztül*) még nem lettem ideges, bár a tájékoztatás elég lett volna a havi egyenleglevélben is. Jót szórakoztam a Tékozló Homár idevágó cikke fölött, és reménykedtem, ez egy ritka kivétel, nem pedig az első fecske.

Kovács Melinda, zombai lakos élvezettel olvassa hetvenharmadik kéretlen reklámüzenetét...

Nos, **nem iratkoztam fel, nem jelentkeztem, sehol nem publikáltam a mobilszámomat**, mégis jönnek, kopogtatnak, én pedig heves izgalmi állapotban postot írok, bár momentán a fejemben keringő gondolatok alapján **(#@!!brrr grr #%!)** szívem szerint inkább ide szánnám ;-)

Szervezze be anyósát, Mici nénit és Edömér bácsit, és talán még nyerhet is...

Lehet, hogy átsejlik a szavaimon, hogy nem vagyok a reklámkedvelők ligájának az alelnöke, de mégis más egy böngészés közbeni banner, amit ha nem akarok, nem nézek, ha úri kedvem úgy tartja, nem kattintok rá, maximum az X-re, ha kitakar valamit. **Az MSN Live Messenger is olyan már, mint egy karácsonyfa**, alsó reklámbanner, amit a Plus sem szed már ki, mint régen. Aztán ott oldalbanner - de nem vagyok én szőrösszívű, jó legyen ez is, oké. **De hogy kéretlen reklám üzenet érkezzen a telefonra, no way!**

Djuice, mert megérdemlem...

Jó pár éve nem voltam rest elmenni **a Polgármesteri Hivatalhoz, és jól letiltottam a postai címem kiadását harmadik félnek**, belenyugodva a logikátlan helyzetbe, hogy még nekem kell ezért rohangálni, ha nem akarom a sok szemetet kapni IRL a postaládámba. Most ezügyben hova menjek?

Sok minden jó és pozitív **begyűrűzhetne** már kis hazánkba, a nyugati életszínvonaltól kezdve sorolhatnám, **de** sokszor olybá tűnik, a valóságshowk, tv műsorokban szereplő noteszgépek emblémájának homályos gombóccal való kitakarása és egyéb idióta, ostoba és szinvonaltalan dolgok mellett végül aztán mégis a legkevésbbé áhított dolgok érkeznek meg.

Egy korábbi cikkben úgy látom, Nagy Britanniában 2003-ban megtiltották az SMS spammelést. Ha valaki tudja, Magyarországon az SMS spammel kapcsolatban mi a törvényi szabályozás, vagy hogy egyáltalán van-e ilyesmi, szóljon!

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás
- Mai szavunk pedig: keyjacking

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/239109

Kommentek:

Ramod 2007.12.23. 11:22:31

Hali!
Lehet már nem aktuális, de gondoltam megosztom a köbvetkezőket:
Az msnben a bal oldali reklámikon sort ki lehet kapcsolni.
Eszközök/Beállítások/lapfülek/ a lista alatt pedig, lapfülek elrejtése.

Személy szerint Kaspersky Internet Security-t használok, ez kiszűri az alsó bannert is.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.24. 11:47:47

Szia Ramod!
Köszi a lapfüles tippet.
Amit pedig a KAV-ról írsz, az még nekem is újdonság volt :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.09.30. 14:47:15

Kéretlen telefon ajánlatról tanulságos olvasmány, sőt a kommentek olvasása is élvezetes ;-)
homar.blog.hu/2008/09/30/nem_ved_meg_a_hazug_telefonos_zaklatoktol_az_adatvedelmi_biztos

Apple Quicktime sebek

2007.11.26. 18:28 | Csizmazia István [Rambo] | Szólj hozzá!

Újabb sebezhetőségről számolt be a Secunia, amely különösen veszélyes besorolást (**extremly critical**) kapott.

A távolról kihasználható hiba az RTSP vagyis a Real Time Streaming Protocol révén támadható **egy speciálisan félreformázott hosszú "Content type"** adatot tartalmazó csomaggal, és az így keletkező puffertúlcsordulás következtében **távolról tetszőleges kód végrehajtására nyílik lehetőség**. **Hol találkozhatunk ilyennel?** Elvileg bármely weboldalon, ahol QuickTime videót lehet nézni vagy letölteni. Sok helyen érhetők el **videoklipek, mozielőzetesek** ilyen formátumben. A hibát a 7.3-as verzió esetében erősítették meg, azonban emellett más korábbi szoftver változatok is érintettek lehetnek mind a Windows, mint pedig a Mac OS X platformon.

Hogyan tovább? Addig is tartózkodjunk a megbízhatatlan linkektől, weboldalaktól és .QTL állományoktól. **Ne használjunk rtsp:// protokollt**, ellenőrizzük a tűzfal beállításokat (554 TCP, 6790-6999 UDP portok), kapcsoljuk ki az Internet Explorerben QuickTime ActiveX vezérlőt, és tiltsuk le a JavaScriptet a böngészőben, sőt kapcsoljuk ki teljesen a PC-t és Commodore64 gépen játékkal üssük el azt a hátralévő csekélyke időt, amíg a javítás megjelenik ;-)

És hogy a tét még nagyobb legyen, **a sérülékenység kihasználását lehetővé tevő kódok nem csak elvileg léteznek**, hanem már meg is jelentek a neten.

Offtopik utóirat:
Mea culpa, revideálom a múltkori erősen dehonesztáló nézeteimet a reklámokról úgy általában. **Ha nem kéretlen**, mint például a Reklámzabálók Éjszakáján, úgy máris megbocsáthatóbb a dolog, sőt néhány szórakoztatót is láttam, kezdve az archív **Cascot akarok kötni.**..-től kezdve a pár friss darabig (oroszlán a kocsitetőn).

Szóval oké, vannak köztük jópofák, elismerem, csak ne jöjjön kéretlenül, és akkor megnyugszik az én lelkem.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő
- Nyári tanácsok utazáshoz
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/242691

Kommentek:

Nincsenek hozzászólások.

Ötéves Windows hiba - a Microsoft időt kér

2007.11.26. 20:06 | Csizmazia István [Rambo] | 2 komment

Címkék: microsoft hiba xp vista 2000 me hacker újzéland exploit 98 nt

A Kiwicon hackerkonferencián az újzélandi **fehérkalapos hacker, Beau Butler** egy olyan Windows tervezési hibát tárt fel, amivel a felhasználók milliói kerülhetnek veszélybe.

A hiba létét a Microsoft szóvivője is megerősítette, melyről a The Age magazin számolt be. Egy olyan hibáról van szó, **amelyet öt éve már felfedeztek, de az akkori javítás nem volt megfelelő**, és erre csak most derült fény. A probléma mind a hat Windows verziót érinti, **köztük a Vistát is** (Windows 98, ME, 2000, NT, XP, Vista).

A **hiba révén át lehet venni a vezérlést a veszélyeztetett gépek felett**, távoli adatolvasás, jelszólopás, internet forgalom ellenőrzés, valamint spam és vírusküldésre való felhasználásra is lehetősége nyílik a támadónak.

A hiba tesztelése közben a hacker csak Újzélandon több, mint 160 ezer sebezhető gépet talált. Állítólag Butler már küldött korábban egy emailes figyelmeztetést, amire a szoftvercég nem reagált. A **Microsoft most felkérte, hogy a hibajavításig ne tegyen közzé részleteket** a felfedezéséről, a biztonsági csapat pedig gőzerővel dolgozik a javításon.

Ajánlott bejegyzések:

- Kártékony böngésző kiegészítők jönnek
- Tízből öt kártevő hátsóajtót nyit
- Hogyan szúrjuk ki a gyanús Android appokat?
- Dropbox csalival terjedtek a kémprogramok
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/242846

Kommentek:

ihatethisindapassthingy 2007.11.27. 07:53:28

Remélem ez nem ismét a window message-es callback "design flaw", mert azt elég nehézkes Windows hibának bekategorizálni.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.27. 15:33:43

Szia!
Cikkíráskor még semmi konkrétumot nem találtam, de később úgy olvastam, hogy a WPAD (Web Proxy Auto Discovery) szolgáltatással kapcsolatos a dolog.
www.astalavista.com/index.php?section=news&cmd=details&newsid=131&teaserId=

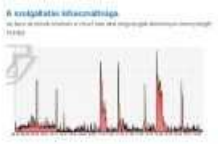
Spóroljunk az erőforrásokkal

2007.11.28. 13:21 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: ötlet vizsgálat erőforrás virustotal

Egy új és okos dologgal **egészítették ki a VirusTotal weboldalt**, amelynek következtében még **gyorsabb válaszidőt remélhetünk** a gyanús fájlok vizsgálatánál.

Az már eddig is működött, hogy magas rendszerleterheltségnél **választhattuk az e-mailes küldést**, ekkor az elemzés eredményét szintén levélben kaptuk meg. Tapasztalataink alapján **a napközbeni munkaidő derekán, úgy 9 órától délután 17 óráig igen sokszor kellett sorbanállni**, és a 2-3 percnél hosszabb várakozási idő sem volt ritka. Az újítás lényege - és itt jön képbe megint a jó kis MD5 hash - hogy az elemzendő fájl MD5 lenyomata alapján a rendszer képes visszakeresni **a már elvégzett vizsgálatokban, és felajánlja a korábbi eredményt**. Ezt megtekinthetjük teljes részleteiben, vagy ha bármilyen okból úgy gondoljuk - például régebbi a korábbi eredmény - **ismételt elemzést is kérhetünk**.



Valószínűleg **sikerül ezzel is rövidíteni a csúcsidős várakozást**, rá fogunk kérdezni spanyol barátainknál a részletekre, az új kiegészítés magyar fordítása pedig (jelenleg angolul van) hamarosan megjelenik.

Ha a bankautomatáknál is **az lenne az alapértelmezett, hogy _NE_ adjon ki egyenlegértesítőt**, és ehhez 2-3 gombnyomás kellene pluszban, nem lenne haszontalan dolog sem adatvédelmi, sem utcatisztasági szempontból :-)

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Informatikai biztonság az egészségügyben
- Akiknek a Captcha kínszenvedés
- Tízből öt kártevő hátsóajtót nyit

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/245396

Kommentek:

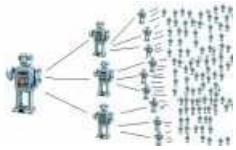
Nincsenek hozzászólások.

Növekvő botnetek

2007.11.29. 14:15 | Csizmazia István [Rambo] | Szólj hozzá!

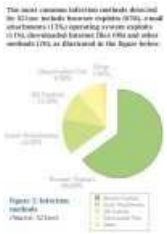
Címkék: zsarolás botnet exploit ess enisa

Az ENISA, vagyis az European Network Information and Security Agency szervezet közzétette legfrissebb biztonsági jelentését, melyben az egyre **emelkedő botnet aktivitásra** és további újkeletű problémákra hívta fel a figyelmet.



A PDF formátumban is letölthető összefoglaló szerint fokozott **veszélyre kell számítaniuk a Blackberry, Windows Mobile és Symbian operációs rendszereket futtató mobil eszközök felhasználóinak**, de növekszik a fenyegetettség **az azonnali üzenetküldök (IM, Instant Messaging) programok (pl. Skype, MSN Messenger) felé is**. Újszerű irányokba is történnek fertőzési, illetve behatolási, kémkedési kísérletek, ezért a Bluetooth kapcsolatok, valamint az SMS és MMS üzenetek is potenciális célpontjai lehetnek a jövő fenyegetéseinek.

A biztonsági ügynökség becslései szerint mintegy **6 millió fertőzött számítógép található a botnet hálózatokban világszerte**, ezek száma kiemelkően magas az USA-ban és Kínában. Egy-egy botnet hadseregben munkálkodó PC-k száma 10 és 300 ezer közöttire becsülhető a spanyol S21sec cég jelentése szerint.



Az ábrán világosan látszik, hogy a korábbi e-mail mellékletekben érekező és az operációs rendszerek réseit kihasználó kártevők mennyiségét sokszorosan (65%) felülmúlják a böngészőkliensek sebezhetőségeit kihasználó exploit kódok.

Jól rímel erre az a hír, miszerint egyes pornográf weboldalak olyan kódokat helyeznek az ingyenes próbaidőszak alatt a felhasználók gépeire, amelyek - a hamis kémirtókhoz hasonlatosan - erőszakosan próbálják meg fizetésre sarkallni az embereket: szűnni nem akaró felugró ablakokkal, melyeket egyszerű módszerekkel nem lehet bezárni, illetve a számítógép újraindítása után sem fejeződik be ezek aktivitása. **A regisztrációs díj** leperkálása után kapják csak meg a lehetőséget **a zavaró szoftver eltávolítására**. **Védelmi pénz beszedése semmiért, egy kis fenyegetéssel, nyomásgyakorlással**, láttunk már ilyet :-)

Hé, te kis klambó, nem kapsz két óriási pofont, ha megmondod, hova ment az autó gazdája!

Azért gyanítom, hogy egy jó vírusirtó-tűzfal párossal biztos nem boldogulna el ilyen könnyen, persze ezzel nem azt akarom sugallni, hogy az ESS felhasználók most rögtön hanyatt-homlok vessék bele magukat az erotikus web-birodalmak sűrűjébe ;-)

Visszatérve a jelentésre, az a technikai feltételeken, biztonsági programokon felül **két fő területre javasol** további erőfeszítéseket: ezek szerint **az átlagfelhasználók felvilágosítására, képzésére** kell kiemelt figyelmet fordítani, valamint **a törvényhozóktól is határozottabb fellépést sürget** a jövő elektronikus bűnelkövetőivel szemben.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/246582

Kommentek:

Nincsenek hozzászólások.

40 ezer kártékony Google oldal hopp

2007.11.30. 12:48 | Csizmazia István [Rambo] | 4 komment

Címkék: google seo weboldal malware codec kodek kártékony

Nem hagyták szó, illetve cselekedet nélkül **a kártevő gyanús keresési találatokat**, ezekről legutóbb a Sunbelt blogjában, illetve a magyar SpamBlogban olvashattunk. Az biztos, hogy az RBN és hasonló rosszindulatú hackerek manipulált reklámjai miatt tényleg kellett már valamit tenni, ezt a részét aláírom.

A Google most több, mint 40 ezer kártékony oldalt vett ki az indexükből. Örvendetes, hogy ilyen lépések történnek, teljesen jogos a dolog. A további nagy **kérdés lehet, hogy később mindez mennyi idő alatt, milyen minőségben és hatékonysággal történik**. Milyen hibaszázalékkal mondja majd egy-egy oldalra, hogy káros vagy nem káros? Akit érdekel - és ez itt a reklám helye - a PC World következő számában a Google és a MetaSploit segítségével kártékony kódokra vadásztunk, az útikalauz és a vadászzsákmány az újság hamarosan megjelenő decemberi kiadásában található.

Vegyünk akkor egy példát! Nézzük meg **a keresésnél a "szalacsi video" szavakat** - ezúton köszi Rita :-) - a találatokat. Azon már fent sem akadok, hogy a kereső Ikeásan letegez, pedig nem szórtunk együtt homokot a tökünkre az óvodában, míg ezzel szemben az AdSense oldalon a nagy komoly "Keressen pénzt webhelyének... pamparam" felirat önözve-magázva fogad.

A Szalacsi videokat, képeket bemutató oldalra sem az ESS, sem más biztonsági programom nem jelzett, az oldal forrásában csak veszélytelen IFRAME taget láttam, és a videok sem kértek semmilyen kodekletöltést, ami ugye már helyből gyanús lehetne.

Ellenpéldaként keressünk rá a "divocodec" szóra, vajon megjelenik-e **"Az oldal káros lehet a számítógéped számára" figyelmeztetés?** Az persze nem, erre nem jelez, akár jöhetne is szerinte.

Hát érdekes ez a gyanús oldal - nem gyanús oldal dolog, annyi szent. Kicsit nehéz átlátni, mennyit könnyít rajtunk a fent említett nagytakarítás? Terelgetve vagyunk valamilyen szinten, szeressük mégis a kártékony, trójait tartalmazó divocodecet, viszont a Szalacsi hívők keressenek magunknak más elfoglaltságot? A világért sem akarnám lebecsülni a weboldalakkal terjedő fertőzéseket, de ugye nem akar Orwellkedni (ejh de szép szó is ez :-) rajtunk senki? Aki a témában olvasni szeretne, annak jószívvel ajánlom a Herbert Schiller: Tudatipar made in USA című könyvet, igen-igen tanulságos.

Egyébként **az elgépeléses weboldalaknak is nagy hagyománya van**, oda pedig nem a keresőn keresztül jutunk el. A weboldalakat hosztoló cégtől, illetve országtól függően ugye nehéz kiiktatni az ilyen káros oldalakat (pl. konkrét URL említése nélkül igen "érdekes" oldalakra lehet eljutni az astalavista elgépelt formáival :-O), ezért valószínűleg könnyebb a megszüntetés helyett az ilyen korlátozó lépés.

Nekem még az is furcsaság, **hogy miért nem link az is, ha mégiscsak megnézném a nem javasolt oldalt**? Miért kell nekem ehhez kopi-pasztázni (höhö, ma úgy látszik nyelvújító napot tartunk :-)? Talán az egyszerűbb lelkű juzereket akarják távoltartani a véletlen kattintástól? Na és persze az is elgondolkodtató, hol vannak azok az oldalak, amiket a Google nem ismer, nem indexel - állítólag a neten ezek vannak többen, sokak szerint mi csak a jéghegy csúcsát látjuk.

Mivel az internet szerencsére szabad, rövid úton - most jósolok, kezemben az üveggömb - megjelennek az újabb keresők, amik csak a Googlenél nemszereplő találatokat listázzák ki vagy pedig azokkal együtt ezeket _IS_ megmutatják. Ugye mindenki emlékszik a McAfee Site Advisorral kapcsolatos korábbi bejegyzésre, ahol több neves site is - igaz csak időlegesen - de a negatív kategóriába esett? **Jöjjön most egy kis gondolatkísérlet! Mi fog történni, ha valaki hasonlót próbálna bevezetni, mint Kínában a Nagy Tűzfal, amivel Tajvanról, és más nem kívánatos oldalaktól akarják távoltartani az ottani nagyérdeműt?** Mi történik majd egy választásnál, ha az egyik párt oldala - minő véletlen - éppen elérhetetlen lesz például a kampány időszak alatt, ki szabályoz majd és ki dönt (Bizottság Együttes rulez:-) az indexben maradásról vagy az onnan kikerülésről, no és ki ellenőrzi azt? Úgy kell kelljünk mostantól reggelenként, hogy rendre megnézzük, nincs-e valamelyik oldalunk éppen feketelistán (hehe, indexen van, ezért nincs az indexben)? Belekerül-e a Dalai Láma oldala vagy a Kuruc.info? És mi történne egy a Google érdekeit veszélyeztető vagy konkurens cég oldalának besorolásával, pagerankjével, ha valaki visszaélne a malware veszélyre hivatkozva, és egy laza csuklómozdulattal kivenné? Persze tudom, ezzel már nagyon is **a teoretikus kérdések vizére eveztünk** sajkánkkal, de azért a lényeg mégis az **"Érdek a világ ura" elv, ugyanis ez mozgatta és ez mozgatja a szálakat** mindig.

Remélem nem sértek szerzői jogot a közléssel, van egy ideillő szuper kis idézet, a régi időkben megjelent scifi történet az általam nagyon kedvelt **Szentmihályi Szabó Pétertől (101 mini scifi - 1988, Füles Mellényzsebkönyvtára), a "Hatalom természete címmel".** Rövid, de velős (sajnos már nem kapni ezt a könyvecskét). Bill Gatestől kezdve minden nagy cég és ország vezetőjével elolvastatnám :-)

"Zurra, a barbár egész életében csak egy dologért küzdött. Azért hogy felszabadítsa szülőbolygóját az idegenek uralma alól. Mert Zurrának és híveinek nem tetszett, hogy a döntések sok-sok fényévnyire innen születnek, s olyan lények döntenek Zurid sorsáról, akik életükben még nem tették ki a lábukat a Naprendszerükből, nem öltek xanikat és nem öleltek vertellai kétfarkú asszonyt. Zurra, a barbár megvetette a Birodalom békés és unalmas hivatalnokait, akik a statisztikai jelentések bűvöletében éltek, és személyes bátorsága kivívta Zurid lakóinak tiszteletét. Kétszer érte lézertalálat, háromszor ültették át az agyát ép testbe, de tri-di beszédeinek költőisége, drámai izzása szemernyit sem csökkent: ő Zurra volt, a Barbár, akinek minden szava a zuridák szívéshez szólt.

A Nagy Felkelés elsöpörte a Zurid sorsát irányító pipogya birodalmiakat, és Zurra, a barbár lett az uralkodója az immár szabad és független bolygónak.

És Zurra, a barbár kivégeztette azokat, akik miatt annyiszor megsebesült és megaláztatott, és számüzetésbe kényszerítette a xanikat, akik aljas módon kiszolgálták a Birodalmat, és annyi vertellai kétfarkú asszonyt importált, hogy minden szabadságharcos kedvét lelhette bennük.

És minden úgy történt, miként Zurra, a király óhajtotta.

És akkor Zurra unatkozni kezdett, és eszébe vette, hogy meghódítja Xaniát, és ő maga is Birodalmat alapít, ahol a szabadság diadalmaskodik, és felszabadítja a rab bolygókat. És vállalkozásait szerencse kísérte, és hivatalnokokat küldött ki a meghódított bolygókra, hogy birodalma ügyeit irányítsák.

De nem tudta, hogy Kedder, a barbár egész életében csak egy dologért küzdött. Azért hogy felszabadítsa szülőbolygóját az idegenek uralma alól... És így tovább..."

Ajánlott bejegyzések:

- Gyerek-barát netezés
- Kártékony antivirusok - villám őrjárat 8.
- Kártékony böngésző kiegészítők jönnek
- 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/247609

Kommentek:

buherator · http://buhera.blog.hu 2007.11.30. 16:05:32

Ezt egy kicsit túlreagáltad szerintem... Lehet hogy a Google maga a gonosz, aki minden szabad órajelciklusát a bolygó lakosságának profilozására költi, de a néhány, MI-k által produkált téves eredménytől az általad vázolt antiutópia szerintem igen messze áll.

A Google egyszerűen nem teheti meg (mint ahogy ebben az esetben sem teszi), hogy letilt oldalakról, mert ezzel saját létét veszélyezteti. A kereső egy _javaslatot_ tesz, és ha a javaslatok 1%-a (ez valószínűleg erős felső becslés egyébként) hibás is, 99%-ban megóvják a felhasználókat a rosszindulatú oldalaktól.
Megnéztem én is az általad említett oldalakat, és két dolog jutott eszembe: az egyik, hogy a szalacsi.hu-t, ha nem tudnám miről van szó, lehet hogy én is kártékonynak gondolnám a rajta elhelyezett, arcbavágó hirdetések miatt. Pedig valamivel jobban tudok magyarul, mint egy MI. A divocodec esetében pedig szerintem ugyanaz a helyzet, mint az adware-anitvirus fronton (de azt hiszem ebbe te jobban belelátsz): a divocodec.com ha nem tévedek egy legális vállalkozás, amely tisztességtelen, de gyakorlatilag jogszerű utakon szerez jövedelmet. Innentől kezdve a Google (pontosabban a stopbadware.org) ugyanúgy nem tehet ellenük semmit, mint ahogy az antivirus sem tehet alapesetben semmit az onlinecasino hírdetésekkel szemben, amit a felhasználó a megfelelő szerződést elfogadva (next,agree,next,next,finish) telepített.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.30. 16:49:47

Szia :-)
Jogos a felvetés, nem akartam én összeesküvés elméletet hirdetni, inkább poénkodtam, szeretem és használom a Googlet, viszont elgondolkodtatni igenis akartam.
A nem kattintható linket a Finjanhoz Secure Bowsinghoz hasonlítottam, ott felteszi a kérdést, hogy bluepill vagy redpill, és megyek az oldalra mindenképp, nem kell címet másolgatni.
A codec és egyéb csalárd progikkal tökéletesen igazad van, jogi okokból is nehéz fellépni ellenük - bár Kaspersky már leboxolt egy ilyen menetet sikerrel, es a divora is siman Troja.blabla kártevőt jelez - a NOD-nál a PUP, vagyis a Potentially Unwanted Programs kategória hozza a jó megoldást, ha bejelölöd a kéretlen veszélyes alkalmazások eltávolítása pipát, akkor például alapból nem engedi feltelepülni a rootkies Mr & Mrs Smith cuccost. Védve is vagy, meg nem is perelhetnek be.
Azért írtam most a postban egy picit hosszabban, mert úgy vélem, az átlagfelhasználó technikai és social naívságát oldani rendszeres közhasznú feladat :-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.11.30. 18:03:15

Közben kijött az Index cikke is a SEO-s csalási esetről:
index.hu/tech/net/xmasgoo30110/

Vidi Rita · http://www.hosnok.hu 2007.11.30. 20:03:21

Halihó!
Megnéztem az Indexen a hírt, (már olvastam amúgy máshol), hát, most szegény seo-sok szerintem izzadnak egy cseppet...

Nem tartom szerencsésnek a "szakma" ilyetén kapcsolatba hozását a sötét oldallal:)

De várható volt már ez, és egy pillanatig sem csodálkozom a történteken, sőt (most én is egy üveggömbbe nézek), ez még csak a kezdet...

A cikked indíttatására ránéztem a szalacsi.hu-ra a linkscanner-rel, és már tiszta, ahogy írtad. Szerintem ilyen esetekben kell írni a Google-nak és magyarázni egy cseppet az oldal bizonyítványát, és le lehet vetetni a káros oldalra utaló elkerülő linket.

Én egyetértek ezzel a dologgal, hogy úgymond "véd" a kereső, de persze ez csak egy pici szelet az oldalra való eljutás számos lehetőségeinek tortájából. Érdekes, hogy az átkattinthatalanság ellenére első helyről csak a harmadikra csúszott vissza az oldal, ha rákeresek szalacsira.

Ha másra nem is jó ez a jelenség, de legalább egy páran tudtunk már erről írni, és ezzel az olvasók közelebb kerülhettek a témához.

Viszont, amin már röhögtem az ez (index cikkből):
"Az oldalak az Internet Explorer biztonsági réseit kihasználva "
meg ez:

"Ha van tanulsága ennek az egész akciónak, akkor az az, amit nem győzök elég sokszor és elég hangosan mondani: mindenki azonnal telepítsen minden biztonsági frissítést a gépére"

ejnye-ejnye...
ennek sose lesz vége...

Csapatmunka és Captcha

2007.12.03. 10:39 | Csizmazia István [Rambo] | 1 komment

Címkék: google captcha torrent jelentés malware rambo űrlap form xrumer botmaster exif

Hogy mire képes **a közösség ereje**, az akár az Index címlapján is látható: vannak jó újságírók és szerkesztők, igyekeznek színvonalas és friss anyagokkal jelentkezni, de már nélkülözhetetlenek a repertoárból a különböző felhasználók blogjai, amik szintén képesek olykor, sőt néhányuk rendszeresen is - érdekes tartalmakat kínálni. Ha most hipp-hopp leszednének minden ilyet, **nélkülük már szinte csupasznak tűnne az oldal**. Most a **Google is a felhasználók segítségére** támaszkodik, és elkészített egy kártékony program bejelentő űrlapot.

Ezzel az új eszközzel bárki jelezheti, ha gyanús weblapra tévedt. A módszer jó, és hasznos, érdemes élni a lehetőséggel. Ha **ma egy oldalt mi veszünk észre és jelentjük, ezzel segítünk másoknak**, holnap pedig mások észrevétele menthet meg minket egy kártékony oldalra való látogatástól, vagy akár egy biztonsági incidenstől.

Az **elv már sok helyen sikerrel működik**, ha rákeresünk például a Rambo 4 filmre, vajon le tudjuk-e tölteni annak ellenére, hogy a bemutató csak 2008 január 25-ére várható, a Torrentz.com oldalon egy rakat találatot kapunk, hogy a Divx változat máris elérhető.

Hagyjuk most bambán figyelmen kívül az oldalon található jelzéseket, és töltsünk le egyet próbaképpen. A majd 700 megás csomag letöltése után hidegzuhany vár ránk: a filmet mégsem tudjuk lejátszani - és minő véletlen ;-) - a sikeres vetítéshez pedig éppen a **Divocodec csomagra lenne szüksége annak, akinek shanghai táncosnő az öreganyja, és baltával pucolja az ablakot**. Mi nem telepítjük ezt trójaival bélelt programot, hanem ismét megnézzük az előbbi letöltési oldalt, de előtte még egy aprócska kitérőt teszünk.

(Jópofa az IMDB oldala, a Rambo 4 filmnél kitett fotók a forgatáson készült képek eredeti, de kicsinyített változatai, amik **megőrizték az EXIF információkat: Karen Ballard készítette egy Canon EOS 5D-vel 2007. július 16-án 11 óra 15-kor**, kézi üzemmódban, 1/500-as záridővel és 5.6-os blendenyílással, de az is látszik, hogy a képet MacIntosh-on Adobe Photoshop segítségével kicsinyítették le a weboldalhoz.)

Na szóval, jól látható, hogy **a netező közösség népes tábora már kinyilvánította véleményét: 19-en jelezték is, hogy ez egy hamis anyag**, egy valaki vírusról panaszkodott, de senki nem volt, aki elégedettségében pozitív voksot helyezett volna a virtuális szavazótérbe.

Vagyis ha figyelembe vesszük a többiek véleményét, akkor nem vagyunk kénytelen a saját kárunkon tanulni - és ez szép, ez jó :-) Ennek fényében úgy véljük, **a Google lépése egy valóban haszos kezdeményezés a malware terjesztő weboldalak ellen**.

A siker azért nem csak rajtunk, bejelentést tevő felhasználókon, hanem **a lapon található Captcha minőségén is múlik majd, meddig áll ellen** ;-) Egy kis borzongatást hagytunk a végére, **az orosz találékonyság újabb bizonyítéka** az XRumer automata Captcha törő, képeket itt találni róla, míg a működést bemutató videó pedig emitt tekinthető meg.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Dropbox csalival terjedtek a kémprogramok
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/250390

Kommentek:

bomi 2008.01.23. 08:56:04

ez az XRumer még ha csak egy szimpla captcha-törő lenne... Az az 'autoregger+uploader for free hostings' sem lehet majd kispályás...

Bigyó felügyelő: ESET SysInspector

2007.12.04. 12:31 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: csomag security smart diagnosztika nod32 eset ess védelmi komplett sysinspector

Az ESS (ESET Smart Security) komplett védelmi csomagja mellé érkezett még egy újdonság is: egy **SysInspectornak nevezett diagnosztikai program**, amely ugyancsak érdekes dolgokra képes. A 32 és 64 bites Windows rendszerekhez készült, és telepítés nélkül futtatható a SysInspector.exe állomány indításával, majd a gép teljesítményétől függően 1-2 perces várakozás (tesztelési ciklus) után egy szép, Vista stílusú ablak jelenik meg.

Az adott rendszer **szoftver- és hardverkörnyezetéről minden részletre kiterjedő információkat jelenít meg** egy fastruktúrában, az alábbi csoportosítás szerint:

- futó folyamatok (Process)
Ez a csomópont részletesen kibontja a futó folyamatok és alkalmazások listáját.

Ebben a hivatkozott DLL könyvtárak is fel vannak tüntetve

- hálózati kapcsolatok (Network Connections)
Itt kapunk egy listát azokról az alkalmazásokról, amelyek TCP vagy UDP protokollon keresztül hálózati forgalmat bonyolítanak le, valamint ellenőrizhetjük az aktuális DNS (Domain Name System) szerver beállításokat is.

- fontosabb Registry bejegyzések (Important Registry Entries)
Ezek közül elsőként az automatikus végrehajtással kapcsolatos (autostart) részek szerepelnek, de a listában található minden lehetséges támadási célpontot jelentő, a belépéssel (Winlogon), a BHO-val (Browser Helper Object), az Internet Explorerrel, stb. kapcsolatos információ is.

- szervizfolyamatok (Services)
Megjelenít minden szervizkent (service) futó folyamatot.

A Microsoft Windows futó folyamatai az 1-es kategórában eveznek

- eszköz meghajtóprogramok (Drivers)
Kilistázza az összes szoftver és harver illesztő programot, verziószámmal, gyártóval, dátummal, stb.

- kritikus Windows állományok (Critical Files)
Ebbe a csoportba a win.ini, system.ini és a hosts fájlok tartoznak. A Win.ini és a System.ini manipulálásával például az autostart folyamatokat lehet manipulálni, míg a host állomány módosításával elérhető, hogy bizonyos weboldalak ne működjenek. Az ilyen átirányításokkal egy támadó például megakadályozhatja a biztonsági programok frissítéseit, de az adathalászok is szokták a hosts mérgezését alkalmazni arra, hogy egy megbízható webhely helyett egy másik URL-re térítsék az áldozat böngészőjét.

- részletes rendszerinformáció (System Information)
Itt az operációs rendszer adatai, környezeti változói, a feltelepített szoftverek és frissítési csomagok listája, a bejelentkezett felhasználók adatait és jogosultságait szemrevételezhetjük.

- fontosabb rendszerfájlok (File Details)
Ebben a csoportban pedig a főbb rendszerfájlok, telepített végrehajtható állományok részletes információit találjuk.

Itt ráncolja a homlokát, mert a StartupMonitor fontos rendszerváltozókkal kerül kapcsolatba, és az alkalmazás egyelőre ismeretlen számára.

Az adatok megjelenítésénél többféle szűrési lehetőséggel is rendelkezünk: a **teljes adatmennyiséget a FULL módban, egy közepes információhalmazt a MEDIUM, míg egy szűk összefoglalót a BASIC módban kaphatunk**. Emellett a különféle bejegyzések különböző, egy **kilencfokozatú veszélyességi skálán** szereplő értékhez tartozó számot viselnek. A 100%-osan ismert, közismert és megbízható állomány, folyamat, elem kapja az 1-es besorolást, a biztonságosnak tűnő, de ismeretlen az 5-ös számmal van jelölve, míg az ismert, de kártékony objektumok a nagyon veszélyes, 9-es csoportba kerülnek. Ezt a kilenc csoportot is ki lehet listázni, vagyis vadászhatunk a különféle veszélyeztettséget jelentő elemekre is. És emellett természetesen ott **van a szabad szavas keresés**, ahol egy beírt kereső szó minden előfordulását vizsgálhatjuk.

Bár hasonló programok régóta léteznek már, hogy csak az ismertebbeket említsük: Sysinternals Autoruns és ProcessMonitor, Stop Startup Monitor, Hijackthis, SIW System Info for Windows, stb., mindenesetre **az ESET SysInspector kártékony programok vizsgálatához egy jól összeállított és hadrafogható univerzális eszköznek látszik** a kártevő ellenes harcban.

A fejlesztők még **a parancsori futtatást** kedvelő powerusereket és rendszergazdákat sem felejtették ki a számításukból: a program GUI nélkül, a commandline-ból is indítható egyedi kapcsolókkal, és képes XML vagy ZIP állományba különféle tartalmú riportokat generálni, és ezeket utólagosan is lehet elemezni, illetve elküldhetők további vizsgálatra.

A **futtatáshoz valóban minimális rendszerkövetelmények társulnak**: 32 vagy 64 bites Intel vagy AMD processzor, NT alapú (2000, XP, Vista, Server 2003) operációs környezet, 35 MB memória, illetve 2 MB szabad hely a merevlemezen. A program egyelőre még béta állapotban van, de hamarosan megjelenik a végleges angol nyelvű változata, amelyet az ESET vásárlói számára ingyenesen bocsát rendelkezésre.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Az XP él, az XP élt, az XP élni fog
- Majdnem mindenki átverhető adathalászattal
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/251763

Kommentek:

Nincsenek hozzászólások.

Duplázás, aminek mégsem örülünk

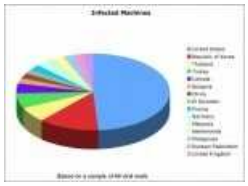
2007.12.06. 13:56 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: malware worm 2007 storm kártevő virustotal 1111

A minap látott napvilágot az F-Secure éves beszámolója, ebben pedig azt írják, a 2007-es esztendőben megduplázódott a kártevők száma. Biztos így van, ha ők mondják, és a dolog a barikád mindkét oldalon érezhető: **minden vírusvédelmi cég úgy látja, hogy az utóbbi időkben hihetetlen mennyiségű vírusminta érkezik a laboraróriumokba**, amik feldolgozása, visszafejtése a hagyományos **kézi módszerekkel már biztosan nem** lenne elvégezhető.

A különböző gyártók víruslabóratóriumai ezért már évek óta fejlesztenek és kísérleteznek olyan eszközökkel, amelyekkel **a feldolgozás egy része automatizálható**. Ezt nagyjából úgy lehet elképzelni, hogy egy ismert féreg 123-ik vagy akár többszáz új variánsát bedobják egy könyvtárba, és a program automatikusan készít belőle egy olyan felismerési definíciót, amelyet már be lehet építeni a vírusvédelmi alkalmazás adatbázisába.

Az elmúlt évben sok mindent láthattunk: a hihetelenül **megerősödött StormWorm férget és a mögötte álló kiterjedt botnet hálózatot**, a pénzügyi csalásokban a Man-in-the Browser trükk megjelenését, elkezdődött a Mac-es gépek elleni próbálkozás, de a Symbian alapú telefonon tulajdonosok homlokára is sikerült ráncokat varázsolni a rossz fiúknak, és az összefoglaló a folyamat további erősödését jósolja 2008-ra is.



Storm Worm helyzet a spamnation.info grafikonján

Azt a felhasználók is érzékelik, hogy egyre több biztonsági incidensről, csalásról kapunk hírt TV-ben, rádióan, újságokból, interneten. Igazából itt **az a csoport veszélyeztetett igazán, aki ezt a bejegyzést sem nézi és szakmai oldalakat sem olvas**, aki a mobiltelefon hangposta kódját 1111-en hagyja, illetve aki abc vagy 123 típusú jelszót használ és sokszor nem is érti és/vagy nem is veszi észre, hogy támadás vagy kár érte. **Jó lenne valahogy őket is elérni a figyelmeztetéssel**, a geekek már amúgy tudnak mindent.

Az értékelésben említett több kártevő miatt természetesen **többször látogatunk el** a 32 víruskeresőt alkalmazó weboldalra mintákat vizsgálni. Ezzel kapcsolatban **több olvasó is jelezte - ezúton köszönjük nekik** - hogy a VirusTotal oldalon a mintafeltöltés után megjelenő ablakban (erről már korábban beszámoltunk, hogy milyen újdonsággal szolgál) hibásan jelennek meg az ékezetes karakterek.

Felvettük kapcsolatot a céggel, jeleztük a problémát, és reméljük a spanyol fiúk hamarosan megoldják ("We are currently working on the different language versions of our new feature.") az Unicode UTF-8 karakterkódolási hibát - várjuk :-)

Miklós napján pedig minden kedves olvasónak Kellemes Mikulást kívánunk :-D

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Gyerek-barát netezés
- Informatikai biztonság az egészségügyben
- Majdnem mindenki átverhető adathalászattal
- Dropbox csalival terjedtek a kémprogramok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/254351

Kommentek:

Nincsenek hozzászólások.

Biztonságos? Biztonságos!

2007.12.07. 14:21 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kártya symbian sms idő douglas john féreg sebezhetőség átmeneti javításig mmc lopásgátló sorozatgyilkosok

Bár önmagáról az ember mindig **korlátozott hatásfokkal mondhat véleményt** (erről lásd az idevágó idézetet a Pipacs, a fenegyerek című klasszikusból: "De, még ha elmeorvos lennék, akkor is kétséges, hogy egy hülye orvos önmagáról megállapított diagnózisa bizonyító erővel bír-e?"), én például elég paranoiásnak és óvatosnak tartom magam, de a következő eset még engem is meglepett. **Nem elég paranoiásnak lenni, annak is kell látszani :-)**.

Amikor egy-egy új O**ffice, PDF vagy egyéb kritikus sérülékenység nyilvánosságra kerül**, megkapjuk a sablonos instrukciót a szoftvergyártótól: **a hiba kijavításáig csak megbízható helyről származó dokumentumokat nyissunk meg, csak megbízható webhelyeket látogassunk**. Muhaha, egyszer elmondhatná valaki, hogy egy párszáz fős munkahelyen keringő, illetve a nemzetközi partnerektől naponta tucatszám érkező (és néha sürgős) munkadokumentumok közül hogyan is kell pedánsan kiválasztania a megbízhatóakat egy átlag dolgozónak.

Olvasom a Symbianos telefonokkal kapcsolatos bejegyzést, és valóban meghökkentő a dolog. Az esetben éppen nem kártevőről, hanem e**gy telefonos biztonsági program összezavarodásáról van szó, ahol is bizonyos körülmények közt a megbokrosodott lopásellenes program** éppen ellentétes hatást váltott ki: **8 másodpercenként SMS-t küldözgetett egy bizonyos telefonszámra**. (Gondolom ez nem kis telefonszámlával járt.) Állítólag formázásálló - mondjuk ezt maximum a saját telefonformázásánál hiszem el, a kártyaolvasómban nem. Az már csak hab a tortán a történetben, hogy ezt a bizonyos 0.95-ös verziójú programot **éppen a szerző kérésére tették bele a felismerési adatbázisba**.

Akik vírusírásból tengetik az életüket, azok most csillogó szemmel, mint zseniális ötletet olvassák ezt, de könnyen meglehet, hogy már dolgoznak rajta, vagy talán rég készen is van ;-) **"Te figyelj, nekem nem látja a telefonom ezt a kártyát, megnéznéd, hogy nálad megy-e? Köszi."** Egy jövőbeli intelligens kártyás kártevő pedig már készíthetne titkos másolatot a **jó prédának számító telefonkönyvről és/vagy az egyéb bejegyzésekről** is, szóval nem lenne veszélytelen a dolog.

A gyanakvás szemlátomást egy olyan dolog, ami szintén állandóan fejlődik, szinte nem lehet túlzásba vinni és **sajnos hozzá kell szokjunk**. Az IRL élet már régóta produkál különféle szabályokat: zárjuk be az ajtót éjszakára, ne vegyük elő a pénztárcánkat nyilvános helyen, ne fogadjunk el édességet idegentől (mert lehet hogy "tudatmódosító cukorka"), stb. Mostantól a **ne tegyünk idegentől, vagy nem megbízható helyről származó memóriakártyát a telefonounkba!** című instrukciónak is át kell hatnia mindennapjainkat - idejutottunk.

Egy kis olvasnivaló extra munició a paranoiás háttérirodalomból:
John Douglas (az FBI Nyomozástámogató Részlegéről): Sötétség, Sorozatgyilkosok és Megszállottak című könyvei.

Ajánlott bejegyzések:

- Gyerek-barát netezés
- 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

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/255262

Kommentek:

Nincsenek hozzászólások.

Webkamerás kukkolók

2007.12.10. 15:28 | Csizmazia István [Rambo] | 24 komment

Címkék: google biztonság hack kamera webcamera webkamerás kukkolók

Egy cikkben olvasom, hogy egy lefülelt észak-karolinai pedofil férfi 110 éves börtönbüntetést kapott és ezt egyáltalán nem sokallom, sőt. Azt hiszem érdemes hangoztatni, hogy **sokan még mindig úgy vélik, a hétköznapi átlagemberek nem célpontok**, nem kell félniük vagy vigyázniuk, pedig vesztenivalója mindenkinek van: pénze, számlája, igazolvány számai, privátszférája, jó híre és nem utolsósorban nyugalma.

Ivory Dickerson bűntársával fiatalkorú lányok számítógépeit hackelte meg, a kifürkészett és begyűjtött személyes adatokkal pedig zsarolta őket és rávette, hogy az interneten keresztül meztelen fotókat küldjenek neki. Annyira alapos volt, hogy **figyelte a lányok kommunikációját, és amikor észrevette, hogy az egyikük egy rokonnal a hackelés gyanújáról beszélgetett, azonnal megfenyegette**. A kémkedéshez a Bifrost trójai kémprogramot használták, ezt pedig emailben (ezt lassan már csak az öregek használják) és azonnali üzenetküldőkön küldözgették. A Bifrost egy viszonylag könnyen beszerezhető kártevő, és többezer verzióban létezik, aminek az a magyarázata, hogy **a készítők igyekeznek mindig úgy fejlesztgetni, hogy a vírusirtók és biztonsági alkalmazások minél kevésbbé legyenek képesek felismerni**. Az FBI ügynökök igyekeztek biztosra menni, és a bizonyíték gyűjtés során néhány ilyen **fertőzött gépet is felhasználtak arra, hogy rögzítsék a kommunkációt**. A házkutatás során rengeteg ZIP meghajtót, minivideo kazettát és DVD lemezt foglaltak le, ami a megfigyelt lányokról készült.

Az hogy **gyermekeink védelmében szükséges a kemény fellépés**, azzal minden jó érzésű ember egyetért, és szükséges az is, hogy a szülők, a felnőttek segítsék a kiskorúak tudatosságát, amivel nem adnak ki magukról az interneten minden adatot idegeneknek.

Az extra érdekességet a történetben inkább az adja, hogy a kémkedés közben a webkamerák figyelése is szerepet kapott, és sokan nincsenek tisztában a veszéllyel. **Ha van egy kamera, akkor a látott kép nem csak nekünk szolgálhat információval**, hanem annak is, aki rácsatlakozik, és ez technikailag egyáltalán nem megvalósíthatatlan.

Két igen szemléletes videoval is alá tudjuk támasztani ezt: egyik és másik. Aki webkamerát használ, **jól teszi, ha kikapcsolja - kihúzza, mikor már nincs rá szükség**, ha pedig privát megfigyelőrendszert üzemeltet, használjon erős jelszavakat és sűrűn olvasson tűzfal logokat.

Benézhetünk egy boltba, ha épp kedvünk tartja: lehet, hogy nem is az egész világnak szánták a látványt? Buli lehet, mikor a boltos reggel begépeli a jelszavát ország-világ előtt :-) És persze **ha mi megyünk valahova vásárolni, nézzünk mosolyogva a képernyőn ülő teddymackó gombszemébe**, ki tudja éppen ki hackelgeti ;-)

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony böngésző kiegészítők jönnek
- 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/259063

Kommentek:

Sáfrány 2007.12.10. 19:56:35

Mekkora egy kamucsávó vagy kisbarátom. Azoknak a WEBkamerákmak a legeslegnagyobb része, amiket az "inurl"-el kezdődő keresésekkel lehet megtalálni ELEVE publikusnak vannak szánva, mert nincsenek lekódolva.
Most akkor mit is találtál fel okostojás? Feltaláltad a Guglit, bravó.

Kihúzni a kamerát, üldözési mániás-e vagy?

amondó (törölt) 2007.12.10. 20:30:55

nem. valószinűleg tapasztalatból tudja, hogy az emberek mennyire nem törődnek a biztonsággal. Felrakja a kamerát online, hogy a kutyust a munkahelyről is nézhesse, de csak addig állítgatja, amíg neki működik, arról nem gondoskodik, hogy másnak ne működjön.

Én nem vagyok hekker, mégis volt olyan, hogy közeli wifi-router konfigurációjába be tudtam lépni, mert az illető nemcsak, hogy wep-titkosítással, MAC szűréssel nem védte a rútert, de még a default gyári jelszót se változtatta.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.10. 20:33:33

Üdv Csilibili!
Wow, úgy érzem nem éltem hiába, volt értelme reggel felkelni, ma feltaláltam a Guglit :-D
A mániára azt mondom, az átlagnál biztosan paranoidabb vagyok, abban a részben igazad lehet, ezt vállalom. Egyébkén volt egy jó kis demo az idei Hacktivity-n: laza rácuppanás egy belsőkamera rendszerre...

dark future · http://www.andocsek.hu 2007.12.10. 20:42:58

IP-kamerákra csatlakozni nem nagy kunszt, főleg akkor, ha nincsenek lejelszavazva :-). Ha meg Gipsz Jolánka USB kamerájáról akarsz streamet lopni, ahhoz valami nehézsúlyú trójaival előbb be kell hatolnod Jolánka gépébe :-), de akkor már ilyen erővel bármihez hozzáférhetsz a gépen.

Comment + : aki ZIP-lemezen ("ZIP-meghajtón" :-)) tárolja 2007-ben a cuccát, az eleve sikeres ember nem lehet...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.10. 20:52:39

@dark future:
Hello dark future!
A ZIP drive-os megjegyzésde szerintem szellemes és találó :-)

@ Egész világ:
Az Index oldalán lévő headlinet NEM én írtam, a szerkesztők kicsit felturbózták a leadet, hogy sokan olvassák ;-) A lényeg abban van, amit dark future ír, hogy két féle eset van: vagy nézegetsz akármiket a Google-val illetve célzottan trójaival támadod a célpontodat és így operálsz.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.10. 21:08:35

Szia superfool!
Szerintem ez nem az, ez inkább szándékos bulivideo :-) Folyamatosan mozog a kamera, szerintem kizárt, hogy titokban készült volna. Egyébként a Spectrumon volt korábban olyan pasi, aki öltözőfülkékben, női WC-kben dugott el kamerát vagy búzt el videozni, és úgy bukott le, hogy egyszer beszakadt alatta a mennyezet és lehuppant a megfigyelt áldozat mellé. Magyar eset is volt, a tornász VB a MOM parkban, ott Csisztu Zsuzsát és a többi tornászlányt vettek fel videóra meztelenül titokban. Szerintem azt is érdemes figyelembe venni, mit érezne az, akinek a saját a nővére/huga/kedvese/felesége esne egy ilyen akció áldozatául, és valaki orvul felpakolná a felvételeket a netre, ezt már biztros senki nem találná jópofának. Érdemes mindig mindkét fél szemszögéből nézni az eseteket.

gravy_t 2007.12.10. 21:27:04

Csizmazia István [Rambo] 2007.12.10. 21:08:35

superfoolra nem kell reagálni, ezeket a videókat az összes blogra bespammeli, ahová csak tudja.

grigorij (törölt) 2007.12.11. 06:31:53

Néhány hsz-ról nekem az egyszeri gyerek esete jut eszembe, aki állandóan hivalkodott, hogy ő már tapasztalt szexelő, mit neki a gumi, ő soha senkit nem csinál fel - erre beszerzett egy AIDS-készletet... Nem értem... Valaki tisztességes hangnemben felhívja valamire a figyelmet, erre néhány nagyokos azonnal nekiesik! Miért hiszi mindenki, hogy a világ kizárólag olyan, aminek ő ismeri?

flimo13 2007.12.11. 08:32:39

Szia!

Csak nem Édesapádnál fogok vizsgázni az ELTE-n?:)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.11. 09:11:27

Szia gravy!
Köszi az infót.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.11. 09:12:39

Szia grigorij!
Egyetértek, ifjú programozói koromban megtanultam, hogy nagy a különbség a "nem lehet megcsinálni" és a "nem tudom megcsinálni között". Mindig jön egy finn, akinek elég ideje van, és feltöri :-) a közmondás szerint. Úgy vélem az helyesebb hozzáálás, hogy ha valaki elég időt szán rá, úgyis bejut, mint az, hogy ide aztán tuti nem nem jut be senki. Ez hamis illúzió és veszélyes hozzállás. Volt szerencsém már húsz éve is olyan fickókkal együtt dolgozni, akik assembler és C programozóként hihetetlen dolgokat mutattak, buherálgattak.
Később a víruslaborban is voltak okos srácok, például az egyikük az F-Secure kódfejtő versenyén is helyezést ért el:
www.f-secure.com/weblog/archives/00001244.html

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.11. 09:15:26

Hello flimo13!
Szerintem nem, csak névrokon lehet, az én édesapám szőlőnemesítő és már nyugdíjas:
www.zalaihirlap.hu/fooldal/20060824_a_nemesito_tiszteletere/print

buherator · http://buhera.blog.hu 2007.12.11. 09:37:44

[flame]
@Csilibili

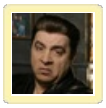
Te gondolom az a fajta ember vagy, aki fikázni szeret, gondolkodni viszont nem annyira:
Ha valóban publikusak azok a felületek, akkor hogy van az, hogy bárki mozgathatja/zoomolhatja a kamerákat? Gondolom a közös erőforrásokkal kapcsolatos problémáról még az életben nem hallottál. Egyébként meg mi az hogy "lekódolni"? Tudod hogy mit jelent maga a szó?

Az ilyen lámákat jobb helyen megeszik reggelire.
[/falme]

Bocs, de nagyon felhúztam magam. A Hacktivitys móka egyébként egy fokkal komplikáltabb volt, ugyanis ott az admin felület nem volt elérhető, csak a titkosítatlan adatfolyam.

krtek2 2007.12.11. 10:20:47

amondó: Csak jelezném, hogy se a wep titkosítás, se a mac szűrés nem ad biztonságot, mindkettő viszonylag hamar feltörhető. Ezeket el lehet felejteni.
A random generált hosszú ssid, plusz ssid szórás tiltása, mindez wpa2 titkosítással a nyerő.



baliquez 2007.12.11. 10:23:13

"Ha valóban publikusak azok a felületek, akkor hogy van az, hogy bárki mozgathatja/zoomolhatja a kamerákat?"

Ugyanmár, first come, first served. Azon felül meg jöhetnek a prioritások ha szükséges, probléma megoldva.
Lehet belőle problémát csinálni persze, hogy felvehesd a fizetésed valamiért.

Épp eleget dolgoztam már rencergizdákkal ahhoz hogy tudjam mekkora kamucsávók vagytok, elkúrni a működő hálózatot rendszeresen (optimalizálás címén), aztán fontoskodva sóhajtozva rendberakni (miközben az egész cég tiszta idegbaj), aztán vinnyogni a sokpénzért meg túlóradíjért. Miközben semmi tapasztalható pozitív változás nem történt.

Persze nem az okostojás pofájára freccsenti a tisztelt megrendelő (befektető stb.) a habosféceszt, hanem a főnökéére, akit mellékesen (hálából a munkahelyéért) folyamatosan átbasz a rencergizda. Hát pacikukit a rencergizdák púzójába, mert a legtöbb megérdemli. Egy böcsületest mutassál, akkor visszavonom.

Lekódolni (mivel nem vagyok programozó) esetemben és itt annyit jelent hogy "kóddal biztosítani és fenntartani az erőforrásokhoz való kizárólagos hozzáférést a kód ismerői számára." Bitbúvároknak biztos mást jelent a lekódolni (gondolom a programozással, programírással lehet kapcsolatban), ez itt speciel köznyelvi kifejezés, lehet kapálózni attól még használatban marad.

Ne idegeskedj, felesleges. Inkább gondolkodj Te is.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.11. 10:40:59

Szia krtek2!
A wifi dologban teljesen egyetértek, kettő perc alatt ki lehet törni wep jelszót, én is kipróbáltam :-)
A WPA2 _jobb_, de rainbow táblával az is nyitható. Ha biztosra akarsz menni, a Radius serveres hitelesítés alapú dolgok maradnak, eddig talán ez a legjobb.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.11. 10:46:56

Kedves baliquez!
Köszi a hozzászólást, megértem az indulatodat, mint minden szakmában, itt is vannak, akik misztifikálják a tudásukat, szellemileg szerényen bútorozottak és másokból élnek. Sajnos én is találkoztam nem egy ilyennel.
Azért hidd el, hogy akad a rendszergazdák között becsületes is, én magam két ilyet is ismerek. Megvan a komoly tudásuk - néha még a hatóság is kér alkalmi tanácsot tőlük, és tudtommal soha nem tettek becstelen dolgot, pedig az IQ és a tapasztalat meg lenne hozzá.

buherator · http://buhera.blog.hu 2007.12.11. 10:55:12

"Ugyanmár, first come, first served. Azon felül meg jöhetnek a prioritások ha szükséges, probléma megoldva."

Igen, de ha public felületen az egyik felhasználó bebillenti jobbra a kamerát, a másik meg balra, a harmadik meg rázoomol valamire, amit a hárommal ezelőtti állapotban látott (mindezt persze válaszidőn belül), akkor senki nem lát semmit, marha jó lesz.
Rendszergazda egyébként nem vagyok és nem is voltam, viszont láttam néhány tucat admin felületet jelszó nélkül kinnt lógni az interneten, úgyhogy hidd el, tudom miről beszélek (és ez nem a rendszergizda, hanem általában a programozó sara)!

A kódolással kapcsolatban ezt olvasd el: hu.wikipedia.org/wiki/K%C3%B3d
magyarul van, érthető. Nem hiszem hogy jogod lenne addig bárkit is "okostojásnak", vagy "kamucsávónak" titulálni, amíg az általad használt fogalmak jelentésével sem vagy tisztában, nem beszélve arról, amiről írsz.

krtek2 2007.12.11. 10:58:08

Valamit összekeversz... A radius hitelesítés, a wpa2 titkosítás. A kettő nem kizárja egymást, hanem együtt működnek. (Otthon persze nem mindenki üzemeltet radius szervert.)
A wpa2-psk, amire Te gondolsz, akkor biztonságos, ha nagyon hosszú és tényleg random kulcsot használsz. Ekkor nem lehet belátható időn belül sniffeléssel megtörni. Csak úgy lehet, ha ellopják valahogy a kulcsot a gépedről...

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.11. 11:14:19

Szia buherator :-)
Koszi a kommentet. Az admin jelszó nélküli cuccokat én is megerősítem, wifi router cserénél volt olyan, hogy az új beüzemelésénél véletlenül egy másik, a környéken lévő cucc adminjában találtam magam. Ez lehet programozói hanyagság egyfelől, és tudatlanság másfelöl: az átlagember azt hiszi, hogy hazaviszi a routert a tescoból és védve lesz mindentől. Pedig a doboz maga nulla, ha nincs vagy rossz a testreszabott konfigja.

@ egész világ:
Az okostojás jelzőre én is azt kérném, vitatkozzunk szakszerűen, NE egymást sértegetve érveljünk, intelligens emberekkén különbözzünk a politikai színtéren zajló adok-kapok fikázós színvonalhoz képest. Előre is köszönöm.

@krtek:
Igen, így együtt gondoltam én is a kettőt. Amit pedig a végén írsz "ha ellopják a kulcsot" pedig a lényeg: ez jobb, mai tudasunk szerint sokkal jobb, de 100%-os védelem NINCS, vagyis technikailag és/vagy social engineeringgel mindig lehet fogást venni.

krtek2 2007.12.11. 11:29:26

Naná hogy nincs 100%-os védelem, de nem is erre kell törekedni. Hanem arra, hogy a biztonság (és a ráköltött pénz) arányos legyen a biztonsági kockázattal (és a hekkelés miatt elvesztett pénzzel). Tehát az otthoni felhasználók wpa2-psk-val is biztonságban érezhetik magukat, mert valószínűtlen, hogy a szomszéd gyerek azért tör be a gépedre ellopni a kulcsot, hogy utána ingyen lóghasson a wifis neteden.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.17. 06:38:46

Egy kis adalék a témához:
A Universal Plug and Playt (UPnP-t) támogató hálózati eszközökben felfedezett sérülékenység egy rosszindulatú Flash állomány segítségével kihasználható, figyelmeztetett a veszélyre a US-CERT. Ha valaki meglátogatja a Flash állománynak otthont adó webhelyet, a támadó lehetőséget kap az érintett eszközök - routerek, kamerák, nyomtatók stb. - átkonfigurálására, és ellenőrzést szerezhet azok felett. Szakértők az otthoni routerek 99 százalékát veszélyeztető sérülékenységet igen súlyosnak minősítik. Miután a behatoló átvette a router vezérlését, megkerülheti a tűzfalat, támadást indíthat a routeren keresztül webhelyek ellen, és megváltoztathatja a hálózati beállításokat. És mivel módja van az elsődleges DNS szerver módosítására is, a routert és az általa vezérelt hálózatot a céljait kiszolgáló zombivá alakíthatja.
www.gnucitizen.org/blog/flash-upnp-attack-faq

titan 2010.04.27. 10:15:52

Szerintem hozzáfűzendő, hogy olyan webcamot érdemes venni, ami jelzi egy LED-del az aktív állapotot, így ha netán sikerülne kikerülni a biztonsági intézkedéseket (amik egy még mindig fontosak), akkor is lehet látni, hogy valaki a kameránkkal garázdálkodik.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2010.04.27. 12:42:04

Anno volt hasonló a Commodore64 1541-es floppynál is, hogy "csak akkor ír", ha ég a led. Aztán kiderült, mégse így van. Gondolom, itt sem szentirás a piros led bekapcsolása a működéskor, illetve ha leragasztom a kamerát, akkor azzal 100% megoldottam a problémát. Persze ezeknközben a géptestbe beépített lehallgató még így is működhet ;-)

A jelszóválasztás csődje

2007.12.11. 13:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: iwiw biztonság jelszó gyenge hossz

Talán nincs is biztonsági szakértő, aki ne hangoztatná egyfolytában **a megfelelően erős és rendszeresen változtatott jelszavak fontosságát**. Ehhez képest bár biztos nem én reklamálom meg először, de **az IWIW jelszavak beállítási lehetősége egyszerűen botrányos**.

A történet rövid és szomorú: **ha valakiben meg lenne az igény**, hogy normális jelszót lőjön be magának, **akkor sem teheti**: az admin felülelet felülről korátozva a mélyen szánalmas 8 azaz nyolc (sic!) karakterben jelöli meg a password maximális hosszúságát - 2007.-ben (38 éve ember a holdon) tisztelt hölgyeim és uraim.

Jó lenne, ha a fejlesztéseknél ez is no meg a **közösségi oldalakon spammelő** kétes elemek távoltartása is napirendre kerülne.

Sajnos heveny izgalmi állapotban kitöröltem a mai kettőt, ezért van itt kérem még októberi illusztráció

Mit tehetünk addig is? Kihasználjuk a kis- és nagybetűk, számok, valamint speciális írásjeleket, és reménykedve várjuk a hosszabb jelszóbeállítás mielőbbi eljövetelét...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Tízből öt kártevő hátsóajtót nyit
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/260307

Kommentek:

Nincsenek hozzászólások.

Webkamerás kukkolók II.

2007.12.12. 18:50 | Csizmazia István [Rambo] | 6 komment

Címkék: zoom internet sony webcamera webkamerás kukkolók

A nagy vihart kavaró múltkori post látszólag elkalandozott a vírusvédelemtől, de **a számítógépes biztonságtól, a kémkedéstől és az ez ellen való védekezéstől már nem állt annyira távol**. Most - **mintegy a dolog lezárásaként, néhány gondolattal kiegészítjük a témát.**

Ha összefoglaljuk az első részt, **a Google segítségével keresgéltünk hozzáférhető webkamerák után**. Akkor ilyen keresőkifejezéseket nézegettünk:

- inurl:/view/index.shtml
- inurl:"axis-cgi/mjpg"
- inurl:"VieverFrame?Mode="
- inurl:"view/index.shtml"
- inurl:"MultiCameraFrame?Mode="

Most is hasonló módon fogunk keresgélni, a mai első kifejezés legyen:
inurl:"viewerframe?mode=motion"

Ez már rögtön érdekesebb, mondhatni haladócsoportos, **itt már lehet babrálni is a kamerát :-)**. Első helyszínünk egy gyárbelső, képméretet lehet váltani, világosíthatjuk a képet, szabadon pozícionálhatjuk jobbra-balra, valószínűleg a főnökök is itt figyelik a termelés menetét, valamint a szorgos dolgozókat.

Keressünk most megint másképp:

- intitle:"Live View / -AXIS"

Ezúttal egy irodát pécézünk ki (magunk közt szólva nem lehet egy nagy öröm ilyen munkahelyen dolgozni, hogy az adatvédelmi vonzatokról ne is beszéljünk) és megpróbálunk zoomolni is egyet az ismerős XP hátterű képernyőre: sajna, **igazi optikai nagyítás helyett csak digitális zoom** van, Pixel Péter köszönget nagy tisztelettel a képernyőről.

A Control után nyúljunk a Setup-hoz. **Igen helyesen nevet és jelszót kér, és nem hagyja** - legalábbis ennyire fapadosan nem - szétkonfigolni az eszközt.

Egy jelszóval védett magyar kamera: mindent a szemnek, semmit a kéznek, ez így van jól

Vigyázó szemünket most egy Sony kamerára vetjük:

- intitle:"snc-rz30 home"

Itt már jobb az eredmény, navigálhatunk és zoomolhathatunk kedvünkre, ráadásul a képminőség sem romlik a nagyítás révén.

Előhozunk egy rendszámtáblát nagytotálba

Néhány további érdekes keresési lehetőség még (Na szóval, jó kis eszköz ez a Google :-)

- inurl:indexFrame.shtml "Axis Video Server"
- inurl:LvAppl intitle:liveapplet
- intitle:"WJ-NT104 Main"

Kivácsiságból rákerestünk az eszköz alapértelmezett jelszavára, ami admin/admin, de itt résen voltak, és ennyire nem adtak magas labdát: megváltoztatták. Feltörhetetlen dolgok nincsenek, ez nem vitás, de az alapvető óvatosság miatt helyesen tesszük, **ha ilyen eszközt vásárolunk, akkor a gyári beállításokat azonnal megváltoztatjuk**, és erős jelszóval védjük. A **routerek esetében is alap dolog, hogy a behatoló elsőkörben kipróbálja a default gyári jelszót. Ha valaki lusta volt, és nem változtatott, már ebben az első körben elvérezhet** - ez nagyon mukinyulas dolog. Részünkről ezzel most (jó időre) lezárjuk a témát, igazából ennyi lett volna a webkamerás kirándulás és a "nagy" tanulság, reméljük azért volt, akinek újat tudtunk mutatni.

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Az XP él, az XP élt, az XP élni fog
- Elégedetlenek vagyunk a Facebook biztonságával
- Utaljunk pénzt a S.O.C.A.-nak
- "Szósölmédia" és nyaralás

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/261885

Kommentek:

MrG 2007.12.13. 14:41:48

Hmmm...
Meglepő a hasonlóság...

www.householdhacker.com/?p=24

zebi 2007.12.13. 15:05:31

női úszócsapat öltözője nem volt?
se iráni atomlétesítmény?

d.hardman 2007.12.13. 15:48:39

aha, hát ez úgy 3 éve még újdonság is volt

nyomasek_bobo · http://sopron.e-cafe.hu 2007.12.13. 16:25:58

Volt erről egy előadás a tavalyi Informatikai Biztonság Napján (Papp Péter, kancellar.hu), de valamiért levették az összefoglalóját az oldalról.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.14. 11:47:01

Üdv mindenkinek!
@ MrG:
Több helyről keresgéltem, de ez az oldal nem volt közte. Azért köszi a linket, ez tényleg egy szép gyűjtemény :-)

@zebi:
Sorry, ezeknek neked kell utánajárnod...

@: d.hardman:
Pontosan ezért írtam ezt "reméljük azért volt, akinek újat tudtunk mutatni."

Csizmazia István [Rambo] · http://antivirus.blog.hu
2009.04.03. 11:29:21

A betörőknek úgy tűnik elég a Google kereső Street View is, hogy alaposan felmérjék a terepet. Egyre többen féltik az otthonuk biztonságát emiatt:
www.penzcentrum.hu/cikk/1017061/1/egesz_anglia_a_google-t_gyuloli_ratamadtak_egy_fotosra_is

Messengeren kopogtatnak

2007.12.14. 22:42 | Csizmazia István [Rambo] | 2 komment

Címkék: msn live messenger trójai kártevő

Egy rövid post következik, kedves cimborám benyelt egy kártevőt, és ilyet még én sem láttam élőben: **MSN accountján keresztül automatikusan üzent nekem (angolul) majd egy fájl kísérelt meg küldeni**.

A küldött ZIP-re persze jól rányomtam és letöltöttem, mi is ez. A belsejében egy .COM kiterjesztésű állomány pihen. Érdekes **a fájl neve is, az MSN partner címéből kreálja**. **Maga fájl igazából egy EXE**, amit valószínűleg a Morphine EXE packer segítségével tömörítettek össze.

Több példányban is elküldte a fertőzött gép, és az érkezett fájlok hossza is rendre változott kis mértékben. **A NOD32 szépen hárította a Win32/Agent.DBP trójait**.

Bedobva a VirusTotalba az alábbi képet mutatta, és Tadaaaam, **végre elkészült a már vizsgált állományok ékezethelyes képernyőképe is** :-D

A cimborával letöltettem a NOD32 próbaváltozatát, ami jól bekaranténozta a trójait, így **most már végre mindenki mehet végre aludni**, jó éjszakát gyerekek, álmodjatok szépeket...

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Az XP él, az XP élt, az XP élni fog
- Android kémprogram persze csak a mi érdekünkben
- Hogyan szúrjuk ki a gyanús Android appokat?
- Safe mód a Mechagodzilla ellen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/264344

Kommentek:

balint96 2008.01.07. 16:51:24

Egy új msnvírus kopogott múltkor,sajnos én nem értek túlzottan ehhez de kíváncsi lennék hogy mi ez?
Kép:kepfeltoltes.hu/080107/msnvirus_www.kepfeltoltes.hu_.jpg

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.11. 14:32:46

Szia Balint96!
Sorry, hogy nem válaszoltam azonnal. Megneztem az altalad kuldott dolgot, itt szuletett belole egy iras:

antivirus.blog.hu/2008/01/08/sarah18

Vírusleírások magyarul

2007.12.14. 18:04 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: magyar lexikon kártevők részletes virusleírás

A Víruskommandó blogon volt Ritának egy szépen összeszedett írása, amely arra hívta fel a figyelmet, a **hazai vírusvédelmi oldalak közül néhányan mennyire kevés figyelmet szentelnek a próbaváltozatok letöltésének**. Néhol órákig kell keresgélni, van ahol valamilyen rejtélyes ok folytán (persze értem én;-) regisztrációhoz kötött, és nemes egyszerűséggel olyan hely is volt, ahol nem lehet próbaverziót letölteni. Mostani őrjáratunknál azt keressük, **hol és milyen minőségű vírusleírásokat találunk ékes magyar nyelven**: azt már most elárulhatjuk, a kép most is nagyon vegyes.

Próbaképpen igyekeztünk keresni **egy részletes leírást a Sasser féregről**, amely az emlékezetes gépújraindításokat okozta 2004 május elején. Már **az is egy jó eset volt, ha egyáltalán találtunk viruslexikont**, ahol viszont voltak leírások, ott meg is találtuk a nem csekély hírnévvel rendelkező kártevőt, abból is a korai verziókat néztük.

Első utunk az ABC rendben első AVG-hez vezet:
http://www.avg.hu/index.php?viewpage=sitemap
Az oldalon egyáltalán **nem szerepel víruslexikon**, így rövid úton lépünk is tovább.

Következik a Dr.WEB:
http://www.doctorweb.hu/
Hosszas fürkészés után **sem bukkan elő kártevő lista**, ezért GOTO a következőre.

Az F-Secure magyar oldalát keressük fel:
http://www.f-secure.hu/oldalterkep.html
Hát bizony **itt sem sorakoznak azok a fránya vírusleírások**, pedig finn oldalon van belőle szép számmal. Itt egy kicsit engedünk a 48-ból, icipicit besegítünk: lévén ez egy saját korábbi munkahely, és tudható, hogy a VirusHíradó oldalon szerepelnek az F-Secure és Kaspersky vírusleírások. Közvetlen link nem vezet ugyan rá - pedig jó lenne - de az "Affiliate network" jegyében készült navigációs fejléc azért átvezet az óhajtott oldalra:
http://www.virushirado.hu/leirasok_gyujto.php

Itt már halmozódik az öröm, sokféle leírás mellett a Sasser is egyenesen ránk kacsint:
http://www.virushirado.hu/leiras.php?id=465
Szép **részletes, használható leírás**, a kapcsolódó Registry kulcs pontos helye, link az eltávolító segédprogramra és a kapcsolódó Microsoft Security Bulletinre.

Következik a NOD32 oldala - ez éppen tegnap kapta meg az Év honlapja díjat - és erőfeszítéseinket itt is siker koronázza:
http://www.nod32.hu/virus/sasser-c

Itt is szép részletes leírás szerepel, **képekkel illusztrálva**, a kapcsolódó Registry kulccsal, és linkkel a kapcsolódó Microsoft közleményre. Plusz egy további érdeme, hogy **az érintett platformok listája, valamint a kártevő összes ismert elnevezése (alias)** is megtalálhatóak egy keresztrefencia táblázatban.

Indulunk a következő helyszínre, a Panda oldalára:
http://www.pandasoftware.hu/
Magyar nyelvű vírusleírásokat nem sikerül fellelni, ezért folytatjuk a kirándulást.

A McAfee magyar képviselete következik:
http://www.piksys.hu/
Erőfeszítéseinket itt is siker koronázza, nem csak lexikon van, de még Sasser leírás is mosolyog felénk:
http://www.piksys.hu/vinfo/sasser.htm

Részletes **leírás, képekkel, linkkel a Microsoft Bulletinre és az egyedi mentesítő programra, az érintett Registry kulcs tartalma**.

A Sophos felé vesszük az irányt:
http://www.swoffice.org/tmsi/sophos/frame_sophos.html
Leírásoknak se híre, se hamva, ezért szedjük is a sátorfánkat.

A Norton következik a sorban:
http://www.symantec.com/hu/hu/sitemap/index.jsp
Kattingattunk veszettül, de **magyar vírusleírásokhoz nem sikerül el navigálni, a linkek zöme angol nyelvű oldalra vezet**.

A BitDefender és az F-Prota következő áldozat:
http://www.virfilter.hu/page.php?pg=bitdefender/bitdefender_antivirus
http://www.virfilter.hu/page.php?pg=fprot/fprot
Sokat nem kell meresztgetnünk a szemünket, **itt bizony egy árva leírás sem található**.

A VirusBuster oldalára kanyarodunk a vége felé:
http://www.virusbuster.hu/hu/viruslabor/leirasok/sasser_a
Van leírás gyűjtemény, és a Sasser féreg is "Jelen" felkiáltással lép előre az oldalról.

A leírás tartalmazza - **igaz csak szövegként - a Microsoft Bulletinre vezető linket, a Registry kulcs leírását**. Az oldal érdekessége még, hogy bár **a leírás itt volt a legrövidebb, de mind a magyar, mind az angol változat** elérhető.

Összességében bár volt részletes magyar leírás mind a VírusHiradó, a VirusBuster valamint a Piksys lapján is, **a NOD32 oldalán található leírás látszott a legalaposabbnak**, legteljesebbnek, esetenként még video anyagot is tartalmazott a szemléletesség kedvéért. A többi webhelyen pedig nem csak az egy szem Sassert, hanem **úgy általában a magyar nyelvű vírusleírásokat is hiányoltuk**.

Ajánlott bejegyzések:

- A PRISM szeme mindent lát
- Kártékony antivirusok - villám őrjárat 8.
- Majdnem mindenki átverhető adathalászattal
- Elégedetlenek vagyunk a Facebook biztonságával
- 25-ször több a mobilos kártevő

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/263728

Kommentek:

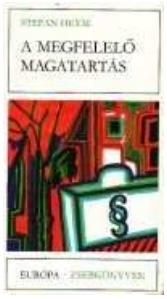
Nincsenek hozzászólások.

A megfelelő magatartás

2007.12.18. 13:28 | Csizmazia István [Rambo] | 2 komment

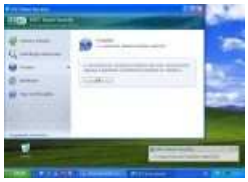
Címkék: frissítés levelező kliens antivírus sorrend av

Ha van akinek a cím visszaköszön, annak gratulálunk, nekünk is tetszett Stefan Heym jó kis könyve. A kölcsönvett címbe most valami egészen mást igyekszünk egy rövidke gondolattal beleszőni: **kisujjtörés helyett a PC bekapcsolásának hogyanjáról és mikéntjéről lesz szó**.



A számítógép indításakor sokan nincsenek tisztában azzal, hogy akár az alkalmazások **indításának sorrendje is fontos lehet**. Manapság már szinte nincs is olyan víruskereső, amelyik automatikusan ne frissítene, vagyis sosem vagyunk arra kárhoztatva, hogy kézzel kelljen megnyomnyi egy "update" feliratú gombot, különben az adatbázis régi marad.

Ennek ellenére eltelhet egy kis idő, mire az antivírus megkezdi, illetve be is fejezi az adatbázis frissítést. Programja válogatja, hogy van ez szabályozva, illetve beállítva: az internet kapcsolat feléledése után többnyire elindul ez a folyamat is. A lényeg, hogy **érdemes végigvárni azt a kicsi időt, hogy először jöjjön a frissítésről szóló kis buborék ablak, és csak ez után tanácsos megnyitni a levelezőprogramot**, addig ne töltődjön le semmi.



Jó tudni, hogy **levélmellékletként érkezhet akár egy vadonatúj, addig ismeretlen kártevő** is, és akár ezen a néhány másodpercen is múlhat a felismerés sikere. Itt aztán tényleg érvényes a "Ki időt nyer, életet nyer" mondás.

Ami még emellett egy extra dolog, hogy **az intelligens karanténnal felvértezett vírusvédelmi programok a frissítési procedúra után újra megvizsgálják**, hogy a korábban karanténba helyezett állományok esetén az új adatbázissal sikerül-e a korábban csak törlésre javasolt fájlok valódi mentesítése, és megteszik ezt a lépést, ha igen a válasz.

Ajánlott bejegyzések:

- Android kémprogram persze csak a mi érdekünkben

- 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/268106

Kommentek:

Moonline 2007.12.18. 23:31:58

Üdv!

Azt lenne a kérdésem, hogy a magyar nyelvű ESS, és a NOD32 mikor lesz elérhető? Mert amint a képen látom már van magyar verzió.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.19. 12:48:26

Szia Dante01!
A képeken még a megjelenés előtti bétatesztes program szerepel, roham léptekben készül a magyar megjelenése, tudtommal heteken belül a polcokon lesz.

A pofonegyszerű megoldás - Frissítve

2007.12.19. 16:24 | Csizmazia István [Rambo] | 4 komment

Címkék: protected megoldás pdf védett fapados nyomtatás fájlba

Éppen több PDF dokumentumból fordítgattunk, mikor is szótárazás közben felugrott (már rosszul kezdődik) egy ablak, miszerint **ez itten egy copy protected állomány, meg hogy a szövegkijelölés nem engedélyezett**. Vannak embertípusok, akik nem szeretnek ilyeneket hallani: eztet kérem nem lehet; ezt megoldották, hogy ne lehessen..., stb. A világért sem szeretnénk elbitorolni Buhera kolléga székét, de **egy olyan hétköznapi, egyszerű fatengelyes (mondhatni: mukinyulas) trükkel háritottuk el Windows alatt az említett nehézségeket** (aki C64-en nevelkedett, annak nincs lehetetlen ;-), hogy magunk is meglepődtünk. Szinte felrémlett a kezetlen-lábatlan alak a Gyaloggaloppból, és kiegyeztünk döntetlenben :-)

Nem akarok jogi hercehurcákban szerepelni, ezért most egy semleges példa PDF fájlon mutatom be a dolgot, íme egy ugyanolyan védett PDF, ifjonti hévvel a "Select Text" gombra bökünk, és keserves arccal konstatálhatjuk az üzenetet: nekünk coki.

Sebaj, jöjjön az univerzális SolidConverter, majd az szépen ledarálja RTF-be (igaz csak az első oldalt csinálja meg a shareware verzió, a teljes dokumentumot csak a fizetős alakítja át. Védett dokumentum bedob, vár, és persze itt is **felkoppanunk: kéne a mesterjelszó, ami persze nincs**.

A kísérlet harmadik percében megszületik a zseniális ötlet: **nyomtassuk ki a PDF-et fájlba, PDF-be, de már a PDFCreatoron** (ezt állandóan használjuk, ingyenes PDF készítő, nem is kellett külön telepíteni) keresztül.

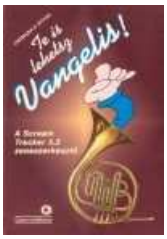
A gondolatot tett követi, és lőn világosság, Hawaii, dj, ésatöbbi. **Az újonnan keletkezett állományból már bátran kopi-pésztezhet** a polgár úri kedvére. Nem kellett hozzá semmilyen világmegváltó furmányosság, extra eszközkészlet, csupán csak egy fapados ötlet.

Tudom, letölthettem volna különböző PDF törő cuccokat, de szerintem **néha jók ezek az agytornásztató, mezitlábas leleménnyel bélelt mellékvágányok is**...

* * * * * **F R I S S Í T V E** * * * * *

Az egyik kommentben Ihatethisindapassthingy javasolta, hogy a védett PDF-et küldjem el magamnak a Gmailre. Nekem nagyon tetszett az ötlet, ki is próbáltam nyomban, sajna a Gmail "hárított", ennek ellenére jópofa az tipp.

Annak idején, mikor (fiatal voltam, hehe;-) a Trackeres zenékről írtam a könyvemet, ott is volt egy jópofaság, amiről megemlékeztem, engedelmetekkel beidézem "Te is lehetsz Vangelis, 1996":



idézet ON

"Bátran kísérletezzünk
Az új ötletek, a fantázia szabad szárnyalása adja a legérdekesebb eredményeket. Bizarr ötletre álljon itt a következő példa:
Valakinek eszébe jutott, hogy mi lenne, ha hangszerminta helyett különböző egyéb állományokat töltene be: úgy mint COMMAND.COM, MAIN.GRP, SYSTEM.INI, akármilyen bitmap, esetleg egy két dokumentáció, FILE_ID.DIZ, paletta állomány avagy ASM forráskód, teljesen mindegy, és ezen próbált meg valamilyen többé-kevésbbé dallomos dolgot összehozni. Nem lett mondjuk egy Santana sláger, sistergős, kattogós, a címe is jellemzően "Agyszipolyozó vadállat" lett. Nem is hallgatható meg egynél többször, de a hozzáállás a lenyőgöző: Ne mondja meg senki, mi lehet a hangszer és mi nem, ha támad valami ötlet, bármivel lehessen trükközni."

idézet OFF

Ajánlott bejegyzések:

- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Mi a közös bennük? Trójai, Chrome, kormányzat
- Tízből öt kártevő hátsóajtót nyit
- Elégedetlenek vagyunk a Facebook biztonságával

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/269533

Kommentek:

buherator • http://buhera.blog.hu 2007.12.19. 23:22:18

Jó trükk, nem ismertem

Üdvözlünk a klubban ;)

ihatethisindapassthingy 2007.12.20. 07:45:39

Én elküldtem volna magamnak a gmail.com-os accomra, az tud automatikus konverziót HTML-be. Azt nem tudom, hogy az ilyen copypaste védelem ellen mit tesz. Mindenesetre külön szoftvert nem igényel :)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.20. 08:46:45

Szia Buherator!
Köszönöm alássan ;-)

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.20. 08:48:14

Szia Ihatethisindapassthingy!
Az ötlet jó, de itt sajna nem válik be: lásd frissítést az eredeti postnál :-(

Ismét a NOD32 az év vírusirtója

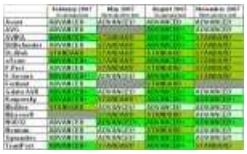
2007.12.20. 13:21 | Csizmazia István [Rambo] | 7 komment

Címkék: az 2007 év vírusirtó nod32 av comparatives vírusirtója

A nemzetközi, független **AV-Comparatives vírusla**boratórium **negyedévente összehasonlítja** a különböző vírusirtó rendszereket. A laboratórium szakértői a tesztelésre beküldött termékeket meghatározott szempontok szerint előtesztnek vetik alá, így a publikálásra kerülő vizsgálatban csak a kiválasztott vírusirtó rendszerek vehetnek részt. Az idén elvégzett négy teszt során a legtöbb vírusirtó szoftver egyenetlen teljesítményt mutatott. Míg sokan szerezték meg az elérhető legmagasabb, Advanced+ minősítést egy vagy két alkalommal, csak az **ESET NOD32 és a Kaspersky tudta ezt háromszor is megismételni**.

A két antivírus rendszer közül az ESET NOD32 teljesített jobban, mely a **három Advanced+ mellett egy Advanced minősítéssel** zárta az évet, míg a Kaspersky ugyan háromszor is megszerezte a legmagasabb minősítést, egy alkalommal azonban Standard besorolást kapott.

Mindezek alapján a víruslaboratórium – a tavalyi évhez hasonlóan – **idén is a szlovák ESET vírusirtóját, a NOD32-t választotta az év antivírus szoftverének**. Az értékelésben a szakértők kiemelték, hogy a NOD32 a tesztek során **nagyon kevés téves riasztást produkált, emellett keresési sebességével, alacsony erőforrásigényével, valamint kitűnő proaktív védelmével** is kiemelkedett a mezőnyből.



Az Év antivírus rendszere díj mellett az **AV-Comparatives öt alkategóriában is értékelte** a vírusirtókat. A Kézi indítású víruskeresés kategória győztese az AVIRA (egy keresőmotoros alkategória), illetve a GDATA AVK és a TrustPort (multi-keresőmotoros alkategória) lett, míg a **Proaktív kézi indítású víruskeresésben az ESET NOD32 győzött**.

A **Legkevesebb téves riasztás kategóriában** a NOD32, a Symantec, az eScan, valamint az F-Secure került díjazásra, a **Kézi indítású víruskeresési sebesség** kategóriában pedig a NOD32, a Fortinet, a Symantec, valamint az AVIRA ért el kiemelkedő teljesítményt. Végül a **Polimorfvírus-felismerés kategóriában 100 százalékos teljesítményével** az ESET NOD32-t és a Symantecet díjazták.

Ajánlott bejegyzések:

- Kártékony antivirusok - villám őrjárat 8.
- Android kémprogram persze csak a mi érdekünkben
- Mi a közös bennük? Trójai, Chrome, kormányzat
- 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/270332

Kommentek:

zlad (törölt) 2008.01.19. 16:33:40

Sziasztok!

Lenne egy kérdésem. Feltettem egy angol ESS Smart Security-t,
lehet ezt valahogy majd magyarítani, vagy kényteln leszek letölteni majd a magyar verziót? A másik kérdés: tanácsos-e a Smart Security-t összeereszteni CounterSpy-al? Ha nem, akkor
mit ajánlotok mellé valami plusz kémprogram-védelemnek?

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.19. 19:51:16

Szia Zlad!
A magyar egy másik telepítőcsomag lesz, el kell indítani, és az angolt leszedi, magyart felteszi és a beállításokat is megőrzi.
A CounterSpy-t nem használom, így erre nem tudok mit mondani, nálam a SpywareTerminator és a SpyBotSD szépen muzsikál az ESS mellett.

Charlie Brown 2008.01.22. 08:28:48

Év vírusirtója? huh.. Az elmúlt hetekben nem győztem kézzel pucolni a gépemről a pendriveokon kapott autorun vírusokat, amikre a NOD olyan magasról fütyült, hogy csak na! :(
Még szerencse, hogy van Kaspersky, Panda meg AVG, igaz leirtani azok se tudták, de legalább sivalkodtak hogy gáz van, miközben a NOD boldogan mosolyogva vakargatta a tökét.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 09:17:34

Hello Charlie!
Nem akarom én itt megvédeni a NOD-ot, de a beállításokkal minden rendben volt? Ha a "Veszélyes alkalmazások detektálása" és a "Kitejesztett heurisztika" be volt kapcsolva, egyszerűen hihetetlen, hogy ilyen történjen, pláne úgy, hogy közben a KAV és a Panda meg észreszi. A két legjobb, leggyorsabb labor pontosan az ESET és a KAV :-O

Csizmazia István [Rambo] · http://antivirus.blog.hu 2008.01.22. 09:19:03

Igazából azt akartam irni, hogy a heurisztikus keresésben ők az ászok...

Charlie Brown 2008.01.22. 10:29:19

Bizony, külön ellenőriztem, minden vacak be van kapcsolva, és direkt megkérem hogy vizsgálja már meg a könyvtárt amibe kigyűjtöttem a kártevőt, és röhögve átengedi az egészet, dll-t, exe-ket, az egész istenverte vírust. Ja, közben az AVG már sikít, hogy vírus van benne.

Pár hete ugyanezt játszottuk el egy másik hasonlóval, és már régesrég tudtam róla és védekeztem ahogy tudtam (thanx AVG...), mire a NOD vírusadatbázisba bekerült, igaz csak félig-meddig, mert irtani azután is kézzel kellett...

zoloe 2008.01.22. 16:32:30

Kedves Charlie,

Légy szíves ilyenkor küldd el nekünk ezeket betömörítve, jelszóval védve a support kukac sicontact pont hu címre. Köszönöm együttműködésed!

Humán faktor

2007.12.22. 21:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság szálloda account butaság postit

Utaztunk egy picit, Bécsben jártunk és kiélveztük a határnyitás örömeit. Szép hangulatos volt a város, nyüzsgő, mégis nyugalmas. Ami miatt szóba kerül ez az egész, **az a szállodában látható** - nem is nevezzük meg a műintézményt, hiszen nem cél a kipellengérezésük - **egészen pontosan a recepciós pultnál**.

Igaza volt Mitnicknek, mikor arról beszélt, minek technikai részletekkel vesződni, mikor leggyakrabban **az ember a leggyengébb láncszem**? És igen, a nem túl jó minőségű (a feltűnést kerülendő telefonnal készült) felvételen jól látszik, a személyzet a hotel információs rendszer **accountját (név és jelszó) a monitor szélére ragasztott sárga postit cetlijén tartotta**, amit odakönyökölve csak az nem olvasott el, aki nem akarta.

Ehhez képes már csak apróság, hogy a mindenki által igénybevehető pénzbedobós számítógép lehetőségei között nem csak internetezés, hanem Messenger lehetőség is volt. Gondolom nem lövök teljesen mellé, hogy **vannak olyanok, akik gyanútlanul szépen begépelik nevüket és jelszavukat egy ilyen közös gépnél**....

Azt, hogy **a Lajtán túl sem mindenki zseni**, korán megtanultam, még az Erőterv billentyűzetét koptattam egy nemzetközi projektben dolgozva, melyben többek között egy híres és jónevű német partner cég is képviseltette magát. Adatállományok érkeztek rendszeresen a partnerektől, ezeket mi összefésültük, kiegészítettük, aztán az eredményt **adathordozón** - ami akkoriban 1.44-es floppy lemezt jelentett, **valamint** a dokumentálási előírási rend alapján **leporellón kinyomtatva is** rendszeresen elküldtük a cégnek, hogy tovább bővítse, az üres mezőket folyamatosan töltse ki, ahogy gyűlnek az adatok.

Volt szerencsém az adatállományok összehasonlító vizsgálatát Clipper nyelven programozni, és több ízben is **feltűnt, hogy a visszakapott dBase állományban rendre előfordultak már olyan kitöltött mezők, melyen visszamenőleg megváltoztak: egy-két tizedes jeggyel elcsúszott a nagyságuk**. A tételes ellenőrzésnél mindig az derült ki, hogy **elírás, az eredeti érték a helyes**, viszont azt elképzelni sem tudtuk, **mitől romlanak el a már egyszer helyesen felvitt mezők**, míg aztán...

Míg aztán egyszer csak fény derült mindenre: kiderült, **a nemzetközi hírű német mérnökiroda egyszer sem használta az általunk küldött adatlemezt, hanem egy dolgozóval minden egyes alkalommal újra és újra begépeltették az éppen megkapott kinyomtatott listából az adatokat** - többezer tételt! Durvoid! Nem szóltak, hogy nem tudják megcsinálni, nem kérdeztek, nem kértek segítséget, hanem lódobogást játszottak a billentyűzeten, többször is teljesen feleslegesen dolgoztattak valakit, és persze **eközben történtek a nevezetes tizedes vesszős elgépelések**...

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Mi a közös bennük? Trójai, Chrome, kormányzat
- "Szósölmédia" és nyaralás
- 25-ször több a mobilos kártevő
- A jelszó érték, vigyázzunk rá

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/272794

Kommentek:

Nincsenek hozzászólások.

Boldog Karácsonyt

2007.12.24. 11:03 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: xmas kellemes karácsonyi ünnepeket

Lassan vége az esztendőnek, és a biztonsági szakma véleménye pesszimista: nagyjából Kellér Dezső és Churchill között helyezkedik el. Az első szerint a "Milyen év lesz jövőre?" kérdésre azt feleli: "Rosszabb mint az előző, de még mindig jobb, mint a rákövetkező". Winston papa pedig igaz, adott egy nagy darab húst a királyi oroszlánnak, de "Csak vért és könnyeket" ígért. Mi ennél többet szeretnénk és **reméljük, azért valahogy sikerül ebben a nehéz és bonyolult világban is megtalálni az arany középutat**, hogy a belebolondulás helyett egy kis figyelemmel, valamint jó biztonsági programokkal felvértezve **biztonságos és nyugalmas számítógépes környezetben élhessünk**. Történeteinkkel, gondolatainkkal a jövőben is igyekszünk ehhez egy cseppet hozzájárulni.

Minden kedves Olvasónknak Békés Kellemes Karácsonyi Ünnepeket Kívánunk!

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- 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/273972

Kommentek:

Nincsenek hozzászólások.

Megágyazunk, beágyazunk

2007.12.26. 10:10 | Csizmazia István [Rambo] | 5 komment

Címkék: flash kompatibilitás karácsony xmas excel embedded beágyazott

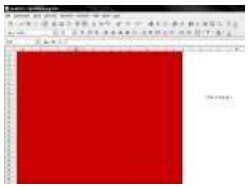
Gondolom, nem mi voltunk az egyetlenek, aki vicces **karácsonyi képeslapként megkapta a táncra, sőt dalra fakadó birkát**, és nagyívű társait. Ami kissé szokatlan egy átlag üdvözlőlaphoz képest, hogy **egy flash állománnyal van dolgunk, ami egy igazi Excel táblázatban húzza meg magát** vagy inkább terpeszkedik - ennek eldöntését már végképp az olvasóra bízzuk...

A számolótáblába ágyazás tényleg jópofa, bár kétségkívül eseményszámba megy, ha nem URL linket, képállományt vagy flasht, hanem egy 1.2 MB-os Excel táblát kapunk karácsonyra. **A zenés részen kívül teljesértű a táblázat, képletezni is lehet**. A dolog azért szerfelett érdekes, mert **az ilyen típusú beágyazás tárgya nem csak jóindulatú kód lehet, hanem kártékony program is elhelyezhető így**, és a vírusirtókat könnyen zavarba lehet hozni (sőt rossz esetben meglepni). A dologhoz nyilván **maga Microsoft is hozzájárul a dokumentum formátumok szerkezete körüli titkolódzásával**.

Pici nyomozgatás után felleltük az eredeti képeslapot a greetings.icq.com weboldalán

Teljes a kakofónia, még a zokniban is dalolnak...

Még egy apró momentum - ami talán a freeware-ek szerelmeseinek lehet rossz hír - hogy az állítólag teljesen kompatibilis OpenOffice (mi a 2.3-as magyar változattak próbáltuk) **nem volt képes normálisan, azaz működőképesen megjeleníteni ezt az állományt**.



Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Informatikai biztonság az egészségügyben
- Az XP él, az XP élt, az XP élni fog
- Akiknek a Captcha kínszenvedés
- Mi a közös bennük? Trójai, Chrome, kormányzat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/275248

Kommentek:

dwdHU 2007.12.26. 15:20:05

fantörpikus

kpityu2 2007.12.26. 15:56:07

Pár éve, egy vezető magyar hardverforgalmazótól vásároltunk egy 800 000 forintos CAD munkaállomást. Az ajánlatot office dokumentumként mellékletben küldték el. Amikor szóvá tettem, hogy mondjuk pdf helyett miért egy vírustelepen küldték az ajánlatot (nem volt benne vírus) ,ami ráadásul minden gépen másként néz ki, azt válaszolták hogy törvény írja elő. Mindenesetre én minden kéretlen office cuccot alapból törlök.

görbén felfele néző 2007.12.26. 16:01:53

"az állítólag teljesen kompatibilis OpenOffice (mi a 2.3-as magyar változattak próbáltuk) nem volt képes normálisan, azaz működőképesen megjeleníteni ezt az állományt"

Ez jó hír az OOo használóknak. :) (mi van ugyanis, ha Santa vírust hozott?)

"maga Microsoft is hozzájárul a dokumentum formátumok szerkezete körüli titkolódzásával"

- Akkor most mivel is kellene "teljesen kompatibilis"-nak lenni?
Talán ezért (is) kell Open Document formátumot használni.

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.27. 17:26:00

Szia Kpityu!
Számomra meglepő ez a "törvény írja elő..." érv :-O
Na persze nem mintha a PDF-be nem lehetne bármit is beleágyazni...
Pl. antivirus.blog.hu/2007/10/05/pdf_a_biztonsagos

Csizmazia István [Rambo] · http://antivirus.blog.hu 2007.12.27. 17:46:40

Szia Görbén felfelé néző!
Jó hír, ha nem nyitja meg a fertőzött állományt, de rossz ha a hasznosat sem :-P
A titkolódzás szinte folyamatos, még anno az első makró vírusoknál jött ez elő: minden AV cégnek magának kellett visszafejtenie a dokumentum formátumokat (DOC, XLS, stb.)

Szerintem is klassz dolog az OO, a világért sem akartam én megszólni, sőt le a kalappal a monopólium ellen küzdő fejlesztők áldozatos munkája előtt. Csak éppen, ha pl. egy cégnél áttérnének, akkor nem biztos, hogy a doksik 100%-ával tudnák használni, hanem a többségével.
Ugyanilyen gond lehet egy telezsúfolt XLS táblával is, pl. egy computeres árlista sok kicsi, agyonformázott mezővel. Az egyszerű dolgokat jól mutatja, a bonyolultabbaknál néha vannak megjelenítésbeli eltérések.
Ha valaki spórolni akar, jó ötet lehet egy MS licenc + a többi gépre free OO, aztán ha gond van, akkor a vezérgépnél még lehet konvertálgatni, vagy a problémás doksit helyben szerkesztgetni.

Keresztelő és a Boldog Új Év

2007.12.31. 11:52 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: vírus folyamat buék névadás kártevő fájl process retrovírus

A kártevők a keletkezett fájlokat manapság már **igen megtévesztően nevezik el**. Íme egy példa: a futó folyamatok közül az LSASS.EXE általában a Local Security Authentication Server program, de van olyan kártevő, amelyik ugyanilyen EXE néven kerül a gépbe. Itt egy jó víruskereső segíthet, és az a megfigyelés: míg az eredeti LSASS a System32 mappában lakozik, a Trojan.Lsass a Drivers/Etc mappába települ.

Íme egy mai hír, érdemes megnézni a létrehozott fájlok listáját:

- %Windir%\iexplore.exe
- %Windir%\System32\mslogon.dll
- %Windir%\diskguard.dll
- %Windir%\find32.exe
- %Windir%\mspwd.exe.
- %Windir%\System32\manager.dll
- %Windir%\System32\ckcn.exe.

Általában is megfigyelhető, hogy a jobb megtévesztés miatt mennyire trükkös neveket használnak a vírusírók, **kinek lenne például bátorsága letörölni mondjuk** egy igen hivatalosnak látszódó HOSTS.EXE nevű állományt a Windows könyvtárából? Persze aki tudja, hogy **alapból ilyen nem is létezik**, annak könnyebb a helyzete, de most a laikus átlagfelhasználó szemszögéből akartuk mutatni, **ha nem pont virus.exe-nek hívják (erre kár is lenne várni) a kártékony kódot, mindig lehet némi zavart okozni** a berkekben ;-)

Van aztán olyan is, hogy egy alkalmazás védeni akarja magát - lehet ez egy biztonsági program (pl. AVG AntiRootkit) vagy akár egy keylogger - és igyekszik saját magát rejtett processzként, de legalábbis **minden futtatásnál random processnévvel létrehozni**, hogy a fix névlistákkal dolgozó programok dolgát ezzel is megnehezítse.

Majdnem minden vírusvédelmi programnak komoly erőfeszítései vannak, hogy saját állományaik sértetlenségét (nincs-e patchelve, fertőzve, kicserélve, letörölve, meghookolva, stb.) detektálni tudja, és **különböző technikákkal megakadályozza** az ilyen jellegű hibás működést. Ez régebben még zömmel csak az egyszerű CRC ellenőrző összeget jelentette, ma egyre inkább a digitális aláírással (de más módokon is) való ellenőrzés irányába mozdul el. Az úgynevezett retrovírusok egyébként pontosan a vírusvédelmi alkalmazások ismert nevű összetevőit támadják: **megkísérlik folyamataikat leállítani, moduljaikat fizikailag is törölni**, illetve újabban szokás még a hosts fájl mérgezésével a frissítési folyamatok meghiúsítása is. Egy klasszikus példa a retrovírus kategóriából a majd 8 éve megjelent Klez.

Itt a Stration AV ellenes ármánykodásait láthatjuk

E kis áttekintés végén **az alábbi retro klipekkel kívánunk minden kedves Olvasónknak bitekben gazdag, vírusokban pedig szegény Boldog Új Évet!**

Ajánlott bejegyzések:

- Kiberzaklatás - mit tehetünk ellene?
- Kártékony böngésző kiegészítők jönnek
- Akiknek a Captcha kínszenvedés
- 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/279919

Kommentek:

Nincsenek hozzászólások.