

Figyeljünk a mobiltárcánkra, a Bitcoinjainkra

2014.01.02. 11:12 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [interjú](#) [malware trend](#) [android](#) [2014 eset](#) [juraj malcho](#) [qrcode](#) [bitcoin](#)

Interjú Juraj Malchoval, az ESET vezető kutatási igazgatójával az aktuális biztonsági trendekről, várható támadásokról, bonyolult vírusokról, sebezhető Androidról és ellopható Bitcoinokról.



Manapság a számítógépes támadások egyre fejlettebbek, egyre összetettebbek. Hogy látja egy olyan szakember, aki az elmúlt tíz esztendőt hivatásszerűen vírusok elemzésével töltötte? Mennyire változtak meg a kártevők az utóbbi egy évtized alatt?

Határozott elmozdulást láthatunk a mobil eszközök irányába. Valóban egyre fejlettebbek, egyre összetettebbek a kártevők, így a mi biztonsági programunknak is hasonlóképpen komplexnek, széleskörű védelmet nyújtó megoldássá kellett válnia. Mivel a támadások és fenyegetések különféle irányokból érkehetnek, így mindenképpen egy többretegű védelemre van szükségünk. Egyetlen védelmi pont ellen könnyű támadást intézni, emiatt a vállalati rendszerek esetén igen fontos, hogy átfogóan gondolkodjunk, és mind a szerverekre, átjárókra, mind pedig a végpontokra megfelelő biztonsági programokat telepítsünk. **A pénzünket és az embereinket akarjuk megvédeni, erre kell tenni a hangsúlyt, mert nyilvánvalóan ezek azok az erővonalak, ahol a bűnözők is indítják a támadásaikat.** Annak a korai korszaknak ugyanis, melyben még hírnévre vágyva, vagy pusztán szórakozásból írták a vírusokat, egyszer és mindenkorra vége, jó ideje már az anyagi haszonszerzésé lett a terep.



Ha például azt vizsgáljuk, hogy a különféle sebezhetőségi vizsgálatoknál, vagy kísérleti támadások (úgynevezett PoC, Proof of Concept) megvalósításakor - ilyenkor a hackelések történhetnek akár csak úgy pusztán kíváncsiságból is - **sokszor tárnak fel olyan tervezési, illetve megvalósítási hibákat a különféle okos eszközökben, amely sebezhetőségek kihasználásával aztán később kártevő incidenseknél is találkozhatunk.** És azt is figyelembe kell venni, hogy ez már régen nem csak a számítógépeinkről és a telefonjainkról szól, hanem tulajdonképpen minden internetképes eszközt ideérthetünk, például mindez veszélyeztetheti az okos televíziókat, vagy akár az intelligens háziriasztókat is.



Láthattuk, hogy a támadók időnként az úgynevezett QR kódokat is célba veszik, hogyan történik ez pontosan?

Az utóbbi időben rengeteg helyen felbukkantak ezek a QR kódok - például az üzletekben a vásárlást, illetve az információ átadást segítő - illetve egyre több olyan okos telefonkészülék jelenik meg, amely már támogatja az NFC (Near Field Communication) technológiát, így természetesen színre léptek azok is, akik ezzel a helyzettel igyekeznek visszaélni. Itt nyilván az a helyzet tartogathatja a legtöbb veszélyt, amikor ez a kód beolvasás és a linkek meglátogatása alapértelmezetten nincs eseti engedélyhez kötve, magyarul nem pityeg és kéri a jóváhagyásunkat, hanem automatikusan lefut valami a háttérben. Ezért érdemes lehet ezt a beállítást ellenőrizni, és ha szükséges, akkor módosítani. Jó példa erre az Android platformon futó Google Earth vagy a Youtube alkalmazás, amelyek telepítésekor az NFC számára teljes körű internetelési engedélyt ("Control Near Field Communication: Full internet Access") kérnek. Mi úgy érezzük, ezek a bárki által szabadon használható QR kódok potenciális veszélyforrást jelentenek, ezért azt szoktuk tanácsolni, ha valaki ilyen technológiát szeretne igénybe venni, használat és terjesztés előtt alaposan tesztelje le a generált kódot.



Mi a helyzet a digitális pénztárcákkal, amelyben sokan a Bitcoinjaikat őrzik?

Mivel a mobiljukat sokan már bankolásra, pénzügyi műveletek végzésére is használják, így ez felkeltette a bűnözők érdeklődését. Bár a mobil kártevők száma a klasszikus vírusok számához mérten igen alacsony - itt jellemzően az Android a leginkább támadott mobilplatform - ám az itteni incidensek jelentősége magas, hiszen az áldozatok komoly veszteségeket szenvedhetnek el, többségében pénzt veszítenek. Számos olyan kártevő variáns ismert, amely a botnettel fertőzött gépek erőforrásait Bitcoin bányászatra használja. A modern trójai programok igyekeznek követni, kifürkészni a pénz útját, így természetesen a hagyományos banki adatok mellett a digitális pénztárcák is célkeresztbe kerültek. Ha bizonyos biztonsági tanácsokat megfogadunk, hatékonyabban vigyázhatunk a virtuális pénzünkre. Ha ugyanis a legrosszabb történik, és ellopják a tárcánkat, akkor a tolvaj vagy levásárolja, vagy pedig áttölti azt a saját virtuális tárcájába. Ha azonnal észrevesszük, elég gyorsan cselekszünk és szerencsénk is van, néha még sikerülhet ilyenkor is megmenteni a pénzünket. A legjobb tanács azonban az, ha a megelőzésre tesszük hangsúlyt, azaz naprakész vírusirtóval rendelkezünk, operációs rendszerünket és alkalmazói programjainkat a megjelenő biztonsági hibajavításokkal azonnal frissítjük, és persze az is fontos, hogy biztonság tudatosan ne kattintsunk figyelmen kívül mindenre. Tartsunk lehetőleg csak kisebb összeget Bitcoinban, illetve mindenképpen titkosítsuk alaposan a pénztárcánkat, ez is egy plusz akadályt jelenthet az esetleges támadók számára.



Tudna olyan támadást említeni, amelyikről bátran kijelenthetjük, ez volt az idei (2013-as) évben a leginnovatívabb?

Ami egyértelműen felgyorsult az elmúlt hónapokban, az a váltságdíj szedő kártevők, úgynevezett ransomware programok széleskörű jelenléte. Bár elterjedtségük alapján nem vezetnek a toplistát, ennek ellenére sokszor találkozhatunk velük, és valóban jelentős fenyegetést jelentenek. Az intenzívebb terjedésre magyarázatot adhat, hogy a CryptoLocker és hasonló kártevőket már a botnetek is terítik, a veszélyességét pedig igazából az jelenti, hogy ezek a zsaroló kártevők erős kulcsokat használva titkosítva felülírják az állományainkat, majd a feloldó kódért pénzt követelnek.

Az eredeti [angol nyelvű interjú szövege itt érhető el](#).

Megosztom

tumblr.

 Tweet

 Pin it

 +1

Ajánlott bejegyzések:

[Kártevő előrejelzés - Ez vár ránk 2015-ben](#)
[2014 az internetes adatvédelemről szól majd](#)
[A váltásdíjas titkosító kártevő visszatér](#)
[Mit tegyek, ha ellopják az androidos telefonomat?](#)
[Célkeresztben a telefontolvajok](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5721160>

Kommentek:

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

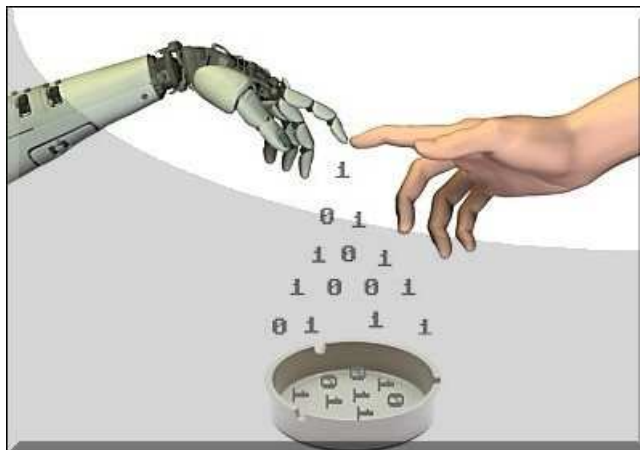
Nincsenek hozzászólások.

Android biztonsági tippek

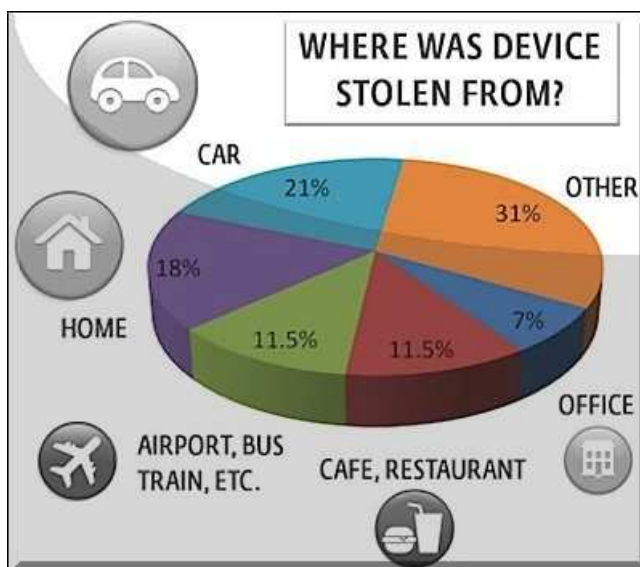
2014.01.06. 16:28 | [Csizmazia Darab István \[Rambo\]](#) | [4 komment](#)

Címkék: [biztonság](#) [security](#) [android](#) [kisokos](#) [microsd](#) [nfc](#) [remotewipe](#)

Ahogy azt az [év eleji jóslatokban is olvashattuk](#), 2014-ben várhatóan tovább növekszik a mobilos kártevők részesedése, ami az Android esetében már így sem volt alacsony. **A 2012-ről 2013-ig terjedő időszak alatt 63%-os emelkedést lehetett tapasztalni**, és nincs semmi jele sem annak, hogy ez váratlanul megállna. **Mit tegyünk a biztonságunkért, ha Androidos okostelefont rejt a zsebünk vagy a retikülünk?**



A kis kijelzős készüléken kisebb az esély, hogy észrevegyük, ha például böngészés közben valamilyen kártékony kód átirányít minket máshová, vagy valamilyen adatunkat egy rosszindulatú alkalmazás kényszerül továbbítja. **Az első, nulladik tanács lehetne az, hogy mindenképpen használjunk biztonsági programot**, az ESET Mobile Security program nem csak a vírusok, kártékony kódok távol tartásában segíthet, hanem a spamszűrést, SMS szűrést, valamint a lopásátlási funkciókat is tartalmaz.



A védelem első pontja mindenesetre a fizikai hozzáféréssel kapcsolatos. Honnan lopnak a leginkább? [A tapasztalatok szerint a legvalószínűbb helyszín a gépkocsi, ez vezet 21%-kal](#). Ne hagyjuk ott, tömegközlekedésen se, illetve **ha elővettük valahol: étteremben, reptéren, szállodában, tárgyaláson, mindig látótávolságban, kartávolságunkban maradjon**.



A mobil készüléken mindig legyen bekapcsolva a jelszavas védelem, és az időzár. Ez lehet ujjunkkal rajzolható minta vagy valódi

A következő pont adataink, alkalmazásaink védelme valamilyen programmal. Például az AppLock alkalmazás pontosan ezt teszi: a kiválasztott funkciók csak egy külön másik jelszó begépelése után aktiválhatóak, így **ezzel senki nem tudja megnézni a címjegyzékünket, kontónkra internetezni, hívást indítani vagy alkalmazásokat telepíteni**. És az sem lényegtelen, hogy a vicces kedvű kollégák sem tudják orvul a telefonunk nyelvét például koreaira vagy mandarin kínaira átállítani :-)



A legnagyobb érték nem az Android operációs rendszer, vagy a készülék, hanem a saját 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. Ha valóban ellopják a készüléket, két probléma merül fel: 1. elvesztjük, ami rajta volt 2. más kezébe kerülnek az adatok. **Mentés birtokában elég csak a 2-es pont miatt aggódni.** Általában az a jellemző, hogy a lopásra szakosodott bandák azonnal kiresetelik a telefont, hogy lebukás után ne maradjon bizonyíték, és használtan mihamarabb túladnak rajta.



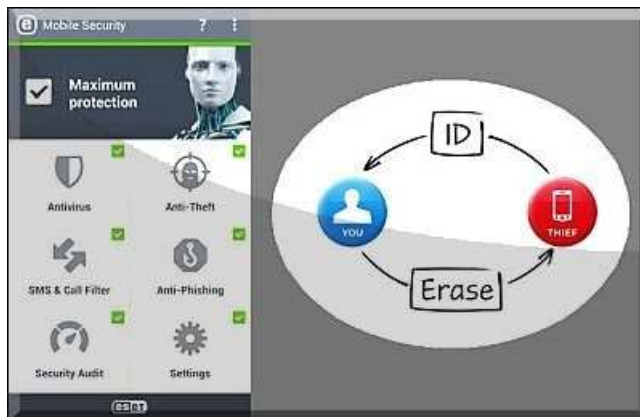
Sose felejtjük el, hogy míg egy asztali gépen esetleg pedánsan kijelentkezünk a Google accountunkkal, hogy a rendszer ne naplózza keresési előzményeinket, **addig a mobileszközöknél tulajdonképpen folyamatosan be vagyunk jelentkezve, így az ilyen típusú adatgyűjtések folyamatosan aktívak.** Emellett érdemes ésszerűen korlátozni a GPS adataink használatát, a nem használt funkciókat - pl. Bluetooth - pedig kikapcsolva tartani.



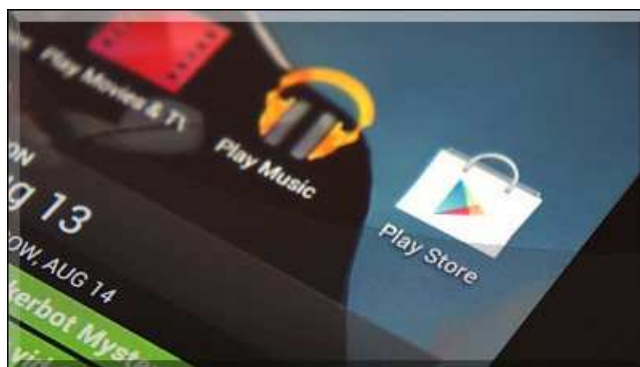
BYOD, azaz saját tulajdonú készülékünk munkahelyi használata esetén célszerű először főnökünkkel és az IT részleggel beszélni. **Ha engedélyezik, és már van erre a célra kialakított policy, akkor ezt kell majd betartanunk.** Adatszivárgási incidenseknél gyakori, hogy ha a céges levelezés egy része is a privát készüléken folyik, akkor annak elvesztése bizalmas vállalati titkok rossz kezekbe kerülését is okozhatja.



Ha már elveszett, ellopták, akkor is vannak teendőink. A **Google Android Device Manager** vagy az **ESET Mobile Security** segítségével felderíthetjük készülékünk földrajzi tartózkodási helyét, illetve szükség esetén távolról is törölhetjük adatainkat. Végül ha nincs más esély, akkor mihamarabb tiltassuk le a SIM kártyát és a telefon IMEEI száma alapján magát a készüléket is.



Bizalmas adatokat - pl. bankkártyánk vagy útlevelelünk beszkenelt fényképét, PIN kódunkat - ne tartsunk a külső microSD memóriakártyán. Ez nagyban megkönnyíti a tolvajok dolgát, ezért titkosítsuk az egész kártyát, vagy legalább az érzékeny dokumentumainkhoz használjunk olyan titkosító külső alkalmazást, mint például a Safe Notes.

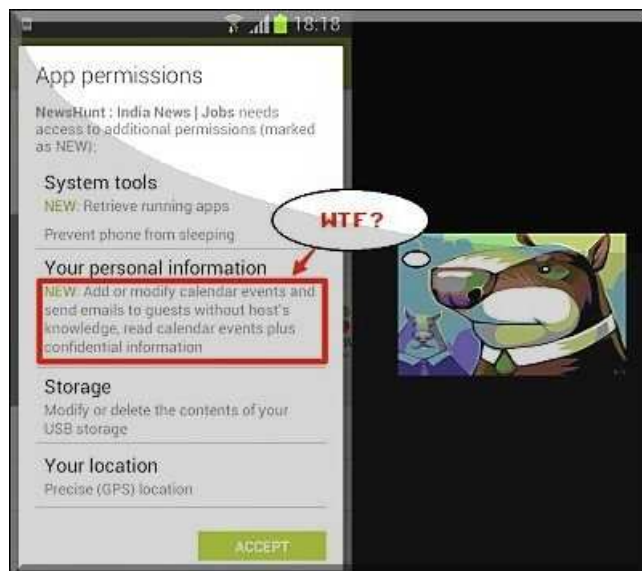


A trójai programok hihetetlen elterjedtsége is jól mutatja, hogy az ellenőrizetlen forrásból történő telepítések mekkora veszéllyel járnak. Lehetőség szerint csak a Google Play áruházból telepítsünk, ami persze korántsem tökéletes, de sokkal biztonságosabb, mint a kontroll nélküli bármilyen forrásból származó appok telepítése.



Sokan a telefon automatikus rootolásában látják a megoldás, és bár a fizetős alkalmazások ingyenes telepítésére, és többek közt tűzfal futtatására is mód nyílik ezzel, ám a kockázatok nem tűnnek el teljesen így sem. Sokak szerint egyfelől ilyenkor a telefon gyártó helyett a módosított operációs rendszer készítőjében vagyunk kénytelenek teljes mértékben megbízni, hiszen nem látunk bele, mit is csinál a szoftver pontosan. Másfelől pedig a magasabb, root jog miatt a lefutó kódok is nagyobb kárt képesek okozni, mintha meghagytuk volna az

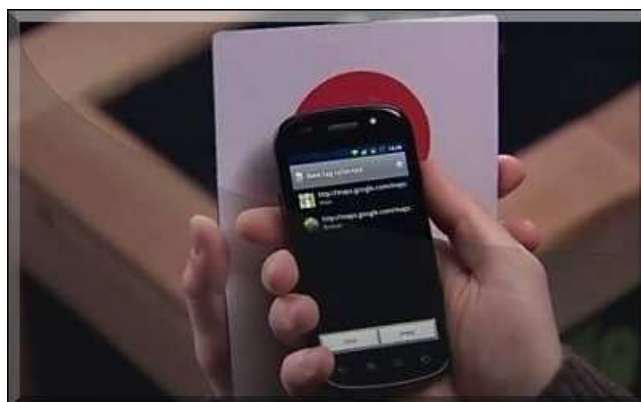
eredeti Androidos változatot. Volt olyan is, amikor az így letölthető ingyenes prediktív szövegbeviteli alkalmazásba például keyloggert csomagoltak a bűnözők.



Vegyük a fáradságot, és mindig 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 később borsos árú SMS küldés vagy egyéb "történet" van.



Soha ne telepítsünk banki alkalmazást kéretlenül kapott üzenet linkjéről. Világszerte egyre nagyobb gondot okoznak a hamis banki appok, amelyek vagy kikerülnek, vagy saját magukon is keresztül engedik a kétfaktoros ellenőrzési mechanizmust. Az egyre több trójai programból egyre több a pénzünket megszerezni akaró kártevő, legutóbb például a Hesperbot volt az, amelyik rosszindulatú linket küldött a felhasználóknak, és igyekezett rávenni őket az állítólagos banki alkalmazás telepítésére. **A bankok soha nem ajánlanak így alkalmazást, ezeket csak és kizárólag a Google Play áruházból telepítsük.**



Ha a telefonunkkal fizetünk, legyünk nagyon óvatosak. Chilében például már igénybe vehető a Near Field Communication fizetési mód. A biztonsági jelentések szerint a PoS, azaz Point of Sale terminálok is gyakorta célpontjai a bűnözőknek, de a 2014-es előrejelzésben azt is olvashatjuk, hogy **egy óvatlan NFC kommunikáció vagy egy Bitcoin QR kód is társulhat valamilyen kifinomult és célzott támadással**. Az érintéses fizetés mód egyre népszerűbb, így széleskörű elterjedésével a jövőben várhatóan egyre több támadási kísérletnek lehetünk majd tanúi.

 Tetszik 16 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Célkeresztben a telefontolvajok](#)
[Androidos engedélyek a szőnyeg szélén](#)
[Kártevő előrejelzés - Ez vár ránk 2015-ben](#)
[Beváltak-e a 2014-es jóslatok?](#)
[Mit tegyek, ha ellopják az androidos telefonomat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5739267>

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](#).



[boriska 2014.01.07. 14:28:15](#)

Ühüm. Elolvastam az alkalmazásengedélyeit az ESET Mobile security & antivirus alkalmazásnak és pont ezért nem merem telepíteni. Többek között aggályos nekem, hogy "... e- mailek küldése a vendégeknek a tulajdonosok tudomása nélkül..... Fiókok hozzáadása vagy eltávolítása,.... SD-kártya módosítása, vagy törlése...."

Kerestem, de mindegyik ilyen szolgáltatást nyújtó program hasonlóan fura. Megoldás?

Válasz erre



[Csizmazia Darab István \[Rambo\] • http://antivirus.blog.hu 2014.01.07. 15:12:37](#)

Szia Boriska!

Üdv a blogon :-). Elmondom, SZERINTEM mi a megoldás. A trójaik korában a szoftverek telepítése egyre inkább bizalmi kérdés. Melyik az a gyártó, aki hosszú távon rászolgált a bizalomra, számomra megfelelő minőséget produkál - ezt kell nézni. Ha megbízok az antivírusgyártómban, azt várom el, felelősséggel járnak el. Az ESET EMS-nél, de tulajdonképpen minden ilyen típusú szoftvernél ugyanúgy ott vannak ezek az engedélyek. Ha megnézzük, miket tesz, vagy tehet a szoftver: letörli, vagy karanténozza a kártevőt, lopás esetén engedi nekünk, hogy egy jelszóval távoli SMS-sel letöröljük a tolvajnál lévő telefont, vagy csak lekérdezzük a GPS koordinátákat - ezekhez pedig kellenek a felhatalmazások.

Ha egy Noname Coorporation vagy Gipsz II. Jakab által 128-ik dinnyeszeletelős játék koppítása kér hasonló engedélyeket, akkor persze igaz, ott azt nem érdemes akkor telepíteni. Viszont úgy látom, a security csomagoknál más a helyzet.

Válasz erre



[boriska 2014.01.08. 10:26:26](#)

Szia! Köszí a választ, meg is értettem, sőt, én is erre a következtetésre jutottam, de akkor is ijesztő. :D

Válasz erre

[kaskala 2014.01.14. 13:17:50](#)

Rambo

mi lehet az oka, hogy letöltöttem a programot, a telefonon jön egy üzenet, hogy sikerült, de sehol sem találom az appok között.

Samsung GT-19300

Válasz erre

Új Picasa képek az albumunkban. Vagy mégsem?

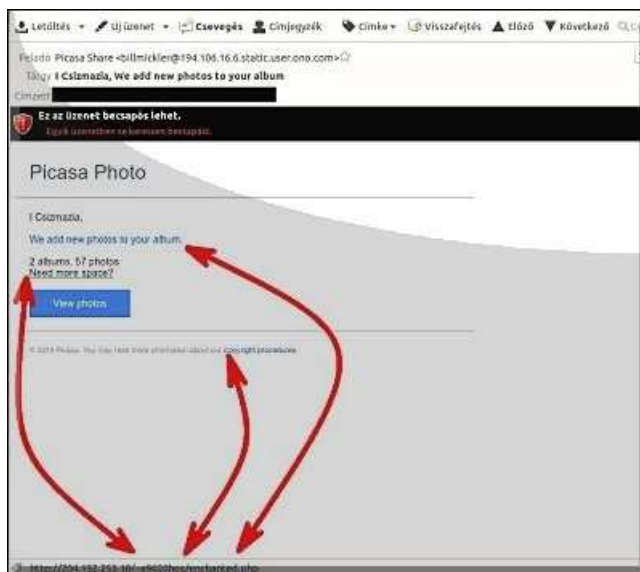
2014.01.09. 11:18 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [spam](#) [picasa](#) [kanadai](#) [vagy](#) [viagra](#) [mégsem](#) [gyógyszerész](#)

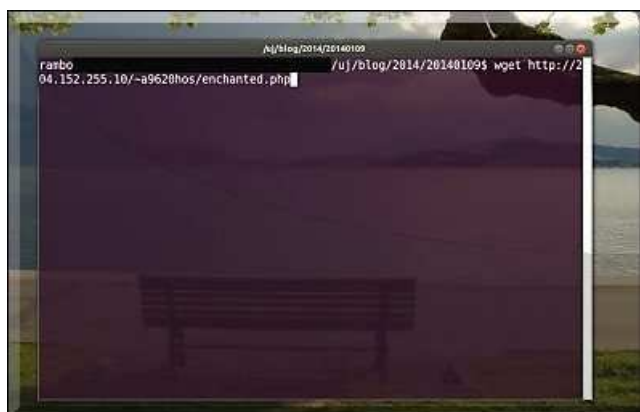
Vagy mégsem? rovatunk már a sokadik epizódját számlálja, volt itt Java frissítéstől kezdve, Microsoft Update-en át, Google Plus meghívó, iTunes számla, e-mail a Youtube-tól, írt nekünk a CERT [és LinkedIn meghívót is kaptunk már](#). 2014-ben is jelentkezőnk, ezúttal új képek érkeztek a Picasa albumunkba - még ha ilyenünk előtt egyáltalán nem is volt :-)



Ne feledjük, a fő lényeg mindenképpen az, hogy **kéretlenül jövő e-mail mellékletre vagy felkínált linkjére nem kattintunk**, hiszen bármi lehet benne. A vezér gondolat mellett **sokat segít még a levelező programunk figyelmeztető jelzése is**: "Figyelem, ez az üzenet becsapós lehet.". Végül pedig a szemre eredetinek látszó Facebook, DHL, LinkedIn és egyéb hivatalos levelek kinézetét **koppintó üzeneteknél ugyancsak hatásos kattintás helyett a linkek fölé vinni az egérmutatót, és mosolyogva "Nice try" motyogása közben elolvasni a valódi URL hivatkozást**.

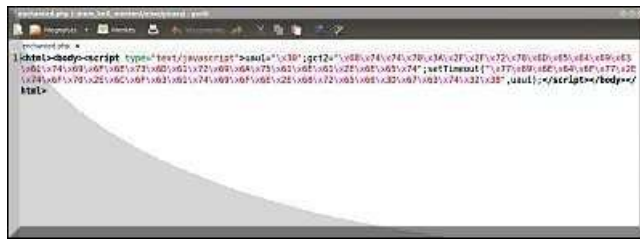


A ma hajnalban érkező levél látszólag arról tájékoztat bennünket, hogy új képek érkeztek a Picasa albumunkba. A fenti okosságok tudatában mosolyogva ugrik elő a szokványos Picasa "picasaweb.google.com" oldal helyett a "hxxp://204.152.255.10/~a9620hos/enchanted.php" link.

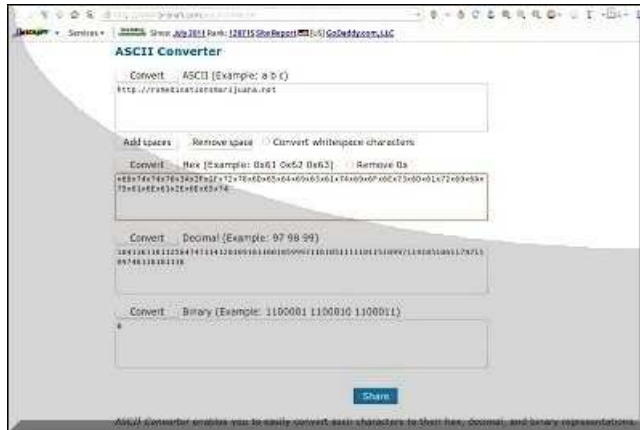


Ha ezt gyorsan le wget-eliük, élénk táru az alábbi kép. **Fatengelyes, primitív uuencode kódolás**, de vegyük most a fáradságot, és

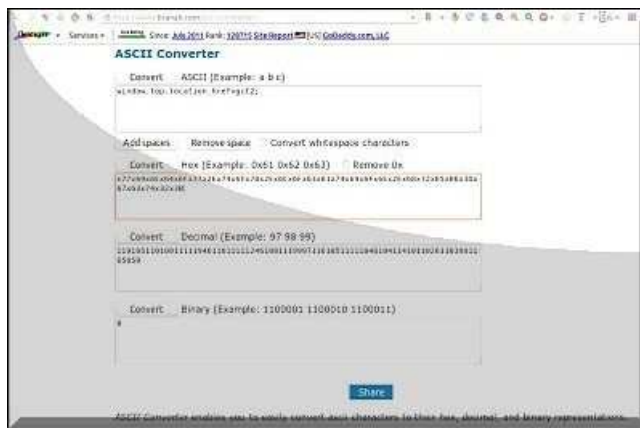
mutassuk be lépésről lépésre, hogy fejtsük vissza.



Válasszunk valamilyen **praktikus online kódkonvertert**, [például a Branah oldalt](#), és egyszerűen másoljuk be zagyva részt. Ha előtte lecseréljük a "\" karaktert semmire, akkor folyamatosan is olvashatóvá válik a link.



A másik kód pedig azt mutatja meg, **hogyan nyitná meg a JavaScript kód a mellékelt rejtett hivatkozást**.



Ha pedig mindez **visszahelyettesítjük**, megmutatkozik az összezavarás előtti olvasható állapot.



Az eredeti "204.152.255.10" domain fő oldala **látszólag egy USA-beli parkolás alatt lévő webhely**.



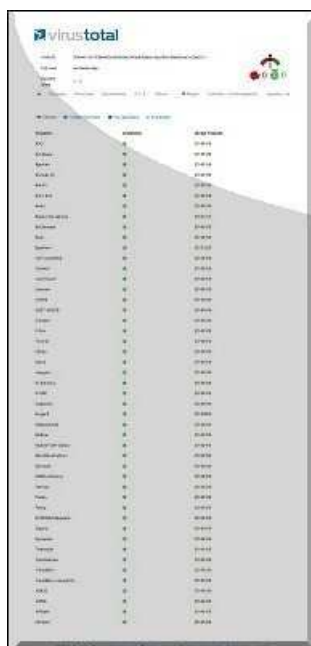
Maga az összezavarással elfedett, és átirányításra kerülő domain pedig egy elég **friss bejegyzésű oldal** [a DomainTools tanúsága szerint](#).



Viagra, Cialis, Levitra és egyéb áhított termékek, jutányos áron. Általános tapasztalat egyébként, hogy a napi átlagos spamtermés jelentős része végződik valamilyen kanadai gyógyszerész oldalra mutató webhellyen.



Nilvánvalóan mivel itt az **átírányítás nem kártevős oldalra mutatott**, nem is kapunk a PHP fájlra semmilyen riasztást a VirusTotalban.



Végül kukkantsunk rá arra, honnan érkezhett a levél, amelyet feladója szerint a "billmickler@194.106.16.6.static.user.ono.com" címről kaptunk.



A [Whatismyipaddress oldal segítségével](#) lehet kicsit kutakodni, ehhez a levél forrásából kimásoljuk a fejléc részt, bekopipasztázzuk az **oldalba**, majd azonnal olvasható is lesz a valószínűsíthető útvonal, esetünkben ez egy madridi cím.



Összegezve: ha el akarjuk kerülni, hogy [különféle linkekre kattintva állandóan egy hamis gyógyszerész oldalon](#), kitöltendő űrlapok mellett vagy kártevővel fertőzött webhelyeken kössünk ki, **kezeljük óvatosan a kéretlen leveleket: olvasás előtt óvatosan töröljük ki őket ;-)**

Tetszik 4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

[Instagram üzenet. Vagy mégsem?](#)
[LinkedIn meghívó. Vagy mégsem?](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Átverés a Google spam](#)
[Telekom számla vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5748530>

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](#).



BonFire 2014.09.08. 13:59:20

A minap kaptam egy olyan e-malit, hogy „Ön a következő képeket osztotta meg a [kepfeltoltes.hu](#) oldalon. [LINK](#) a képekhez...

Akár még igazi is lehetett volna; gondolkodóba az ejtett, hogy még életemben nem töltöttem fel képet a nevezett oldalra, így vagy tévedés, vagy csalás történt, és megpróbál rávenni, hogy kattintsak a linke, ami alatt ki tudja, mi rejlik.

Csak óvatosan!
Válasz erre

Óvakodjunk a trójai programoktól

2014.01.10. 10:07 | [Csizmazia Darab István \[Rambo\]](#) | [2 komment](#)

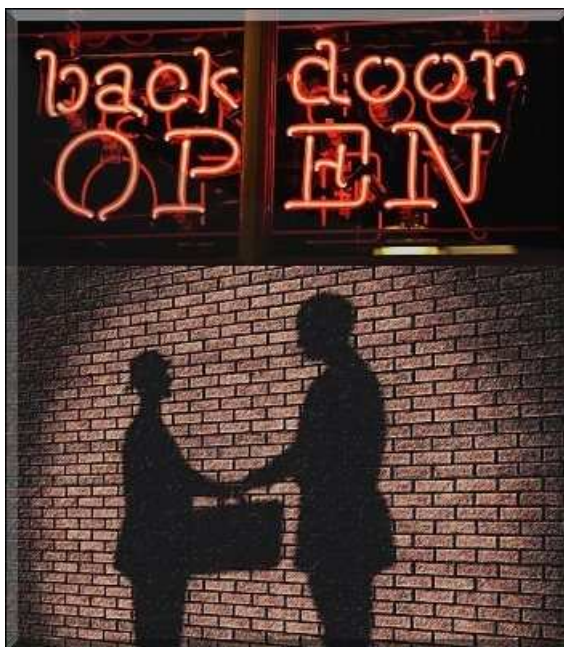
Címkék: [statisztika](#) [radar](#) [december](#) [adatok](#) [nod32](#) [havi](#) [report](#) [threat](#) [vírusstatisztika](#) [2013.](#)

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



A lista első felében az év végén sem történt változás az előző hónaphoz képest, **így ismét az a Win32/Bundpil féreg vezeti a mezőnyt, amelyik külső adathordozókon terjedve valódi károkozásra is képes**, hiszen a meghajtóinkról mind a futtatható, mind pedig a mentési Backup állományainkat törölheti. Ismét erősödött a Conficker féreg, ezúttal a hatodik helyet foglalja el, és két hónap szünet után újra a Top tízben találjuk a Win32/Virut férget. Ez rejtett hátsó ajtót nyit a gépen, a fertőzés után kapcsolatba lép távoli vezérlő szerverekkel, ezzel a támadók teljes mértékben átvehetik a számítógép felügyeletét.

Új résztvevővel is találkozhatunk, még pedig a kilencedik pozícióban szereplő Win32/TrojanDownloader.Wauchos személyében. Ez egy olyan trójai program, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. **Hátsó ajtót nyit a megtámadott rendszeren, melyen keresztül parancsokat fogad**, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetősége.

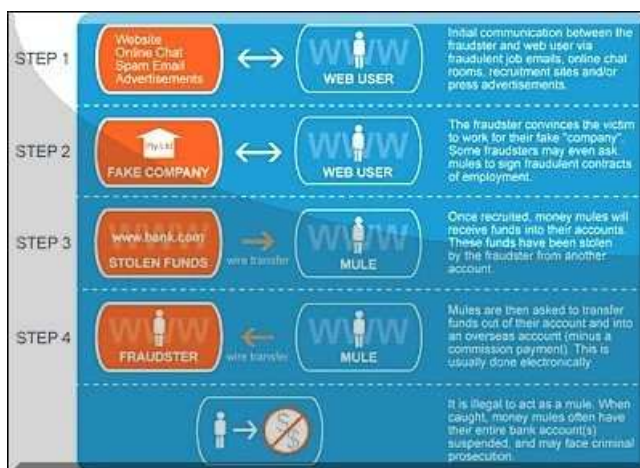


Az ESET Threat Radar Report e havi kiadásában az ilyenkor szokásos év végi összefoglaló mellett szó esett egy olyan átverésről is, amelynél cégek olyan spameket kapnak, miszerint egy állítólagos kínai domain registrar a mi vállalatunk nevét tartalmazó .asia alatti bejegyzési kérelmet kaptak. A levél írója jóváhagyást kér tőlünk, ehhez pedig a mellékelt kártékony linkre kellene kattintani, vagy a csatolt mellékletet kellene lefuttatni. Érdemes tisztában lenni a módszerrel, és óvatosnak lenni. Az ismeretlen feladóktól érkező kéretlen levelek linkjeire, mellékleteire pedig sosem szabad kattintani.



Ezenkívül számtalan csalás, adathalászati kísérlet is említésre kerül, ám a legnagyobb hangsúlyt ezúttal a pénzek tisztára mosásával kapcsolatos úgynevezett öszvér (mule) átverés kapta. A bűnözők - akik megvásárolják vagy csak bérlik a botneteket - a lopott banki adatok segítségével úgy szerzik meg a számlákról a pénzt, hogy hamis álláshirdetésekből balekokat toboroznak.

Általában jól fizető könnyű otthoni munkavégzést ígérnek, és az áldozatok látszólag "pénzügyi asszisztens" vagy "pénzügyi igazgató" álláslehetőségekre jelentkeznek, ám valódi feladatuk a saját bankszámlájukra érkező összegek továbbutalása, aminek fejében egy csekély százalékot megtarthatnak. Nem árt azonban tisztában lenni azzal, hogy a tudtukon kívül csalinak használt "munkavállalók" akár tíz évet is kaphatnak pénzmosásban való részvétel miatt.



Decemberi fontosabb blogposztjaink között többek közt beszámoltunk arról, hogy **nem kell ahhoz James Bondnak lenni, hogy olyan titkaink legyenek, amiket nem akarunk mindenkivel megosztani**. Egy pár érdekes dologról írtunk [a titkosítással kapcsolatban, mindezt néhány praktikus jó tanáccsal](#) is kiegészítve.



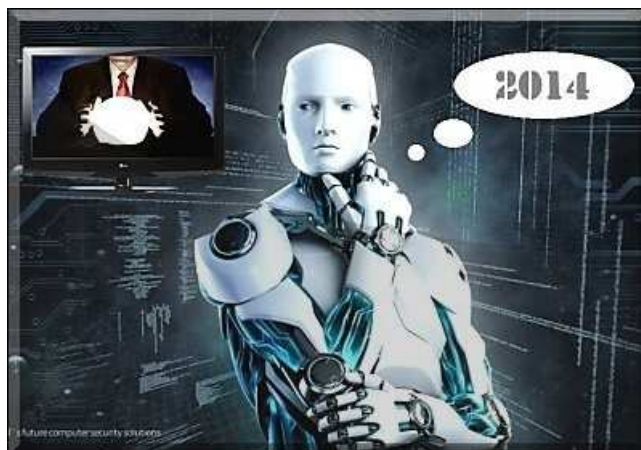
Az ünnepek előtt ismét egybegyűjtöttük [a biztonságos internetes vásárlással kapcsolatos aktuális tudnivalókat](#). A mellékelt 12 pontban minden olyan lényeges dolog szerepel, amire érdemes figyelni, vigyázni a karácsonyi ajándékok beszerzésénél, illetve mindenfajta internetes vásárláskor.



A botnetek is nagy erővel terjesztik azt a Bitlocker nevezetű zsaroló programot, amely a merevlemezünk, illetve adataink - ezúttal már 2048 bites RSA kulccsal történő - elkódolásával fenyeget bennünket. [Összefoglalásképpen, csokorba gyűjtöttük a védekezéshez szükséges legfontosabb tudnivalókat](#).



Az ESET idén is összeállította a káros fenyegetésekkel foglalkozó éves előrejelzését, ebből pedig az derül ki, hogy [2014-ben a szokásos fenyegetések mellett - Edward Snowden nyomán - a felhasználók online adatvédelme lesz](#) az egyik elsődleges fókusztema.

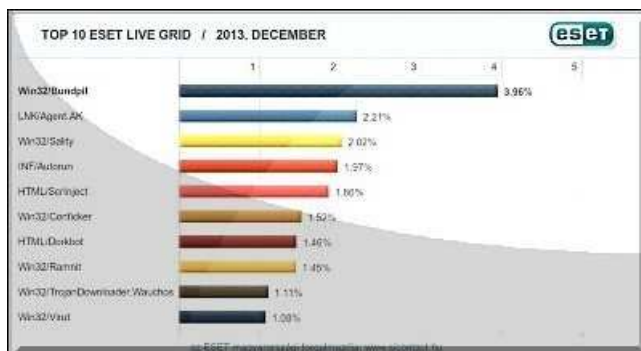


Akit pedig az is érdekel, hogy [mit jósoltunk még 2013. elején arról, hogy milyen vírusok várhatók majd az idén](#), annak érdemes lehet elolvasni az erről szóló értékelésünket. [Ebből kiderül, vajon mennyiben váltak be ezek](#), illetve megtudhatjuk azt is, hogy összességében milyen évet zártunk a kártevők, átverések, támadások szempontjából.



Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2013. decemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 18.64%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtevesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.



1. Win32/Bundpil féreg

Elterjedtsége a decemberi fertőzések között: 3.96%

Működés: A Win32/Bundpil fűrés hordozható külső adathordozókra 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.



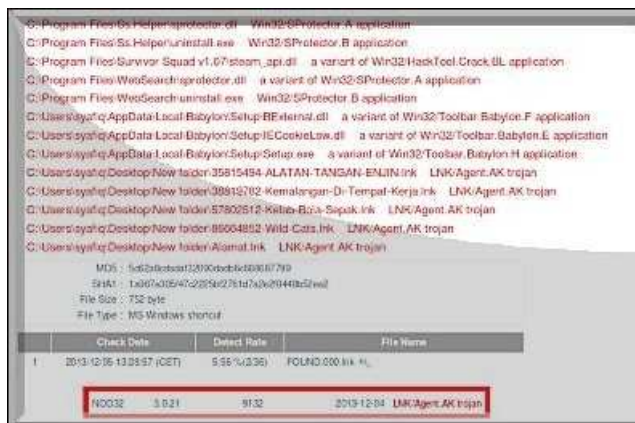
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



2. LNK/Agent trójai

Elterjedtsége a decemberi fertőzések között: 2.21%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokot 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. Vírusselemlzők 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 decemberi fertőzések között: 2.02%

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 megkísérel lekapsolni a védelmi programokhoz tartozó szerviz folyamatokat.

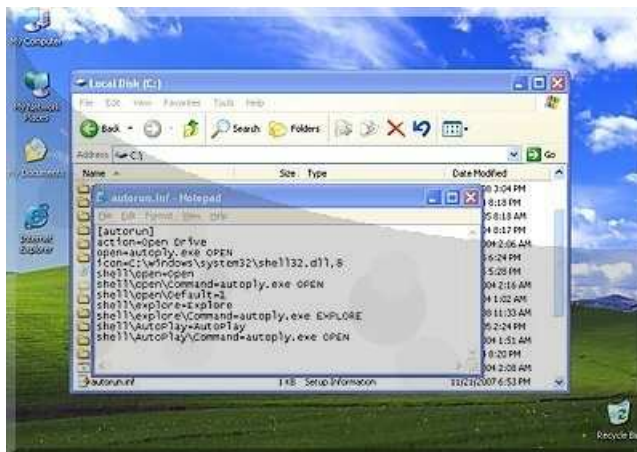


Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description

4. INF/Autorun vírus

Elterjedtsége a decemberi fertőzések között: 1.97%

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



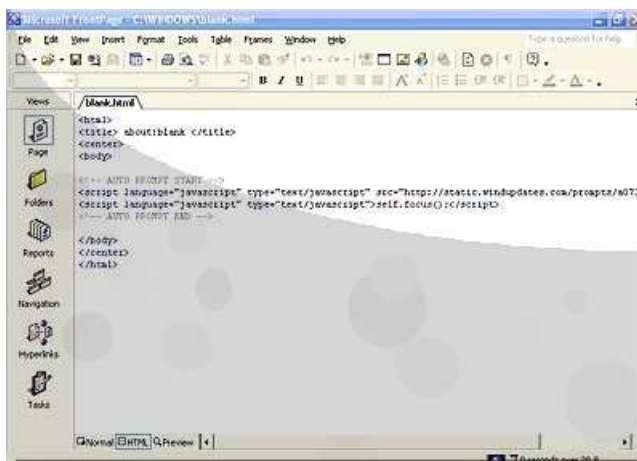
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>



5. HTML/ScrInject trójai

Elterjedtsége a decemberi fertőzések között: 1.86%

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/Conficker féreg

Elterjedtsége a decemberi fertőzések között: 1.52%

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 eljárásán 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.

9. Win32/TrojanDownloader.Wauchos trójai

Elterjedtsége a decemberi fertőzések között: 1.11%

Működés: A Win32/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Különböző registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor lefusson a kódja. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.

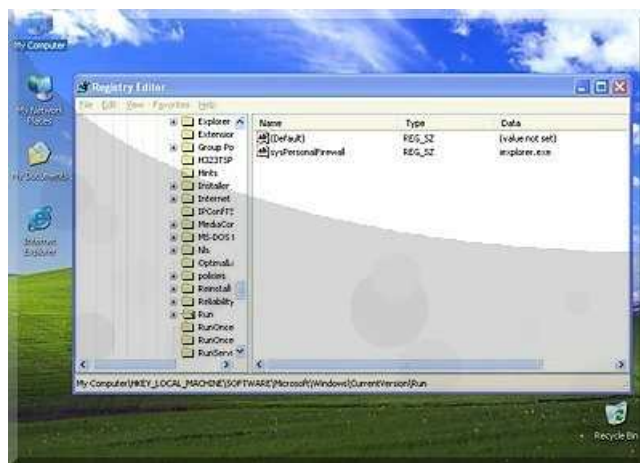


Bővebb információ: http://www.virusradar.com/Win32_TrojanDownloader.Wauchos.A/description

10. Win32/Virut féreg

Elterjedtsége a decemberi fertőzések között: 1.08%

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% alkönyvtárba iexplore.exe néven, majd különböző 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 5 személy kedveli ezt Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)
[Megtévesztések és álhírek terepe a Facebook](#)
[Virusstoplista 2015. január hónap](#)
[A HTML trójaiak riogattak minket októberben](#)
[Végre kiesett a Conficker féreg](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5747530>

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](#).

rolls 2014.01.11. 12:28:06

Azért kattintás közben elbizonytalanodtam egy pillanatra, - de még működik a vas.

:)))

Köszönöm az infókat.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> 2014.02.02. 21:00:38

[@Tomi1977](#): Szia Tomi

Koszi szépen a kommentet, érdekes az oldal, nem emlekeztem rá, hasznos.

Az emberiség másik fele nevében viszont lekapcsoltam a kommentedét, nehogy a link másiknak bajt okozzon.

Meg egyszer koszi :-)

Válasz erre

Androidos engedélyek a szőnyeg szélén

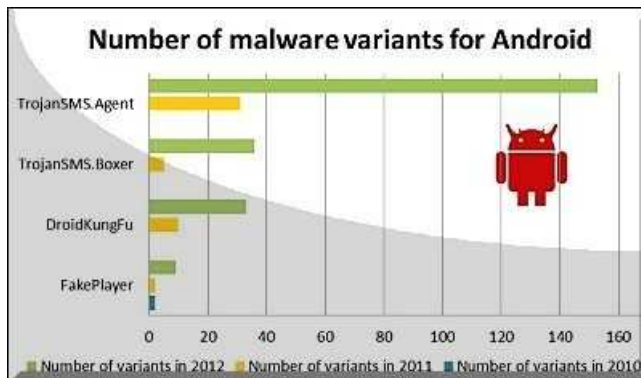
2014.01.13. 15:52 | [Csizmazia Darab István \[Rambo\]](#) | [8 komment](#)

Címkék: [biztonság](#) [mobile security](#) [android app](#) [eset](#) [ems](#) [engedélyek](#) [ops](#) [snoopwall](#)

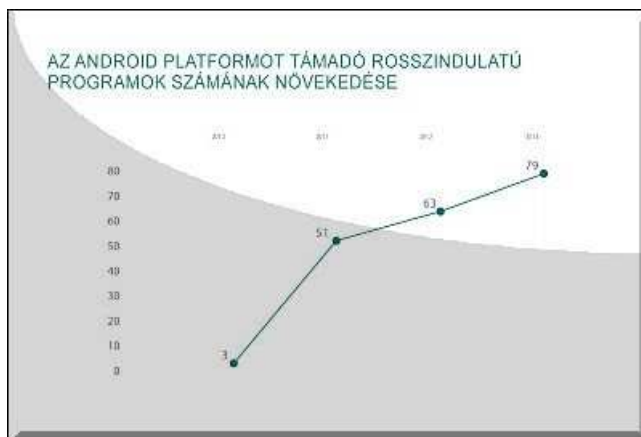
Többször is emlegetjük az Android biztonságát, és nem azért, mert nem szeretjük. A nyíltságnak - ami azért nem a teljes forrás kód nyitottságában mutatkozik meg ;-) - előnyei és hátrányai is vannak, és láthatóan igaznak bizonyultak az előrejelzések az Androidos kártevők, átverések, incidensek tekintetében, hogy [a régi Windowshoz hasonlóan ez lesz-lett az Új Vadnyugat](#). Minden antivírus cég [két számjegyű növekedésről számol be a 2013-as évben](#). Az hogy egy programot [honnan telepítünk, mikre kér engedélyt, és hogy megnézzük-e egyáltalán, hogy mikre kér](#), nagyon is fontos kérdés.



A [2014-s jóslatok is foglalkoznak az Androidos veszélyekkel](#), és nem árt tudni, hogy az ide készült internetbiztonsági csomagok már jóval több dolgot tesznek, mint egy sima antivírus: spamszűrők is egyben, lopásgátló funkciókkal is rendelkeznek, és hasonlók. A kártékony alkalmazásokkal kapcsolatosan folyamatos hangsúlyozni szoktuk, hogy mindig vegyük a fáradságot, 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, gondolkodjunk, vagy akár inkább álljunk el az installtól, és keressünk másik alternatívát.



Igen sok esetben ugyanis a felhasználó figyelmetlenül maga engedélyezi a számára kártékony funkcionalitásokat, és akkor nincs miért csodálkoznia, ha aztán borsos árú SMS küldés vagy egyéb nemkívánatos jelenség van. A fejlesztők lustaságból igen gyakran mindenfajta engedély kérést benne hagynak akkor is, ha a kódnak valójában nincs is rá szüksége, de a kártékony kódok, vagy az úgynevezett freemium játékok is gyakran lopják el a személyes adatokat, eladva azokat hirdetőknak, és nem mellesleg keményen rátenyerelve a hasznos hálózati sáv szélességünkre.

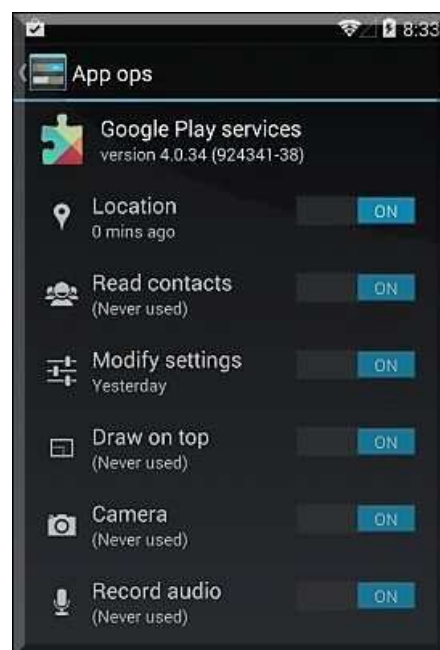


Most egy SnoopWall Privacy Firewall nevű alkalmazás megjelenésével [ismét terítékre került a túlbujázó engedélyekkel kapcsolatos probléma](#) a TheRegister hasábjain. Ez az új eszközkezelőként beépülő program képes arra, hogy folyamatos ellenőrzés alatt

tartsa az engedélyeket, beleértve az olyan adatvédelmi, biztonsági szempontból kényeseket, mint a mikrofonunk távoli használata, a kameránk távoli ki-be kapcsolása, GPS pozíciónk és WiFi adataink továbbítása, SD adathordozónk írása, olvasása, formázása, címjegyzékünk harmadik féllel való megosztása, emelt díjas számok értesítés nélküli hívása, stb.



Megemlítik emellett azt az App Ops nevű korábbi hasonló alkalmazást - ami egyébként a klasszikus tűzfalakhoz hasonlóan rootolást igényelt - amely 4.3 és 4.4 alatt volt képes figyelni a meglévő, és változó engedélyeket, és még ki-be is engedte kapcsolni ezeket a jogosítványokat. A dolog pikantériája, hogy a korábban sokak - többek közt az EFF, Electronic Frontier Foundation - szimpátiáját is elnyerő igen hasznos feature-t [a Google egy későbbi 4.4.2 frissítéssel váratlanul visszavonta](#), és mindezt azzal magyarázta, hogy csak valamilyen tévedés miatt került bele korábban ez a kísérleti funkció.



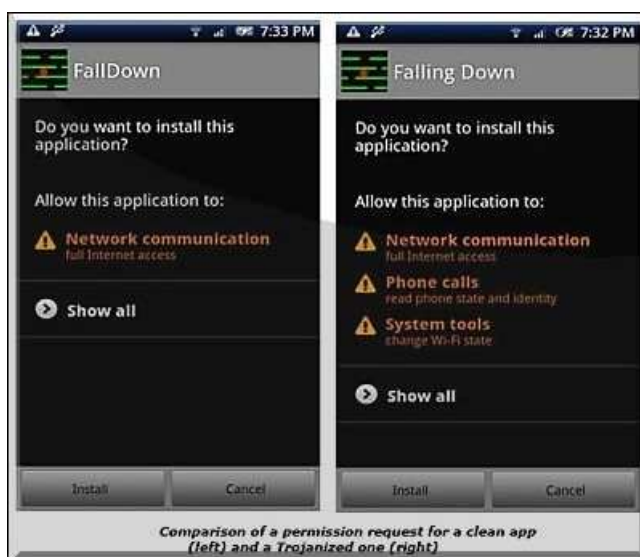
De nincs okvetlenül szükség külön alkalmazásra ehhez, nézzük meg például, mit nyerünk azzal, ha már eleve egy androidos biztonsági csomagot használunk. Ahogy említettük, ez már régen nem csak Symbianos időkől ismert pusztán egyelővetű antivírus, hanem rengeteg extra funkciót is tartalmaz. A teljesség igényével ezek a következők: valós idejű vírusvédelem, kéretlen alkalmazások keresése, heurisztikus védelem, ütemezhető ellenőrzés, SMS spam szűrés, MMS szűrés, hívásblokkolás, lopásgátló táv-lezárás, táv-törlés, eltávolítás védelem, SIM kártya azonosítás, GPS nyomkövetés, biztonsági diagnosztikai vizsgálat, és akkor ami miatt mindezeket felsoroltuk: a telepített alkalmazások auditálása.



Magyarán itt is rendelkezünk valamennyi kontrollal, például [az ESET Mobile Security programban a biztonsági audit menüpont alatt tudjuk a telepített alkalmazások engedélyeit \(monitors installed apps permission\) figyelemmel kísérni](#). Végezetül azt is érdemes azért megjegyezni, hogy azon túl, hogy valóban nem mindegy, hogy egy programot honnan telepítünk, meg hogy mikre kér engedélyt, a trójaik korában a szoftverek telepítése egyre inkább bizalmi kérdés. Melyik az a gyártó, aki hosszú távon rászolgált a bizalmunkra, ki az aki számunkra megfelelő minőséget produkál - ezt kell nézni.



Ha megbízunk az antivírusgyártóban, azt várjuk el, hogy felelősséggel járnak el. Az ESET EMS-nél, de tulajdonképpen **minden** ilyen típusú védelmi szoftvernél ugyanúgy ott vannak ezek a kért kényes engedélyek, ami sokaknak elsőre esetleg ijesztő lehet. Ha azonban megnézzük azt is, miket tesz, vagy tehet a szoftver: letörölheti, vagy karanténoshatja a kártevőt, lopás esetén engedi nekünk, hogy egy jelszóval távoli SMS-sel letöröljük a tolvajnál lévő telefont, vagy csak lekérdezzük a lopott készülék GPS koordinátáját - akkor világossá válik, ezekhez kellenek a szükséges felhatalmazások.



Természetesen az is igaz, ha egy Noname Corporation vagy Gipsz II. Jakab által írt 128-ik dinnyeszeletelő játék koppintása kér hasonló, feleslegesnek és a program szempontjából indokolatlanul tűnő engedélyeket, akkor persze nem szabad ezt engedélyezni, és nem érdemes telepíteni. Visszatérve az App Ops-ra, **magunk részéről éppen az ilyesfajta, az operációs rendszer által tartalmazott és részletesen szabályozott beállítási lehetőségeket tartanánk jónak és hiányoljuk most.**



A legszuperebb az lenne, ha még fel is telepítettünk ilyen engedély halmozó appot, az "akcióknál" jönne a választási lehetőség: "engedjem neki", vagy "tiltsam neki", és emellett a "csak most egyszer" vagy "mostantól mindig" opcióval kiegészítve. De az appoknak ettől függetlenül természetesen működni kellene, akár azon az áron is, hogy fusson homokozóban az SMS küldés, vagy kapjon valami letárolt kamu adatot: pl. GPS koordinátának Bázakerettyét esetleg Los Angeles Alsót - kb. ugyanezt teszi most a TMN, azaz TrackMeNot böngészőkiegészítő is a hamis referer megadásokkal. Most viszont App Ops mentesen, Android által gyárilag tartalmazott lehetőségek nélkül kb. egymilliárd felhasználó szív ennek hiánya miatt.

 Tetszik 21 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Célkeresztben a telefontolvajok](#)

[Mit tegyek, ha ellopták az androidos telefonomat?](#)
[Megjelent a Google Play-en az ESET for Android](#)
[ESET védelem Androidra](#)
[Béták reggelire II.](#)



Hirdetés

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/5756423>

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](#).

[Shopping 2014.01.14. 11:37:41](#)

sztem ma már az ÖSSZES app mindenre engedélyt kér.
ha nem adod meg nem települ... :(
Válasz erre

[biododírium 2014.01.14. 13:22:52](#)

Kik határozzák meg azt, hogy egy app mire kérjen engedélyt?
Az app tulaja vagy a google is beleszólhat?
Régebben próbáltam csak teszt jelleggel pl az IWIW-et. Ott is benne volt, hogy bármikor csinálhat fényképeket a teló kamerájával a tudtom nélkül.
Mire föl? Kinek fontos ez a lehetőség és miért?
Válasz erre

[Warlimont 2014.01.14. 14:11:08](#)

@Shopping: Ha egy elemlempa app engedélyt ker a személyes adataidhoz meg GPS pozícióhoz, akkor azért kuldd a pixaba... :)
Szamomra a nagyobb kerdes inkabb az, hogy mi van, ha nem is ker az app engedelyt, csak ugy hozzafer a dolgokhoz...
Válasz erre



[Csizmazia Darab István \[Rambo\] • http://antivirus.blog.hu](#) [2014.01.14. 15:24:05](#)

Szia Shopping!

Vannak azért permission friendly alkalmazások is, amelyek vagy semilyet nem kérnek, vagy csak azt, amire tényleg szükség van. Ha mindegyiknél ez lenne a helyzet, akkor nem is lenne gond. Ez a feljesztő sara, a Google nem kéri tőle, hogy tegyen bele minél többet, nem jár érte mennyiségi bónusz ;-)

Válasz erre



[Csizmazia Darab István \[Rambo\]](http://antivirus.blog.hu) • <http://antivirus.blog.hu> 2014.01.14. 15:30:36

Hali biododírium!

Ha az ember utánéz, hogy az app miket tehet, nagyjából ki lehet következtetni, sok-e vagy kevés az engedély. És persze embere is válogatja, én például egy Facebook appot sosem használnék telefonról, míg másoknak ez természetes.

Egyetértek Warlimonttal, ha ordít róla, hogy feleslegesen látszó dolgokat akar, hagyni kell és keresni másik alkalmazást.

Egyébként nyilván ez az engedélyezősdi sok mindenről tehet, de azt is nézni kell, ha telepítéskor még nem akart semmit, bármelyik frissítéskor behúzhat új engedélyeket, amikre a Next-next-finish-hez szokott felhasználók egyetértenek.

Fejlesztők szerint egyébként ha valaki nagyon ért hozzá, úgy is lehet dolgokat csinálni, hogy nulla engedélyt kér látszólag.

Válasz erre



[Csiken Disztroly](http://youtu.be/ipFHAAR8H-A) • <http://youtu.be/ipFHAAR8H-A> 2014.01.14. 15:35:10

Az "android biztonsága"-kifejezés egy oximoron.

Válasz erre



[Csizmazia Darab István \[Rambo\]](http://antivirus.blog.hu) • <http://antivirus.blog.hu> 2014.01.14. 15:37:07

Jó ötletnek tartanám amit a cikkben is írtam: az App Ops szerű teljeskörű engedély menedzsment, alaphangon biztosított feature, ami szerintem az OS fejlesztőjének lenne a feladata, hogy ne mondjam kutyakötelessége ;-)

Az sem lenne utolsó, ha engedélyek alapján lehetne keresni a Google Playen, ha jól láttam, nincs még ilyesmi.

Válasz erre



[twollah / bRoKE n hOPe, sUppLeX](http://freewaresoftwarenews.blogspot.com/) • <http://freewaresoftwarenews.blogspot.com/> 2014.01.14. 15:51:57

A legegyszerűbb megoldás ha nem telepítünk minden szart a telefonra.

A fíngos, bofogos, WiFi, mobilinternet gyorsítás, ingyen SMS kuldo, ujjlenyomat olvasos, vetkoztetos, falon atlato kamera programok mar eleve gyanusak.

Erdemes továbbá:

- azokat a programokat feltenni amit sokan használnak.
- el kell olvasni a kommenteket, hogy masok milyen velemenyen vannak a programrol.
- kerulni kell a tort programokat, sose lehet tudni, hogy mikor rak bele valaki valami meglepetest.

Ha erdekel egy program akkor vegyuk meg es ezzel a fejlesztot tamogatjuk.

Ha megse tetszik akkor sincs veszve semmi, 15 percen belül visszakerhetjuk a penzunk.

Erdemes feltenni az AppSales programot, az akcios appokrol ertesit minket.

En igy szoktam bevasarolni.

Pl.: a 15 dollaros OfficeSuite Pro 7-et 99 centert vettem meg.

Es meg sorolhatnam tovaab a jo vetelnek tuno programokat amiket igy vettem meg.

Válasz erre

Vigyázatlanok vagyunk a neten

2014.01.15. 11:52 | [Csizmazia Darab István \[Rambo\]](#) | [9 komment](#)

Címkék: [kampány](#) [biztonság](#) [internet védelem](#) [biztonságtudatosság](#) [Cyber Streetwise](#)

Egy friss felmérés eredményei azt mutatják, nem igazán teszünk meg minden tőlünk telhetőt azért, hogy óvjuk a biztonságunkat. A több, mint 22 ezer felhasználó megkérdezéséből született tanulmány szerint például a netezők több, mint fele nem telepít antivírust a gépére. A brit kormányzat most szeretne ezen javítani, és egy oktatási kampánnyal jelentkezett.



A hagyományos PC környezetben 22.672 fogyasztó közül csupán 44%-uk mondta azt, hogy rendelkezik biztonsági szoftverrel, és emellett rendszeresen telepíti is a megjelenő Windows és egyéb operációs rendszerekhez tartozó biztonsági frissítéseket, hibajavító foltokat. Pedig köztudottan a biztonság ebből a három területből állhatna össze: védelmi szoftverek, rendszeres hibajavító frissítések és biztonság tudatos viselkedés. Ezek csak és kizárólag együttesen nyújthatnak megfelelő védelmet, hiába az antivírus, ha közben lyukas az operációs rendszer, vagy ha valaki mindenre kattint, mindent telepít, ami csak jön és mozog.



Ennél is rosszabb azonban a helyzet a mobilrendszerek világában. Hasonló felvetésre ugyanis ott ugyanez az arány csak mintegy fele, egész pontosan 21%, azaz itt már tízből csak ketten használnak valamilyen biztonsági szoftvert, és tartják közben frissen a rendszerüket. Emellett hasonló arányban, az emberek ötöde nincs tisztában a lehetséges fenyegető kockázatokkal, [míg 32%-uk azt sem érti, egyáltalán mire is jó egyáltalán egy internetbiztonsági szoftver.](#)



A számítógépes bűnözők elleni harc nem nyerhető meg pusztán technikai eszközökkel, és törvényekkel, muszáj a biztonságtudatosság, oktatás területén is folyamatosan megjeleníteni. Életünk, munkakörülményeink teljességgel megváltoztak a korábbi évekhez képest, és ebben mindenkinek: magánembereknek, munkavállalóknak, kis vállalkozásoknak egyaránt muszáj beletanulniuk, és folyamatosan képezni magukat, hogyan védjék meg adataikat, cégüket, bizalmas információikat az incidensektől, támadásoktól.

A [Cyber Streetwise felvilágosító kampányoldalon](#) rajzokkal, videókkal is kiegészítve próbálják mindezeket szemléletesen, könnyed közérthetőséggel, tanácsokkal is kiegészítve összefoglalni brit felhasználók számára.



Mi itt most **rajzfilm** helyett inkább korábbi, hosszúsága miatt két külön fejezetre bontott hosszabb írásunkat linkeljük be, amely persze nem ölel fel minden fenti területet, de a magánélet, privát szféra tekintetében legalább sok olyasmiről ír, ami a napi vírusos, kártevős, adathalászos posztjainkban méltatlanul kevés említést kap. A "[Minden, amit a privacy-ról tudni akartál... I. rész](#)" főként a Facebookkal, hamis profilokkal, túl könnyen kitalálható jelszavakkal foglalkozik, míg a "[Minden, amit a privacy-ról tudni akartál... II. rész](#)" a személyes adataink kezeléséről, Google kereséseinkről, alapértelmezett megosztási beállításokról és hasonló elgondolkodtató dolgokról szól, **bemutatta, hogy milyen kockázatok, veszélyek jelentkezhetnek azon túlmenően, hogy például vírussal fertőződik a gépünk.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Célkeresztben a telefontolvajok](#)
[Safer Internet Day 2014](#)
[Gyerek-barát netezés](#)
[Védtelesen hagya a bootoló PC-t a 2009-es Norton](#)
[Miért romlik el minden?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5759413>

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](#).

[zsoci](#) 2014.01.16. 01:07:26

A vírusirtó egy felesleges, erőforrásszabáló, indokaltan marhaság.
Csak arra jó, hogy rátukmáljanak a vevőkre egy újabb felesleges softwaret, egy csomó pénzért.

Én sose használok, és mégis tele a gépem vírusokkal. És jééé, a windows sem omlik össze folyton. Az előző Vista 6,5 évig volt a gépem. És ha mégis tele lesz egyszer? Majd újratelepeitem.

Válasz erre



[enpera](#) • <http://uborkakonzerv.blog.hu/> 2014.01.16. 06:53:27

[@zsoci](#): akkor tudtadon kívül vírusos a géped.

Válasz erre



[laptop szerviz](http://www.doctorhouse.hu) • <http://www.doctorhouse.hu> 2014.01.16. 08:00:03

@zsoci: ne írj itt ileneket, mert mindjárt jön az informatikai szakértők hada és életfogytiglanra ítélnék :)

Válasz erre



[Csizmazia Darab István \[Rambo\]](http://antivirus.blog.hu) • <http://antivirus.blog.hu> 2014.01.16. 08:24:23

Én úgy vélem, még sosem volt szükség ennyire vírusirtóra, mint most. Leesnek a karakterek az alsó sorba, zenél a Yankee Doodle, újraindítja a gépet a Blaster - kit érdekel?

De ha mondjuk a trójai programok dömpingjét nézzük, és nem számítjuk a kémkedést, adatlopást, akkor ha kitörlik az adatokat, fotókat, dokumentumokat, munkákat, az a felhasználók 95%-nak igenis fáj.

A CryptoLocker például alig negyedóra alatt visszaállíthatatlanul ledarálja ezeket a fájlokat gépedről:

*.odt, *.ods, *.odp, *.odm, *.odc, *.odb, *.doc, *.docx, *.docm, *.wps, *.xls, *.xlsx, *.xlsm, *.xlsb, *.xlt, *.ppt, *.pptx, *.pptm, *.mdb, *.accdb, *.pst, *.dwg, *.dxf, *.dxg, *.wpd, *.rtf, *.wb2, *.mdf, *.dbf, *.psd, *.pdd, *.pdf, *.eps, *.ai, *.indd, *.cdr, *.jpg, *.jpe, *.jpeg, *.dng, *.3fr, *.arw, *.srf, *.sr2, *.bay, *.crw, *.cr2, *.dcr, *.kdc, *.erf, *.mef, *.mrw, *.nef, *.nrw, *.orf, *.raf, *.raw, *.rw1, *.rw2, *.r3d, *.ptx, *.pef, *.srw, *.x3f, *.der, *.cer, *.crt, *.pem, *.pfx, *.p12, *.p7b, *.p7c

Ismerve az általános mentési hajlandóságot, gyakoriságot ez sokaknak könnyen okozhat tragédiát. A Windowst újra tudod telepíteni, a saját elvesztett munkát viszont nem, olyat nem árulnak a boltban ;-)

Válasz erre

G4B33 2014.01.16. 14:22:16

@Csizmazia István [Rambo]: Yankee Doodle.. még a régi szép időkben elkaptam már azt a vírust..:D

Válasz erre

Tomi1977 2014.01.17. 14:00:44

Szia Rambo!

2 dolgot szeretnék kérdezni ezzel kapcsolatosan:

Nekem alap dolog, hogy legyen a gépen vírusirtó. Viszont, amit nehezen tudok megemészteni, az a Windows frissítése. Épp most telepítem a gépemet, de nem tudom mi legyen, bekapcsoljam-e vagy ne a frissítést. Most Windows 7-et használok és Office 2010-et, de tudom, egyszer ezeknek a programoknak is eljön az ideje, amikor a Microsoft nem készít hozzá javításokat, úgy, mint most azt az Xp esetében teszi majd.

Mit csináljon az, aki megkedvelt egy programot, hozzánőtt, és nem akar újra váltani? Márpedig ha annak idején nem váltok majd, akkor veszélynek leszek kitéve. Én azonban nem tudom megszokni a Windows 8-at, felesleges dolgokkal van tele, nincs szükségem az Office 2013 új szolgáltatásaira sem.

Csak a terméktámogatás miatt mindig új verzióra beruházni és bővíteni a gépet nagyon sok pénz. Nekem legalább is.

Másik kérdésem, hogy baj-e, ha régebbi NOD 32-öt használok? A 4.2-öt nagyon megszoktam, rendkívül gyors, kevesebbet fogyaszt, mint az új.

Köszönöm válaszat előre is!

Válasz erre



enpera • <http://uborkakonzerv.blog.hu/> 2014.01.17. 14:26:59

This is one half....

Válasz erre



[Csizmazia Darab István \[Rambo\]](http://antivirus.blog.hu) • <http://antivirus.blog.hu> 2014.01.17. 18:15:10

Szia Tomi1977!

A Windows, Java, Flash stb frissítése nélkülözhetetlen ahhoz, hogy a közismert és széleskörben kihasznált sebezhetőséget bezárd a gépeden, enélkül - és persze vírusirtó és óvatosság nélkül - nincs biztonság, ez van.

Az XP szeretetet megértem, nekem is van egy 9 éves notebookom XP-vel, 2 alaplaptercsén vagyok túl, ha bekrepál, akkor hagyom is, de addig elketyeg, én is szeretem. Azért ha április 8 után nem lesznek biztonsági javítások, rosszabbodni fog a vírushelyzet szerintem, és állítólag a kártevőterjesztők is csendben visszatartják a közben felfedezett 0day-eket addig, hogy biztosan nem legyen rá foltozás.

A NOD-dal az a helyzet, hogy bátran használhatsz újat is, a 6-os és 7-es újra gyorsabb, és kevesebb erőforrást igényel, ebben volt egy kicsi visszaesés korábban. Szóval az újak is simán futnak XP-n, nálam például a 7-es Smart Security. Korábban használni lehet ugyan, de biztosan kompromisszum ez a biztonság rovására, hiszen az újabb, illetve javított modulok csak az új verziókban üzemelnek.

Ha mégis váltanál Windowst, nekem a 7-es szimpatikus - magánvélemény - a 8 nekem se jött be, igaz hogy ezek persze erősebb hardvert igényelnek. (Egyébként meg ha szeretsz kirándulni az OS-ek világában, a Linuxok közül is lehet LTS, azaz hosszú távon támogatott disztrókat találni, például még a PAE előtti gépekre is pl. a Linux Mint 13-as, és hasonlókat.)

Válasz erre

[Tomi1977 2014.01.20. 21:54:35](#)

Szia!

Nagyon köszönöm válaszod! A Win 7-et használom már régóta, csak a frissítés kérdése volt bennem tisztázatlan. Közben utánaolvastam, a frissítést tényleg nem lehet megúsni. Biztonsági cégek is úgy nyilatkoztak, hogy nem tudják garantálni a biztonságot frissítetlen gépen, a kártevők egyszerűen megkerülik a védelmet.

Válasz erre

A Starbucks mobilfizetés esete a clear texttel

2014.01.17. 10:08 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [hiba](#) [itunes](#) [jelszó](#) [daniel](#) [app](#) [wood](#) [startbuck](#) [cleartext](#)

Jó dolog a kényelem, minden áron azonban nem érdemes törekedni rá. Mint az a beszámolókból kiderült, a Starbucks kávélánc mobilos platformon működő fizetési applikációja nem csak földrajzi adatainkat tárolta sima olvasható szöveggént, hanem ráadásul a jelszavainkat is.



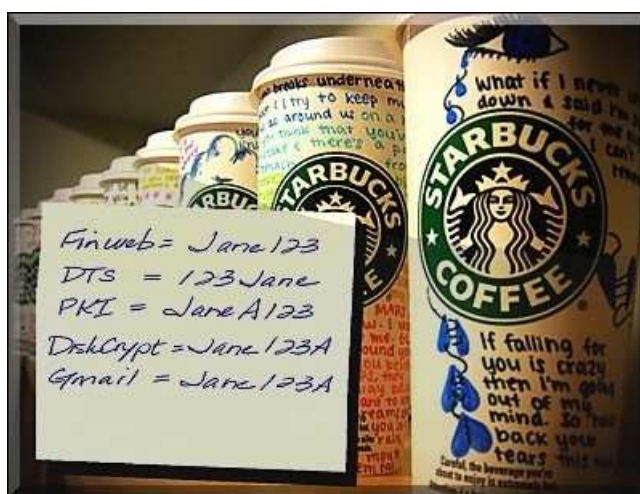
Ha még azt is hozzá vesszük, hogy az USA-ban ez a leggyakrabban használt mobil alkalmazás, akkor többet várnánk el egy ilyenről, és szinte érthetetlen, hogyan lehetett ezt így elkészíteni. [A hitelesítő adatok tárolása oly módon, hogy ahhoz bárki, aki a telefont csatlakoztatja egy számítógéphez, simán láthassa a jelszavakat és felhasználóneveket - nem fog bekerülni a kódolás aranykönyvébe.](#) Ha esetleg mégis tanítani fogják ezt a biztonságos programozás tantárgy keretében, akkor is maximum elrettentő példaként.



A "könnyű használat" és a "kényelem" jegyében csak egyetlen egyszer kellett megadni a jelszavunkat, amikor aktiváljuk a fizetési lehetőséget, [onnantól kezdődően ez folyamatosan él, és korlátlan költést tesz lehetővé.](#) Dönthettek volna úgy, hogy biztonsági okokból nem tárolják a jelszavakat helyben a készüléken, dönthettek volna úgy, hogy titkosítva tárolják, dönthettek volna úgy, hogy minden vásárlási tranzakciónál jelszót kérnek, de ezek egyikét sem tették. Vicces módon az app csak és kizárólag akkor kéri be újra a passwordot, ha pénzt fizetünk be rá ;-).



Nos ha ott ellopnak egy telefont, [akkor ezek miatt ez főnyereményt jelent a tolvajnak](#), arról nem is beszélve, milyen sokan vannak még mindig azok, akik ugyanazt a jelszót több helyen is, vagy ami még rosszabb, minden egyes helyen azonosat használnak. Akkor ugye mellékszálként végig lehet aratni a levelezésen át a közösségi oldalakig mindent.



Daniel Wood biztonsági kutató mindezt még tavaly novemberben jelezte, majd miután hónapokig nem kapott választ, [idén januárban publikálta is a történetet](#). Akkor aztán beindultak a lépések, "Ügyfeleink biztonsága rendkívül fontos számunkra, ezért aktívan figyelemmel kísérjük a kockázatokat, nem volt semmi új információ" kezdetű sajtó nyilatkozat, majd a gyors "extra layers of security" hozzáadásának bejelentése. **Hogy rendre miért mindig ez a forgatókönyv, amikor a különféle óriás cégeknek segítő szándékkal újra és újra hibát jeleznek, az az Élet egyik nagy, szomorú és teljességgel megfejthetetlen rejtélye.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

- [LastPass a pácbán](#)
- [Éljen soká az alapértelmezett jelszó 2.](#)
- [Nekem nyolc](#)
- [Lopott Minecraft jelszavak szivárogtak ki](#)
- [Munkavállalói adatok szivárogtak az Nvidia-tól](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5762452>

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](#).

Yeto 2014.01.17. 13:07:39

Hát, azért ez nem olyan nagy rejtély ha csinász egy személyiségprofilt azokról az emberekről akik ezért felelősek.
Válasz erre

Telekom számla vagy mégsem?

2014.01.20. 11:57 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [spam](#) [telekom](#) [vagy](#) [pdf](#) [számla](#) [trójai](#) [villanyszámla](#) [virustotal](#) [mégsem](#)

Alig pár napja csak, hogy [a Picasa képek miatt került egy írásunk](#) a Magyarországon világhírű "Vagy mégsem?" rovatunkba, de máris itt a következő adag, a téma jószerivel kifogyhatatlan. Egyfelől érkezett egy Telekom számla, másfelől villanyszámát is kaptunk "Helló Ügyfél!" megszólítással. Pocsék időt semlegesítő poszt következik.



A "Vagy mégsem?" rovat állandó részeit mostantól [nem írjuk le minden egyes alkalommal, akit érdekel olvasson vissza például itt](#). A főlényeg: kéréten levélként érkező linkre, mellékletre sose kattintsunk, legyen az állítólagos feladó bárki. Másik főlényeg, a primitív vonal szerint sokszor a feladó e-mailcíme is egyből szemet szúr, másrészt az egér mutató kattintás nélküli link fölé húzása (hover) is orbitális ukrainai, orosz, brazil és egyéb webhelyeket mutat rendre a banki, PayPal és egyéb behazudott URL-ek helyett, ezekre érdemes figyelni.



Mai két versenyzőnk közül az első egy állítólagos villanyszámla, melyben közlik velünk, hogy a 2013-es évi villamos energia fogyasztásunk elérte a limitet (ezmie?), ám ha igény tartanánk kedvezményes energia tarifára, akkor nincs is más dolgunk, minthogy kattintsunk az új, kedvezőbb fizetési feltételeket tartalmazó számlát tartalmazó mellékletre. Itt legalább adtak a látszatra, mert a feladó "Customer Service Department <editor@iexpressusa.com>", persze ennek fényében már kevésbé logikus, hogy akkor a számlát miért is a [http://mc-prokill.4fan.cz](#) domainről kellene letölteni ZIP-ben, de never mind, nem kell mindent érteni :-). Lekapva a fenti állományt és kicsomagolva a zipet, a [korábbi kettős fájlkiterjesztést nyomokban idéző](#), de azt barbár megoldásként abszolváló fájl tárul elénk:

"2013.6734766.pdf".....exe"

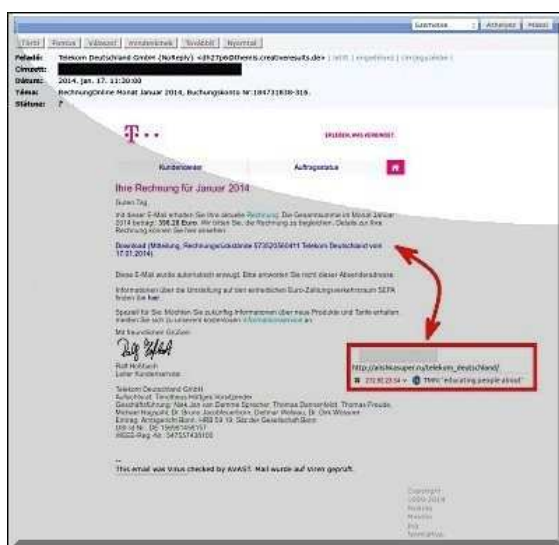
Igen, vállalkozókedvűeknek lehet saccolni, hány darab underscore karakter is van ebben a fájlkiterjesztésben, a választ majd ismertetjük a zárszóban, a helyes tippelők között értékes PDF villanyszámlákat sorsolunk ki :-)



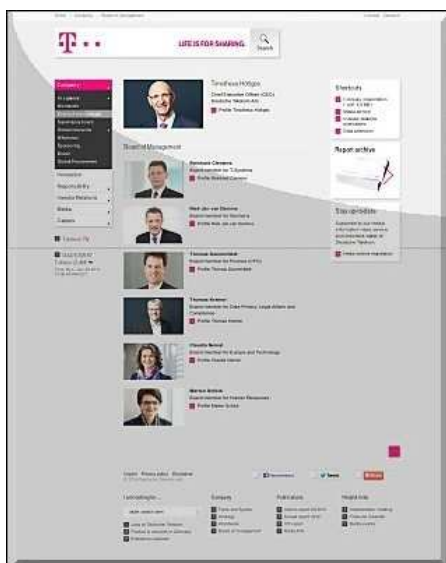
Dobjuk is be gyorsan kedvenc VirusTotalunkba, ahol aztán azonnal látszik, hogy sajnos nem ezen a kedvezményekkel felruházott tételen fogjuk megspórolni a következő C osztályú Mercink árát. A kártevőt [szombaton még egyedül csak az ESET detektálta](#), mostanra viszont [már a motorok mintegy fele jelzi, hogy egy jól fejlett trojan downloader](#) próbálkozott ügyeskedni házuk táján, aztán így járt.



Ma számlás napunk van, jön is rögtön a másik, ami pedig egy német nyelvű telefonszáma, mely pedánsan jelzi, hogy valamilyen rejtélyes okból kifolyólag nem a magyar T csoport, hanem a kinti akar tőlünk úgy mindössze potom 398 Eurót beszadni. A levél feladója a Telekom Deutschland GmbH, akivel jó esetben nem is vagyunk üzleti kapcsolatban. A "Guten tag" kezdetű levelükben egyrészt tájékoztatnak arról, hogy ezt az állítólagos 2014. januári számlát bátran kifizethetjük, hiszen létezik az egységes Euró övezet, másrészt itt is gálánsan mellékelik a számlát, amely rejtélyes módon a "hxxp://alishkasuper.ru/telekom_deutschland/" webhelyre mutat. Ide látogatva kapunk egy index.html állományt, ami valójában egy ZIP, benne egy kacifántosan szép nevű "Mitteilung_Rechnungsruckstande_9901169820005294_Telekom_Deutschland_GmbH_vom_Januar_2014.exe" fájlt találunk.



Itt a levél alatt az ügyfélszolgálati vezető, a felügyelő bizottság, és a teljes menedzsment tagság neve ott sorakozik, nyilván amiatt, hogy ezek láttán biztos többen fizetik be a 398 eurót ;-). A készítőik vették a fáradságot, és lekoppintották az eredeti oldalról a vezetőség névsorát, amelyben ott van egy igazi van Damme is, aki persze egy másik, és nagy valószínűséggel aligha spárgázik a Volvo kamionok visszapillantó tükrén két T csoportos telefonszámla kontírozása között. Érdekes bizalomépítő trükk, hogy egy létező antivírus ellenőrzési igazolását is ott lehet olvasni a levél alsó sorában, de mi ennek sem dőlünk most be.



Dolgozzanak csak a víruskeresők, ezért itt is bepottyantjuk a "számlát" a VirusTotalba, aminek meg is lesz az eredménye. Szombaton még itt is csak 10 motor detektálta ezt a trójait, a mai hétfőre azonban jelentősen felzárkózott a mezőny, és immáron 29-en is észlelték a 48 közül.



Összegezve, kezeljük óvatosan a kérértlen leveleket, még ha számlás linket vagy mellékletet is tartalmaznak, és olvasás előtt gondosan töröljük ki őket :-)
) Másfelől pedig vegyük észre azt is, [korántsem biztos, hogy minden spam csak veszélytelen kanadai gyógyszerész oldalakra](#) vezet, mert igen sokszor találhatunk kártevőt is a linkek végén, vagy a csatolt mellékletekben, vagyis tényleg nem árt az óvatosság.
 (A helyes válasz: 108 darab alálhúzás karakter :-)

Tetszik 20 személy kedveli ezt Regisztrájl, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pinit** **G+1**

Ajánlott bejegyzések:

[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Be nem fizetett számla. Vagy mégsem?](#)
[Instagram üzenet. Vagy mégsem?](#)
[Új Picasa képek az albumunkban. Vagy mégsem?](#)
[Erősítsük meg új mailcímünket. Vagy mégsem.](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5771803>

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](#).



Pa Lee 2014.01.21. 11:52:11

Ó, én ma a Z-Telekomtól kaptam levelet, de sajnos nem tudom megmondani, hogy egyszerű kereskedelmi spam, vagy a fentiekhez hasonló vírusos meglepi volt-e, mert (hogy klasszikust idézzek) olvasás előtt gondosan töröltem.

Válasz erre



eßemfaßom meg áll • <http://tahobloggerek.blog.hu> 2014.07.28. 15:06:42

aki egy előre nem egyeztetett mailben érkező csatolmányt megnyit, az megérdemli. Úgy tanul a gyerek, ha megnyitja a tefelesegedmeztelenul.jpg.exe -t
Válasz erre

Epikurosz 2014.12.02. 11:36:58

Szóltam nekik, hogy csálnak a nevükben. Teljesen jó németséggel van írva az egész, nagyon gáz.

A 108 pedig szent szám az indiai mitológiában. :D
Válasz erre

Figyeld a kígyót! Nem semmi. Hanem átverés :-)

2014.01.22. 11:22 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [videó](#) [urbanlegends](#) [facebook](#) [csalás](#) [átverés](#) [megosztás](#) [előre szenzációs](#) [lájlok](#)

A Facebook üzenetben egy hátborzongató videót ígérnek, amelyben egy óriási kígyó megeszi az állatkerti gondozót. Ha ilyen üzenetet kapunk egy Facebookos ismerősünktől, igen nagy a valószínűsége, hogy őt is átverték, és áldozatul esett egy csalásnak. Ha előre lájk vagy előre megosztás kell egy érdekes videó megtekintéséhez, legyen "aha" élményünk, hogy átverés az egész.



A dolog úgy működik, hogy [ha valaki mégis rákattint, az összes ismerőse üzenetet kap a nevében, és csak terjed, és terjed](#). Az is előfordul, amikor előbb egy appot kell előre engedélyezni, ám ha ezt tesszük, ezzel valójában elfogadjuk az alkalmazás készítője által megadott feltételeket, és hozzáférést biztosítunk számára személyes adatainkhoz. Olyan forgatókönyv is lehetséges, hogy a kattintó egy hamis Facebook oldalra kerül, ahol "újra be kell jelentkezni", és ott szépen ellopják a jelszavát, vagy "hiányzó" kodeket, azaz kártevőt telepíttetnek fel vele, és hasonló. [Ez a mostani kígyós kampány is egy átveréses lájkgyűjtés](#), ráadásul itt az [eredeti afrikai képet is könnyen](#) megtalálhatjuk a WhiteAfrican weboldalon, ez 2005-ből való. Ha bármilyen képnek utána szeretnénk nézni ("The real intelligence hero is Sherlock Holmes, not James Bond."), akkor a jópofa [TinEye féle reverse search](#) keresőt érdemes használni, itt [a kígyós képre keresve kapjuk](#) rögtön a képhasonlóság alapján az alábbi sort, Ká minden másod- és harmad-unokatestvére szerepel rajta a Dzsungel könyvéből :-)



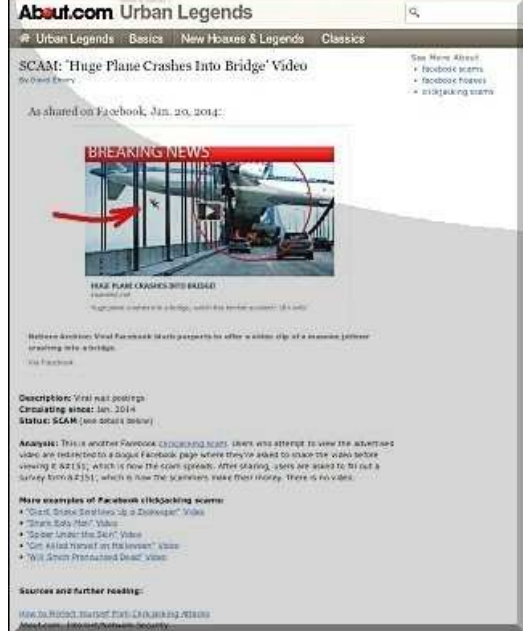
Jól láthatóan erre a régi felvételre lett aztán 9 évvel később ráfotoshopolva az állítólagos keresztben lenyelt állatkerti gondozó, és a video indításnak látszó gombok a csaláshoz. [Egy nagyon hasonló átverés volt tavaly Justin Bieber kapcsán](#), ott is a fotoshop játszotta a főszerepet, és persze ott is vissza lehetett nyomozni hasonló módszerekkel az állítólagos pucér felvételek alapjául szolgáló eredeti képet.



Ha csak pár híresebb ilyen előre lájkolós átverést kellene gyorsan megemlíteni, egyáltalán nem kapnánk inhüvelygyulladást a keresés miatt végzendő fokozott erőfeszítéstől, hiszen csak úgy hemzsegnek az ilyenek. A ["Mit visel ez a lány a strandon több ezer ember szem láttára kérdésre"](#) adandó helyes válasz meglepő módon nem a kacagányt vagy dolmányt, hanem a "fürdőruhát" :-). De említhetjük a 2011-es ["Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót"](#) esetet is. És persze ide sorolható az az átverés is, [ahol az indián nevünket lehetett megtudni, persze szigorúan csak egy előre lájk után](#).



Az alapvető gond ezzel, és minden más hasonlóval, hogy [ismeretlen cégeket, rejtett dolgokat ELŐRE KELL LÁJKOLNI, ahhoz, hogy egyáltalán megtudjuk, mi is az](#). Illetve hát kelleni éppen nem kell, csak sajnos láthatóan sokan mégis megteszik ezt.



Összegezve: ne legyünk hiszékenyek, ne hagyjuk magunkat kiszolgáltatni a csalóknak. Mindig, mindennap lesz olyan új állítólagos szenzációs videó, amivel megpróbálják becsapni, átverni az embereket. Legutóbb például [szellemet nézhettünk itt blogon](#), de a másik például egy két nappal ezelőtti állítólagos repülőgép balesetet bemutató videót ígér, még egy, [a gépből látszólag kizuhanó emberalak is oda lett montírozva](#) a nagyobb hatás kedvéért :-O



Emellett jól jöhet a naprakész antivírus, a jó kis script blokkoló NoScript böngésző kiegészítő, és [az ingyenesen használható ESET Social Media Scanner](#) is ide sorolhatjuk, amely ellenőrzi az üzenőfalán megjelenő posztokat, híreket és felhasználói üzeneteket is, hogy azok ne tehesenek kárt a gépünkben.



Ha pedig igaz híreket akarunk olvasni, egyszerűen menjünk el egy mértékadó hírportálra. Ha pedig videókat akarunk lájkmentesen, előre megosztás nélkül szabadon megnézni, akkor irány a YouTube és hasonló videomegosztó portálok.

Tetszik 160 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pint** **+1**

Ajánlott bejegyzések:

[Robin Williams utolsó telefonhívása. Vagy mégsem?](#)
[Megtalálták az eltűnt maláj repülőt! Vagy mégsem?](#)
[Indiánok a Facebookon](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5774779>

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](#).



**[Tom és Jerry fan](#) • <http://www.tomesjerryfan.hu> 2014.01.22.
22:03:17**

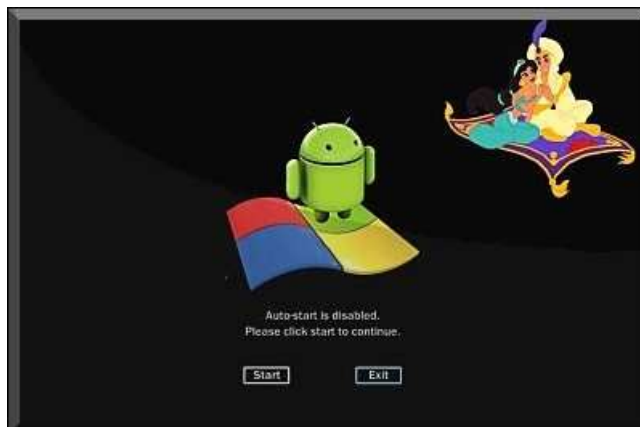
Magyar lapok esetében (bár már sok külföldivel is működik) javaslom a Lájktörőt: www.facebook.com/lajktoro/app_760091234018986 . Szépen kiadja a "lájkkal" (vagy megosztással) védett tartalmat, így legalább kiderül, hogy mit is kéne előre "lájkolni".
Válasz erre

Android és Windows, Windows és Android

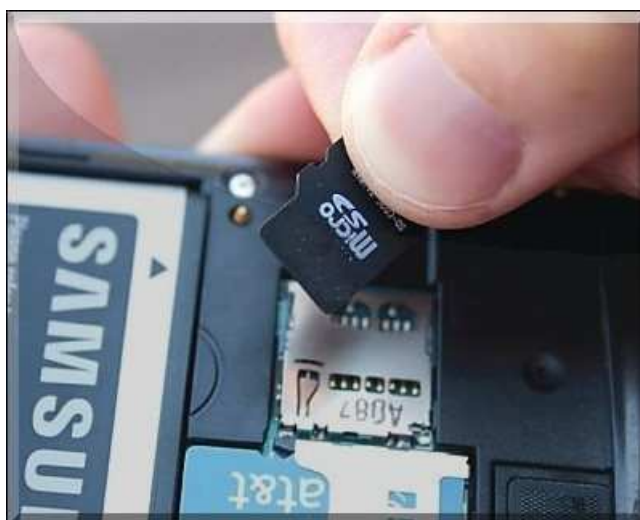
2014.01.24. 12:06 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [windows debug usb club trójai android computer kártevő banki chaos jacob appelbaum](#)

Emlékezhetünk korábban, hogy a kártevőkkel kapcsolatos meredek emelkedés miatt [az Android platformot az Új Vadnyugatnak, illetve az új Windowsnak is neveztük](#). Nos, most nem emiatt került egymás mellé itt a két operációs rendszer, más összefüggések nyertek napvilágot, nevezetesen olyan új kártevőt találtak, amely terjedése érdekében összeköti őket, részletek a folytatásban.



Essünk gyorsan túl azon a részen, melyben [az idei évi jóslatok azt írták, folytatódik a legnépszerűbb mobilplatform elleni támadások sora](#), és tovább emelkedik ezek száma. A felvezetés után akkor kezdjünk egy találós kérdéssel, mi a leggyakoribb kapcsolat a Windows és Android rendszerek között? Azok nyerték a hangszórót, akik memória kártyára tippeltek.



Előtte viszont még nézzük meg azt, mi az a két dolog, amely rontja a hagyományos védekezési módszereinket. Az egyik, ha nem a legelterjedtebb és legújabb Nexus lapul a zsebünkben, nem sok az esélyünk, hogy jöjjön rá biztonsági, illetve rendszer frissítés. Ha pedig valamilyen másod vagy harmadvonali, gyengébb hardverrel rendelkező készülékünk van, akkor nem hogy ritkán, hanem akár soha nem is frissül. Ehhez még csak nem is kell például ZTE-nek lenni, hiszen a régebbi Samsung modellek is rendre kimaradnak frissítésekből, így mondjuk teljes életciklusukban, egészen a kidobásukig az eredeti gyári, például a 2.3.x-es verzióval ketyegnek. [A másik pedig a kaotikus és indokolatlan engedélyek kérése a telepítendő alkalmazások részéről, amelyre sokan nem is figyelnek](#), de még ha figyelnek is, a folyamatos verziófrissítésekkel akkor is [akkora mozgás, változás van, hogy szinte képtelenség ezeket nyomon követni](#).



És akkor jöjjön a várva várt kártyás dolog. Ugye, ha valaki adatokat - dokumentumokat, zenéket, filmeket, egyebeket - **mozgatni akar a két rendszer között, akkor háromféle módon is megteheti**. Valamilyen Airdroid szerű alkalmazással wifin keresztül másolgat, **vagy** rádugja egy USB kábellel a telefont a számítógépre illetve kiveszi a rendszerint microSD kártyát, és az adapterfoglalattal

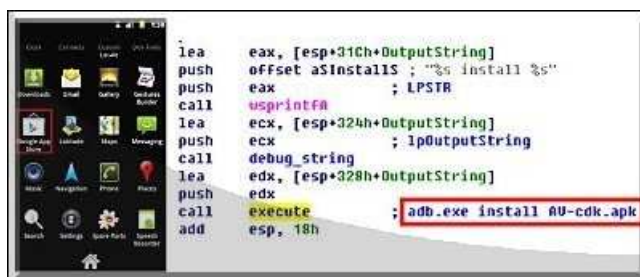
csatlakoztatja a PC-hez, ami statisztikai alapon főleg Windowsos.



És akkor itt lépett be az a már korábban ismert Androidos kártevő, amelyik **nagy trükkösen azt csinálta, hogy letöltött egy Windows futtatható PE EXE kártevőt az SD kártya gyökerkönyvtárába, és létrehozta vagy módosította az itt szereplő Autorun.inf állományt.** A módszer zseniális, ez ugyanis, amikor a Windows géphez csatlakozott külső meghajtóként, automatikusan lefutott és szépen végrehajtódott a kártékony EXE fájl.



Oké, ez eddig a múlt, lássuk milyen újabb, nem kevésbé leleményes támadásra figyeltek fel nemrég biztonsági kutatók. **Az új kártevő megfordította az irányt, ez most egy olyan Windows trójai, amely megfertőzi a számítógépet és először DLL könyvtárát rendszer szintű szolgáltatásként (service) regisztrálja.**



Ezután egy kártékony APK csomagot kísérel meg letölteni, majd amikor a telefont az USB kábelén csatlakoztatják, telepíti is az Androidra azt a kártevőt, melynek fő célja, hogy banki alkalmazások lecserélése trójai változatra, majd a pénzmozgás közbeni SMS üzenetek elfogása, illetve eltérítése. A fertőzött készüléken ilyenkor egy hamis "Google APP Store" nevű, a hivatalos Google Play piactér ikonjával szereplő alkalmazás felbukkanása is árulkodó jel lehet. A most felfedezett változat egy [legitim, koreai banki alkalmazásnak próbálta meg álcázni magát.](#)



Az incidenshez kapcsolódva hasznos tudnivaló, hogy az USB hibakeresési mód, ha éppen nem használjuk, akkor legyen mindig kikapcsolt állapotban, hiszen [enélkül a fenti fertőzőési módszer nem is képes működni](#). Nyilván itt azon túl, hogy a védekezés érdekében [alaposan megválogatjuk, milyen programot telepítünk az okostelefonunkra](#) még az is szükséges, hogy mind a számítógépünkön, mind pedig az Androidos eszközön fusson naprakész védelmi szoftver, és lehetőleg ne bankoljunk arról a mobil eszközünkről, amely a klasszikus kétfaktoros autentikáció helyett (két fizikailag külön készülék) helyett egyetlen telefonon fut mindez.



Aki pedig még ennél is jobban szeretne elképedni, annak a **30-ik Chaos Computer Club Konferencia rendezvényén elhangzott egyik remek előadást ajánljuk a figyelmébe, "Szolgálunk és Lehallgatunk (Hacktion a való világban)" címmel**. Aki végignézi, és aztán Jacob Appelbaum prezentációja során elhangzottak közül semmin sem lepődik meg, az bátran kommenteljen nekünk, és mesélje el a titkot, hogyan csinálja :-)

Tetszik 8 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Kamu Android app hajt a pénzünkre](#)
[A váltságdíjas titkosító kártevő visszatér](#)
[Itt az első váltságdíjas titkosító kártevő Androidon](#)
[Újra Bitcoin bányász kártevő a Google Play-en](#)
[Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5779465>

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 éves a mobil malware

2014.01.28. 09:22 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [telefon evolúció](#) [symbian malware](#) [mobile év 10](#) [android kártevő](#)

Tortát nem sütünk, gyertyát sem gyújtunk, de azért egy kicsit emlékezünk. Visszanézünk, honnan indult, meddig mosolyoghattunk lekicsinyítő ajakbiggyesztéssel, és mikortól jelentett aztán már komolyabb fejtörést, illetve veszélyeket. És a hol tartunk most, [mi várható a 2014-es esztendőben](#) felvetés sem maradhat ki egy ilyen összefoglalóból.



Alig [pár hónapja emlékezhettünk arra, hogy 25 éves lett számítógépes féreg](#). Most újabb évfordulóhoz érkezünk, **a mobilos kártevők hajnala ugyanis éppen jó tíz évvel ezelőtt kezdődött**. 2004-ben ugyanis igen érdekes jelenségről kaptunk hírt. A Symbian operációt rendszert futtató mobiltelefonok kerültek veszélybe [a még kezdetleges Cabir nevű vírus miatt](#). A zseniális újdonság az volt, hogy **a fertőzött készülék a bekapcsolt vezeték nélküli Bluetooth kapcsolaton keresztül igyekezett továbbadni a vírust egy bizonyos hatótávolságban (néhány méter) található másik telefonra**. Kiválasztott egy aktív Bluetooth vevővel rendelkező telefont, és ezek után erre az egy készülékre folyamatosan küldte tovább magát. A kártevőt az azóta már megszűnt 29A formáció ValleZ nevű tagja készítette demonstrációs célból: valódi "büntetőrutint" nem is tartalmazott, és a forráskódja is elérhető az interneten. Illetve **a büntetés tulajdonképpen az volt, hogy a telefon igen hamar lemerült a Bluetooth kapcsolat miatt**.



Még minden 2004-ben járunk, amikor egy újabb kártevőverzió tette próbára a felhasználókat. [Megjelent a Skulls, azaz Koponyák nevű kód, amely szintén Symbian-alapú mobiltelefonokat tudott megtámadni](#). Azt használta ki, hogy **a rendszer automatikusan bemásolta a rendszerfájlok nevével egyező nevű fájlokat a telefonba**. Települése után megfertőzte a készülékeket, és ez nemcsak abban nyilvánult meg, hogy **minden ikont egy koponyával helyettesített, hanem az alkalmazásokat is elérhetetlenné tette**. Ilyenkor két eset közül választhattunk: vagy leformáztuk a telefon – ekkor elveszett minden személyes adatunk, vagy szervizbe kellett menni vele.



A valamivel később, [2005-ben felbukkant CommWarrior](#) már számos tulajdonságában felülmúlta a Cabirt. Már nemcsak egyetlen készüléket választott ki a fertőzéshez, hanem minden, a hatótávolságában lévő és aktív Bluetooth kapcsolattal felvértezett telefont igyekezett megfertőzni. Ennél is érdekesebb, hogy saját magát már el is rejtette a feladatkezelőben (szemben a Cabirral, amelyet megtalálása után simán kilőhettünk a FExplorerrel), emiatt sokkal életképesebbnek bizonyult.



2006-ban aztán a RedBrowser volt az első olyan rosszindulatú program, amely nem csak a Symbianos okostelefonokat volt képes megfertőzni, de [minden olyan eszközt is, amelyik képes volt a Java \(J2ME\) alkalmazások futtatására](#). A JAR formátumú kártevő WAP oldalak böngészési lehetőségét ígérte WAP kapcsolat nélkül egy RedBrowser nevű alkalmazással, **károkozásra is alkalmas volt, ugyanis emelt díjas SMS szolgáltatásokkal manipulált, ezekből SMS-enként öt dollárt kaszáltak az ismeretlen, gyaníthatóan orosz illetőségű készítőik.**



Hogy még egy további mérföldkövet említsünk, [2008. februárjában bukkant fel a Windows Mobile rendszerre íródott úgynevezett InfoHijack](#). Ez a Kínában terjedő károkozó **kikapcsolta a Windows CE telepítéssel kapcsolatos biztonsági beállítását**, és a megfertőzött készülék gyári sorozatszámát, a futó operációs rendszer adatait, valamint egyéb információkat elküldte a kártevő szerzőjének. Az így manipulált eszközök a későbbiekben védtelenek maradtak káros kódok letöltésénél, hiszen a biztonsági figyelmeztetések már nem jelentek meg. **Magyarán egy klasszikus korai trójai hátsó ajtót láthattunk PocketPC-re, amely teljes hozzáférést biztosított ezzel a támadóknak.**



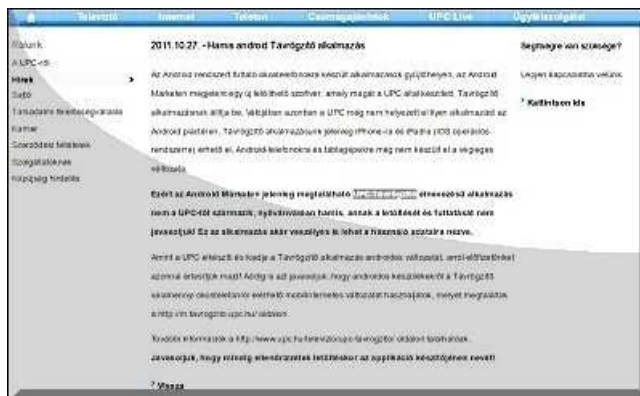
2009. novemberében egy ausztrál fiatalember, visszaélve a jailbreakelt iPhone telefonokat használók tudatlanságával és/vagy lustaságával, az alapértelmezett deafulat root SSH-jelszót - "alpine" - felhasználva írt egy C nyelvű férget. Ez távolról belépett mások telefonjába, lezárta az SSH-portot és felmásolt néhány állományt, többek közt lecserélte az inkriminált iPhone-ok háttérképét Rick Astleyre. A vírusíró, a 21 esztendő Ashley Towns csak egy jó balhének tartotta az esetet, azonban a publikált forráskódnak köszönhetően később több valódi kártevőváltozat is készült belőle. **Egy későbbi verzió például - az IKEE.B - már botnet hálózatot is tudott szervezni a megfertőzött gépekből.**



2010-ben jelent meg a ZytMo trójai, amely olyan veszélyes variánsa is felbukkant, amely [a fertőzött telefonon elfogta a banki kétfaktoros azonosításhoz tartozó SMS alírási üzenetet](#). A Zeus mobil trójai változata adathalász módszerekkel terjedt, és ebben igyekeztek arra rávenni az átvett felhasználókat, hogy töltsék le a fertőzött Androidos alkalmazást.



Azóta pedig - különösen Android platformon - az utóbbi három évben folyamatos a kártékony kódok megjelenése, amit jelentős részben az is elősegít, hogy [ez a platform lett a legnépszerűbb, és világszerte legelterjedtebb mobil operációs rendszer](#). Leleményben pedig nem szenvedtek hiányt a támadók, gondoljunk csak arra a 2011-es esetre, amikor is felbukkant egy magyar nyelvű trójai is. A UPC Távrögzítő elvileg arra képes, hogy ha nem érnék haza idejében, telefonunkról távolról online akkor is felvehetjük kedvenc műsorunkat. Ez mind szép és jó, a hiba csak az volt, hogy bár a UPC ezt akkor egyedül csak az AppStore-ból letölthető alkalmazásként iPhone és iPad készülékekre készítette el, [mégis feltűnt egy Androidos változat egy néhány hónapr a hivatalos Android Marketen és éppen "UPC Távrögzítő" néven](#). Hogy pontosan mikor és ki készítette, és mit is tett az alkalmazás a felhasználók gépével, azt már nekünk sem sikerült kipróbálni, mert rövid pályafutását végül a kitiltás koronázta meg, ám a statisztikák alapján addigra már több ezer letöltés történt.



2012-ben pedig [az úgynevezett USSD \(Unstructured Supplementary Service Data\) vezérlőkódok lehetővé tették a cyber-bűnözőknek, hogy távolról töröljenek adatokat a telefonkészülékekről](#), például úgy, hogy a felhasználót egy URL címre irányították, akár közvetlenül, akár egy egyszerű szöveges üzenettel vagy QR kód használatával. A [vírusvédelmi szakma hamar reagált a kritikus eseményekre](#), például az ESET 24 órán belül ingyenes blokkoló programot készített, melyet az Google Play piactérről bárki letölthetett, majd később ezt be is építette a Mobile Security for Android védelmi csomagjába.



[Azóta is folyamatosan jelennek meg az újabbnál újabb trükkök](#). Az egyik ilyen tavalyi Androidos kártevő például letöltött egy Windows futtatható PE EXE kártevőt az SD kártya gyökérkönyvtárába, és létrehozta vagy módosította az itt szereplő Autorun.inf állományt. A módszer zseniális, ez ugyanis, amikor a Windows géphez csatlakozott külső meghajtóként, automatikusan lefutott és szépen végrehajtódott a kártékony EXE fájl. De hogy magyar nyelvű átverésről is szó essen, a különféle ingyenes, azaz a freemium modell alatt futó, az ingyenességért reklámokat megjelenítő Android alkalmazásoknál lehet [belefutni abba, hogy a kijelzőn félreérthető, rendszerüzenetek látszó hirdetések jelenhessenek meg](#). Ahol például egy hamis vírusirtó esetében igen könnyen megtörténhet, hogy valaki vigyázatlanul rákattint, és ezzel automatikusan elfogadja az apró betűst, miszerint feliratkozik egy nagyjából hetente 15 EUR-ba - kb. 4400 HUF - kerülő szolgáltatásra, ami állítólag átvizsgálja a telefonját. Ha ezt az összeget összehasonlítjuk bármely, a Google Play hivatalos piactéren kapható fizetős legális antivírus teljes éves díjával, rögtön látszik, mekkora becsapás.



A napokban pedig egy [olyan új trójairól számoltak be, amely a Windows rendszerről fertőzi meg az Androidos rendszert](#). Amikor a telefont legközelebb USB kábelen csatlakoztatják a fertőzött Windows géphez, az telepíti a kártevőt az Androidra, melynek fő célja a banki alkalmazások lecserelése trójai változatra, majd a pénzmozgás közbeni SMS üzenetek elfogása, illetve eltérítése. A fertőzött készüléken ilyenkor egy hamis "Google APP Store" nevű, a hivatalos Google Play piactér ikonjával szereplő alkalmazás felbukkanása is árulkodó jel lehet. A most felfedezett változat egy legitim, koreai banki alkalmazásnak próbálta meg álcázni magát, de nyilván nincs rá garancia, hogy idővel később más országok bankjai ellen nem jelenik meg majd hasonló.



Vagyis a jelek szerint eljutottunk oda, hogy [tényleg az Android lett az új Vadnyugat](#), de persze vigyázni azért minden platformon kell. Emellett pedig már valóban érdemes a mobiltelefonunkon is védelmi programot használni, valamint [a megbízható forrásból való letöltés az](#), ami még hatékonyan megóvhat minket a nagyobb kellemetlenségektől.

[Tetszik](#) Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [G+1](#)

Ajánlott bejegyzések:

[25-ször több a mobilos kártevő](#)

[A Google Play vigyáz rám](#)

[Beváltak-e a 2014-es jóslatok?](#)

[Megfertőzheti-e számítógépünket az e-cigaretta?](#)

[A váltságdíjas titkosító kártevő visszatér](#)



Hirdetés

A bejegyzés [trackback címe](#):

<http://antivirus.blog.hu/api/trackback/id/5786028>

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 Darab István [Rambo] • <http://antivirus.blog.hu> **2014.01.28. 22:19:52**

Mai ide kapcsolódó hír, hogy gyorsan terjed az első androidos bootkit:
www.hwsz.hu/hirek/51690/android-bootkit-trojai-kartevo-kinai.html

Válasz erre

antyg 2014.01.29. 09:37:07

Üdv Mindenki! Jó a cikk!

Egy kérdésem lenne... a mobilokon kiadott vírusok nem öregebbek? Tudomásom szerint az első vírus mobil készülékre (akkor még ugyan nem voltak okos készülékek) a Timofonica volt még 2000 júniusában. (a vírus főleg a spanyol Telefónica előfizetői körében terjedt). A víusról többek között itt is lehet olvasni: www.kaspersky.com/news?id=68

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.01.29. 19:10:36**

Szia Antyg!

Üdv a blogon :) Könnyen lehet, hogy ebben igazad van, ám az első említésre méltó, szélesebb körben elterjedt és közismert mobiltelefonos kártevő a Cabir volt.

A timfonica rémlett halványan, bár a linkeden a részletes leírás url már sajna nem működik. A PoC (Proof of Concept), azaz kísérleti kártevők néha nem lesznek annyira híresek, például a PC vírusoknál az 1986-os Braintól számítottuk az elsőt, az terjedt el széleskörben, annak ellenére, hogy 1981-ben már létezett a Maces Elk Cloner, ami korát messze megelőzve az Apple lemez boot szektorába írt.

A cikk úgy született, hogy láttam máshol az évfordulót, és nem csak lefordítottam azt, hanem kiegészítettem azokkal, amikkel én is találkoztam, és amiket jelentősnek mérföldkönek gondoltam.

Válasz erre

Mentési tippek CryptoLocker ellen

2014.01.30. 11:46 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [backup tippek](#) [mentés](#) [kártevő](#) [zsaroló](#) [cryptolocker](#)

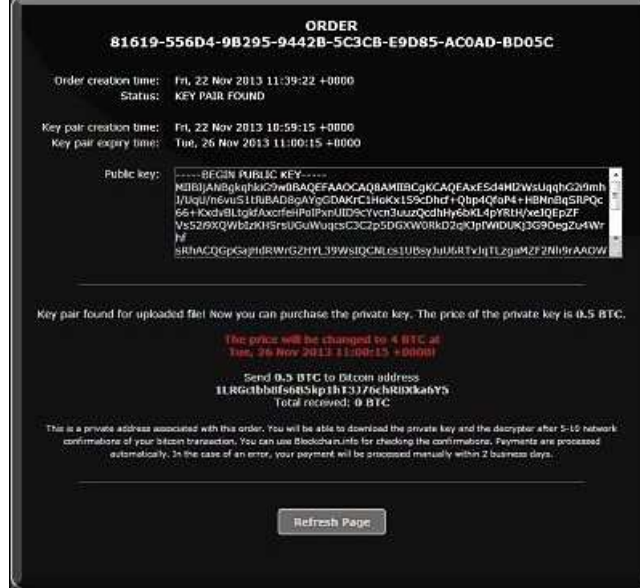
Egy korábbi posztunkban már szépen [összefoglaltuk a legfontosabb tudnivalókat a merevlemezünk, illetve adataink 2048 bites RSA kulccsal elkódoló zsaroló kártevővel](#) kapcsolatban. Ahogy ott is elmondtuk, az a **legfontosabb, hogy a legnagyobb hangsúlyt a megelőzésre tegyük, mert a mentés sokszor nehézkes, vagy időnként akár nem is lehetséges.** Ebben egyfelől a naprakész védelem, másfelől a frissen tartott szoftverkörnyezet, valamint a biztonságtudatos viselkedés segíthet nekünk. És még valami: **a rendszeres és alapos mentés, most éppen erről lesz szó.**



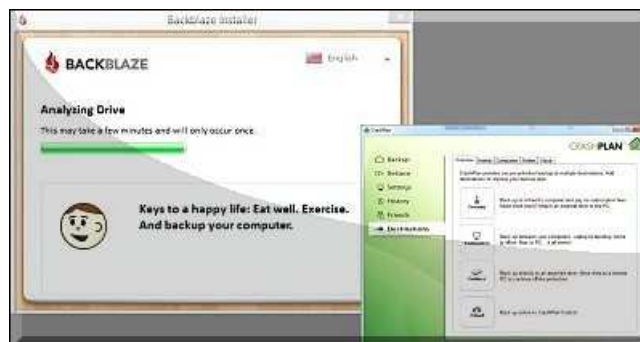
Miért fontos a rendszeres és külső adathordozóra való mentés? Mert a helyreállítás enélkül gyakorlatilag lehetetlen. Sőt, semmilyen garancia nincs arra sem, hogy az esetleges váltságdíj fizetés után valóban kapunk privát kulcsot, és újra hozzáférünk az adatainkhoz: vagy igen, vagy nem. Azért említsük meg a "kért" összegeket is: nem kispályáznak, ugyanis **300 eurótól (körülbelül 90 ezer forint) egészen a brutális 3000 USD-ig terjedő (2200 EUR, azaz 680 ezer forintnak megfelelő) summát** - emlékezzünk csak arra, hogy pár éve a hamis antivírusok még 50 dolláryi "aprópénzzel" is beérték. Emellett nehezíti a helyzetet az is, hogy **egyes kártevők képesek a helyi backup állományainkat is törölni**, sőt a Cryptolocker újabb variánsai sajnos már szisztematikusan vadásznak a rendszer visszaállítás adatfájljaira. Illetve egyes friss Cryptolocker verziók **a korábban még esetlegesen kiskaput jelentő úgynevezett Shadow Copy fájlokat is könyörtelenül megsemmisítik**, természetesen pedánsan még az elkódolási procedúra előtt.



Így akkor marad nekünk a mentés, mint egyetlen hadra fogható módszer, de ezt sem mindegy, hogyan tesszük, ezért most ehhez adunk néhány hasznos tanácsot. Először is azt kell tudni, ha a mentés csupán helyi: vagyis az említett backup, local shadowcopy, rendszer-visszaállítás vagy éppen helyi tükrözés, **akkor ez nem ér semmit, mert a kártevő letörli, illetve a helyben tárolt tükrözött másolatokat is letitkosítja.** Emellett, hogy ne legyen olyan egyszerű az élet, azt is fontos megemlíteni, hogy ha már egyszer bejutott a gépünkre a Cryptolocker, akkor **minden Windows alatt mappelt - értsd felcsatlakoztatott, betűjellel megosztásként hozzárendelt - meghajtónkon is végiggyalogol a titkosításával, így sajnos az összes bedugott USB tárolónk, hálózati meghajtóink, de még a felhős tárhelyünk is áldozatul eshet.** Ez pedig még akkor is így van, ha az adott megosztás nem is Windows alapú gépen található, de onnan elérhető, sajnos mi láttunk így Linuxos megosztást tönkrezúzni.



Az első talán az lehet, hogy győződjünk meg arról, ha a mentésünk készen van, akkor azonnal le legyen választva a tároló eszköz a rendszerről. Ugye a fentiek miatt a nap 24 órájában csatlakoztatott külső merevlemez állományai ugyanúgy elvesznek, mint a helyi tartalom. **Emellett pedig készítsünk rendszeresen csak olvasható formátumban - CD, DVD lemezekre is.** Mind a megírt optikai lemezeket, mind pedig az esetleges külső winchestert érdemes a géptől távol, például egy másik lakásban, tűzbiztos széfben tárolni. Természetesen a kisebb adatkapacitás nehezíti a feladatot, de **ennek ellenére hasznos, mert egyelőre olyan vírust, amelyik DVD lemezekre írna, egyelőre még nem ismerünk :-)** És azt csak zárójelben jegyezzük meg, a mentést titkosítani is érdemes, hiszen ha egyedi csak azt lopnák el, akkor is veszteséget szenvedünk el.



A felhős tárhely is besegíthet a mentésben, mi mindazonáltal itt is a titkosított tárolásban hiszünk, de ezt döntse el mindenki maga. Felhő tárhely esetében kétféleképpen is menthetünk: vagy egy dedikált munkakönyvtárunkat, meghajtónkat szinkronizáljuk vele valós időben, vagy alkalmanként oda is feltöltjük a mentési köteteket. **Számos ilyen felhős alkalmazás nem hagyományos betűjeles megosztásként viselkedik, hanem saját tárolási formátumban dolgozik,** így ezek zömével elkerülhető, hogy ott is dűlés, pusztítás legyen. **Azt sem szabad elfelejteni, ha beüt egy esetleges fertőzés, azonnal meg kell akadályozni, hogy a sérült adatok felülírhassák a korábbi tiszta mentési fájlokat.**

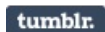


Amint említettük, legyen párhuzamosan több különböző verziónk is a mentésből, ne mindig bambán és gépiesen felülírva az előzőt. Ha egyszer kiderül, hogy esetleg mégis bejutott a fertőzés, akkor így nagyobb eséllyel találunk korábbi sértetlen állapotot, lesz miből válogatni a nehéz órákban. Itt végül is ellentmondunk annak a régi szabálynak, hogy ne tároljunk semmit se redundánsan, most éppen pontosan erre van szükség.



Egy jó mentési szisztéma kiválasztása, megtervezése persze hosszabb ideig tart, de mindenképpen érdemes vele foglalkozni, ne legyünk lusták, mert egyre inkább nélkülözhetetlen. Ahogy láttuk, muszáj rendszeresen nem csak inkrementális (egymásra épülő), hanem néha teljes különálló mentéseket is végezni, sőt ezek közül valamilyen logika és ütemezés alapján egyes adathordozókat nem felülírva azokat véglegesen örökre megőrizni. Végül, de nem utolsó sorban régi vesszőparipánkat is emlegetjük újfent, miszerint [csak a kipróbált, visszaállítással is tesztelt mentés nevezhető valódi mentésnek](#).

 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Bitcoinos zsaroló járja be Európát](#)
[Védd a CryptoLocker terjesztőjének fejére](#)
[Kisokos a Cryptolocker kártevő ellen](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Magyarországra is megérkezett a CTB-Locker](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5789739>

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](#).

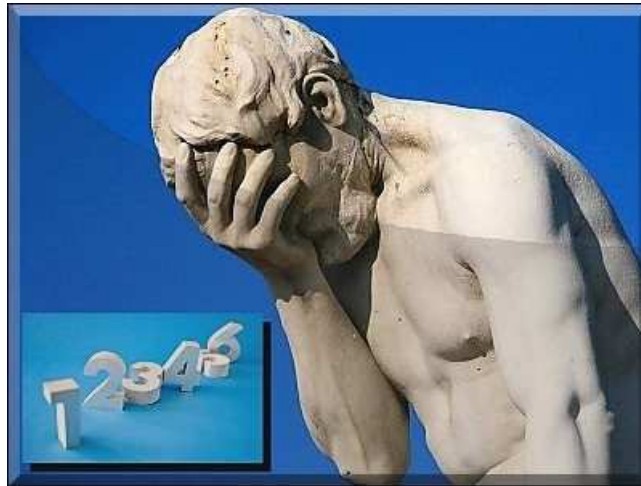
Nincsenek hozzászólások.

Így bánunk a jelszavakkal

2014.02.03. 11:31 | [Csizmazia Darab István \[Rambo\]](#) | [14 komment](#)

Címkék: [usa](#) [jelszó](#) [felmérés](#) [erős](#) [infografika](#) [jelszómenedzser](#)

Érdekes megnézni, hogyan kezeljük a jelszavainkat, milyen gyakran változtatjuk, mit választunk hozzá a készítéskor: inkább a kutyánk neve vagy véletlenszerű karakterek? Infografikás sorozatunkat folytatva ezúttal egy ebben témában készült felmérés eredményei szerepelnek egy látványos és tanulságos ábrában.



Amikor előadást tartunk a biztonságról, minden esetben előkerül a jelszavak témája, és egy klasszikus idézet szerint: "ez olyan, mint a fogkefe: mindenkinek van, nem adjuk kölcsön és néha lecseréljük". Annyi mindenesetre bizonyos, fontos eleme a biztonságnak, hiszen [ha túlságosan rövid vagy könnyen kitalálható, feltörhető, úgy járhatunk vele, mint annak idején Sarah Palin](#).

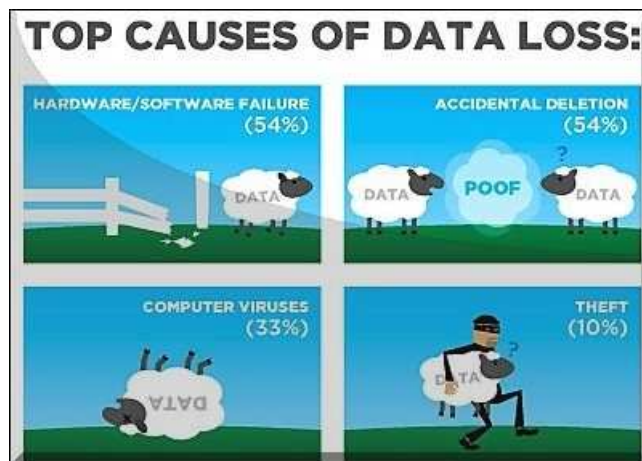


Az ábra végül is önmagáért beszél, de néhány adatot azért kiemelünk belőle. **16 százaléka a felhasználóknak sosem változtatja meg a jelszavát, és 18%-uk figyelmen kívül hagyja a jelzést, ha az általa leggyakrabban használt online vagy közösségi oldal jelszócserére figyelmeztető üzenetet küld neki.** A családtag, háziállat neve sajnos még mindig sokszor szerepel a jelszavakban.



De mindenesetre pozitív, hogy 39% egyedi és véletlenszerű adatokat használ fel ezek készítésekor. Végül egy utolsó kiragadott adat, a

fiatalok és a tanulók voltak azok, akik a legkevésbé éltek a komplex jelszoalkotási lehetőségekkel, amelynél kis- és nagybetűket, számokat valamint speciális karaktereket is kevernek az erős, és nehezen kitalálható jelszó megalkotása érdekében.



Arra nézve még **érdekesek lettek volna az adatok, hogy mennyire egyedi jelszavakról van szó, ugyanis az egyik leggyakoribb hiba még az is, hogy egy és ugyanaz a jelszó minden egyes belépési helyszínen**, erre azonban ezúttal nem tért ki az idézett kutatás. A felmérés eredményei egy korábbi, az Egyesült Államokban végzett interjú eredményét foglalja össze, és kétezer megkérdezett felnőttkorú válaszadó adatait tartalmazza.



Ha valaki arra kíváncsi, [mit ne válasszon jelszónak](#), akkor elrettentő példákat itt talál. Ha pedig [a jó jelszó választása a cél](#), akkor [ebben az összefoglalóban](#) próbáltunk meg minden létező fontos részletet egy helyen összefoglalni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

• [1 traceback](#)

Ajánlott bejegyzések:

[Így változtunk Snowden óta](#)
[Tűzre, vízre, és jelszóra vigyázzatok!](#)
[Informatikai biztonság az egészségügyben](#)
[Biztonságtudatosságból közepes alá](#)
[Bankolás idegen gépről, levelezés nyitott wifiről](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/5795671>

Trackbackek, pingbackek:

[Trackback: Hogyan kezelik a felhasználók a jelszavaikat?](#) 2014.02.07. 17:23:52

Egy érdekes infografika arról, hogy hogyan kezeljük jelszavainkat. A felhasználók 16%-a sohasem változtatja meg a jelszavát, még akkor sem, ha az általuk használt szolgáltatások jelszóváltoztatási figyelmeztetést küldenek nekik. Forrás: ESET, ...

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](#).



[Pikk 2014.02.03. 11:39:01](#)

A jelszó használatánál a felejtés elleni biztonság lép előre és a saját jelentéktelenségünkre épített bizalomra építve egyesek minden alkalomra és programra egy és csakis egy jelszót alkalmaznak :)

Válasz erre

[hvuk 2014.02.04. 10:40:36](#)

"Arra nézve még érdekesek lettek volna az adatok, hogy mennyire egyedi jelszavakról van szó, ugyanis az egyik leggyakoribb hiba még az is, hogy egy és ugyanaz a jelszó minden egyes belépési helyszínen, erre azonban ezúttal nem tért ki az idézett kutatás."

Ez szép és jó, azaz jó dolog, hogy mindenhova külön egyedi jelszót válasszunk, továbbá még mondjuk fél évente változtassuk is meg és mindegyik jelszó legyen egyedi és tők véletlenszerű, ráadásul csak fejben tartsuk nyilván és ne írjuk le. Mert ugye ez lenne az ideális. De mi a megoldás arra, ha valakinek 20-30 jelszóra van szüksége (nekem például kb. ennyire van)? Mert két jelszónál még működhet ez a módszer, de ne mondja nekem senki, hogy fél évente változó teljesen random jelszavakból 20-30-at fejben tud tartani (autisták nem számítanak :))!

Szóval mi erre a megoldás? Nem szónoki a kérdés, nagyon kíváncsi vagyok, hogy a "hivatalos" álláspont mi, mert ha ésszerű és használható akkor én rögtön lecsapnék rá.

Válasz erre



[Csizmazia Darab István \[Rambo\] • <http://antivirus.blog.hu>](#) [2014.02.04. 11:17:32](#)

Szia Hvuk!

Én az egyedi jelszó híve vagyok, és szó sincs arról, hogy 30-at vagy 300-at kellene fejben tartani, sajna én nem vagyok Pataki Ferenc fejszámoló bűvész.

Én a legjobbnak azt tartom, ha ez egy titkosított dokumentumban van tárolva, ehhez pedig elég 1 azaz egy, one, agyin, ein, uno jelszó megjegyzése, ez nyitja mondjuk a Truecrypt, AES Crypt, Jetico vagy hasonló kötetedet.

Lehet aztán persze jelszómenedzsert is választani, én ezeket valami miatt kevésbé szeretem, talán mert már láttam rá támadási lehetőségeket, például:

www.esecurityplanet.com/network-security/keepass-security-flaw-found.html

De ott is csak egyet megjegyzel, míg n darabot meg tárolhatsz benne, szóval jelentősen egyszerűsíti és segíti az életet, és sokkal jobb, mint az azonos password mindehol, vagy a Postit a monitor szélén :-)

Válasz erre

[hvuk 2014.02.04. 11:44:45](#)

Köszí a tanácsot!

A titkosított dokumentummal az a gond, hogy több helyről netezik az ember ugye. Laptopról, mobilról, céges gépről, stb... Persze viheti az ember magával pendriver-on a titkosított fájlt, de azért ismerjük el, hogy ez nem az igazi, totál kényelmetlen módszer. További gond, hogy amikor megnyitod a titkosított fájlt egy open office-ban, akkor lazán lenézhető az _összes_ jelszabad a képernyőről. Nem beszélve arról, hogy sok helyen van biztonsági kamera, ami gyakorlatilag azt jelenti, hogy nem csak lenézhető, de még _fel_ is veszi_ egy kamera a jelszavad. Oké, ez lehet, hogy túlparázásása a dolgoknak, de eleve az egyedi jelszó megkövetelése is parázás. :)

Amúgy a legérdekesebb az, hogy dolgoztam olyan munkahelyen ahol az összes ügyfél összes általunk használt userid-ja és jelszava el volt tárolva egy olyan password vaultban, ami nem volt külön jelszóval védve (elég volt a céges hálón lenni vagy VPN-en keresztül bent lenni, bár ehhez kellett a céges jelszó). Én ezen elhültem, pedig nem vagyok egy biztonságmániás ember. :)

Válasz erre

[hvuk 2014.02.04. 11:45:56](#)

[@hvuk](#): "További gond, hogy amikor megnyitod a titkosított fájlt egy open office-ban"

ITt nem magára az Open Office programra gondoltam, hanem arra, hogy az iroda maga nyitott, magyarul "open office". :)

Válasz erre





Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu>

2014.02.04. 12:40:27

Hát én szigorúan ketté szoktam választani a magán és a céges dolgokat. Magán accountba sosem lépek be munkahelyi gépről, ehhez még megfigyelő kamera sem kell, csak egy proxy a számtechén, utána a rendszergazda és az, akinek hivatalból oda kell adnia, vagy csak odaadja, akkor lép be a nevedben, amikor akar, vagy ameddig ezt nem veszed észre.

Akkor legyen külön egy titkosított állomány csak a munkahelyi jelszavakról, amit felvehet a munkahelyi kamera, és nem gond, ha az egyébként a biztonságért felelő munkahelyi rendszergazda lát csak, ez így rendjén van.

A másik titkosított jelszó fájl meg a privát, nem céges telefonodon van, és ott szigorúan nem wifiről, hanem 3G-val nézegeted a magán dologaidat, akkor az átlagos jelszólopások ellen (nem a hárombetűsek ellen) védve leszel.

Árnyalja a képet aztán, ha valódi maximális biztonságra (ami nem is létezik) törekednél (pl. egy keresztapa vagy), akkor számos csapdát kell kivédeni - pl. nem lehetne Androidos telefonod sem, ami hazatelefonálja a Google szerverekre a wifid jelszavát, stb., stb.

Válasz erre



doggfather • <http://apengeele.blog.hu/> 2014.02.04. 12:50:47

van ám köztük nem egy olyan amit alig lehet elhinni, hogy bárki is komolyan gondol.

Válasz erre

Démonmac1 2014.02.04. 13:18:41

az adobe meg az i love you volt a két kivétel, amivel még nem találkoztam:) de az összes többi...

Válasz erre

nemjogasz 2014.02.04. 14:05:38

Szerintem ez a mindenhova egyedi atombiztos jelszót, amit havonta váltogatsz és soha nem írsz le, ez biztos nem működik.

Eleve biztonságos jelszót nem nagyon tudja megjegyezni az ember, ez már csak ilyen biológiai adottság, nem arra vagyunk tervezve, hogy 10 véletlen karaktert megjegyezzünk.

Ezért szerintem teljesen irreális dolog minden szírszarhoz atombiztos jelszót elvárni, meg a havonkénti váltogatást. Ez a módszer működött, amíg 2-3 jelszó volt az életünkben, ma már nem.

A jelszótároló program se jó megoldás, mert elveszhet a file, ha meg van róla biztonsági másolat, akkor az valószínű nem a legfrissebb. Ezenkívül ha több gépről dolgozunk, exponenciálisan nő a kockázat, hogy az egyik legalább fertőzött, és akkor oda minden jelszavunk. Úgyhogy szerintem a legjobb stratégia, ha kettébontjuk a jelszavakat: fontos és nemfontos. A fontosban halmazban legyen kevés jelszó, ezek legyenek "ideálisak", és tartsuk fejben őket. A nemfontosakat meg lehetnek egyszerűek, kit érdekel, ha pl. ezt az indapassomat feltörik? (Lehet próbálkozni, akinek kedve van:-)), lehet őket több helyen használni, vagy titkosítva tárolni, esetleg ne adj isten felírni. (pl. otthoni wifi jelszavát fel lehet írni, ha nem tartunk a családtagoktól, elvégre ha valaki bejut a lakásba, a legkisebb problémánk a wifijelszó lesz...)

Ha belegondolunk, mivel ma már napi rendszerességgel használunk "idegen" gépeket, lehetetlen kivédeni az evil maid attackot. Úgyhogy minden jelszót csakis ott használjunk, ahol kell. Pl. céges gépen magánjellegű dolgokat nem. Ismerősnél, vagy szállodából, netkávézóból és egyéb megbízhatatlan helyről meg céges dolgot sose, de még magánjellegűt se.

Válasz erre

szita szita péntek 2014.02.04. 16:34:07

Életszerűtlen, hogy az emberek rendszeresen új és új jelszavakat találjanak ki, jegyezzenek meg minden felületre - már az elvárás is badarság. Az esetek 99.9%-ában több energiát követel, mint amennyit a jelszóval védett adat ér. A maradék 0.1%-al meg bántunk óvatosan. (Bár megjegyzem, ha TÉNYLEG fontos az adat, akkor nem biztos, hogy pld. a neten egyáltalán fenn kell lennie.)

Válasz erre

Egy Hun Hunniából 2014.02.04. 16:34:23

Fiatal szőke csak a munkahelyen (hétfőn) telefonál a rendszergazdának:

-Gyere le nem tudok belépni a gépembe.

Helyszínen a rendszergazda kérdi:

-Mi volt a jelszavad amire emlékszel, hogy működött?

Válasz:

SEX!

Az ifjú rendszergazda nem is kérdezett többet ezek után!

(Megtörtént eset! Ha jól emlékszem csak a caps lock okozta a gondot ;-D)

Válasz erre

qwertzu 2014.02.04. 17:44:20

@hvuk:

keepass.info/

Én ezt használom.

Feltölti az ember egy online tárhelyre, portable progikkal együtt. Telepítesz egy szinkronizálót a használt gépeidre. Ha valami jelszó változik, akkor módosítod, mented, a szinkronizáló menti, az online tárhelyre. Valamint minden használt gépeden lesz egy offline lokálisan tárolt változat. Ha jól tudom vannak mobilos portok is.

" További gond, hogy amikor megnyitod a titkosított fájlt egy open office-ban, akkor lazán lenézhető az _összes_ jelszabad a képernyőről. Nem beszélve arról, hogy sok helyen van biztonsági kamera, ami gyakorlatilag azt jelenti, hogy nem csak lenézhető, de még _fel_ is veszi_ egy kamera a jelszavad."

A fenti progit használva nem lesz látható a képernyőn a jelszavad, ha nem akarod.

Válasz erre

hvuk 2014.02.04. 18:15:18

@qwertzu: Kösz, megnézem majd. De ugye az online tárhely sem az a tuti biztos megoldás.

@nemjogasz: Én az általad írtat követem jelenleg: kevésbé fontos helyekre egy egyszerű jelszót használok, fontos helyekre meg ha nem is véletlenszerű karaktereket, de legalábbis eléggé nehéz jelszót (kisbetű-nagybetű-írásjel-szám ezekben mind van).

Én egy kicsit a mobiltól parázok. Ha elhagyom akkor ugye az email kliensen keresztül lazán hozzáférnek a leveleimhez. Ok, jelszó védi, de azért azt nem egy igazán nagy nehézség feltörni. Innentől kezdve meg eléggé bukós a dolog.

Válasz erre

báró Csekonic 2014.02.04. 20:21:00

Szerintem itt is prioritásokat kell felállítani: pl. a netbank jelszava sokkal fontosabb (hogy ne kerüljön ki és ne is találják ki) mint egy fórum-jelszó.

Ennek megfelelően lehet egyedi v. több helyre azonos a jelszó és egyszerűbb v. bonyolultabb.

A gond ott van, hogy sokal a legfontosabb helyeken is egyszerű, kitalálható jelszavakat használnak - egyformát az összes helyen ráadásul.

Válasz erre

A CryptoLocker ellen a megelőzés a legfontosabb

2014.02.06. 11:46 | [Csizmazia Darab István \[Rambo\]](#) | [23 komment](#)

Címkék: [váltságdíj](#) [infografika](#) [cryptolocker](#) [filecoder](#)

A botnetek is nagy erővel terjesztik azt a zsaroló programot, amely adataink elkódolásával fenyeget bennünket. **Mit lehet tenni, ha egy ilyen kártevő bejutna a Windowsos gépünkbe? Erről rajzoltunk most egy szemléletes infografikát.**



Ennek az esélye jelentősen minimalizálható, ha az operációs rendszerünket, és alkalmazói programjainkat gondosan és időben frissítjük a megjelenő biztonsági javítófoltokkal, valamint valamilyen teljes körű internetbiztonsági csomagot is használunk. **Viszont ha mégis megfertőződünk, és a dokumentumainkat 2048 bites egyedi RSA kulccsal titkosította a vírus, úgy már nagyon nehéz bármit is tenni.** Meg lehet ugyan próbálkozni a rendszervisszaállítással, de egyrészt ez nem állít vissza teljes körűen minden adatot, másrészt a CryptoLocker újabb variánsai már képesek a Backup állományainkat is törölni, sőt célzottan vadásznak is a rendszer visszaállítás adatfájljaira. Egyes friss CryptoLocker verziók [a korábban még esetlegesen kikaput jelentő úgynevezett Shadow Copy fájlokat is megsemmisítik](#), sajnos még az elkódolási procedúra előtt.



Érdemes-e váltságdíjat fizetni? Lehet még esélyt adni az esetleges váltságdíj kifizetésnek, bár a biztonsági cégek ezt általában - az emberrablási esetekhez hasonlóan - nem javasolják. Ennek ellenére meg lehet próbálni a fizetést, hiszen az adatok értéke sokkal nagyobb, mint a hardveré, ha nem éppen pótolhatatlan. **Ennek lehetőségéről azt kell tudni, hogy ebben a helyzetben bűnözőkkel üzelünk, és ahogy a beszámolók egy jelentős részéből kiderül, hogy a fizetés ellenére sem történt aztán semmilyen pozitív változás.** Néhány esetben azonban valóban megjöhethet ez a működő feloldó kód, így maximum utolsó mentsvárunk lehet ez, de semmiképpen nem a nagybetűs bombabiztos megoldás.



Mindig győződjünk meg arról, ha a mentésünk elkészült, akkor azonnal le legyen választva a tároló eszköz a rendszerről, mert a nap 24 órájában csatlakoztatott külső merevlemez állományai ugyanúgy elvesznek, mint a helyi tartalom. **Emellett pedig készítsünk rendszeresen mentéseket csak olvasható formátumú adathordozókra is - például CD, DVD lemezekre.** Mind a megírt optikai lemezeket, mind pedig az esetleges külső winchestert a géptől fizikailag távol, védett környezetben ajánlatos tárolni. Egyes felhős tárhelyek is besegíthetnek a hatékonyabb mentésben, ugyanis számos ilyen felhős alkalmazás nem hagyományos betűjeles megosztásként viselkedik, hanem saját tárolási formátumban dolgozik, így ezekkel elkerülhető, hogy ott is adatvesztés történjen. **Azt sem szabad elfelejteni, ha mégis beütne egy esetleges fertőzés, akkor viszont haladéktalanul meg kell akadályozni, hogy a sérült adatok a továbbiakban felülírassák a korábbi tiszta mentési fájljainkat.**



Emiatt kiemelten fontos egy jó mentési szisztéma kiválasztása, megtervezése. **Tanácsos rendszeresen nem csak inkrementális (egymásra épülő), hanem időnként teljes önálló mentéseket is végezni, sőt ezek közül valamilyen logika és ütemezés alapján egyes adathordozókat nem felülírva azokat véglegesen is örökre megőrizni.** Legyen párhuzamosan több különböző verziónk is a mentésekből, ne kizárólag egyetlen kópia álljon rendelkezésre, amely rendszeresen felülírja az előző egyetlen mentésünket. Ha ugyanis mégis bejutna a fertőzés, akkor így hamarabb találunk korábbi sértetlen állapotot, és nagyobb eséllyel lesz miből válogatni. **A CryptoLocker kártevőt az ESET termékei Win32/Filecoder trójai néven detektálják.**

 **Tetszik** 63 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Magyarországra is megérkezett a CTB-Locker](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Védd a CryptoLocker terjesztőjének fejére](#)
[Gyorshajtási bírsággal is terjed a CryptoLocker](#)
[A CryptoWall bevétele átlépte a milliós határt](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5801059>

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](#).

[Illés Dávid 2014.02.06. 21:30:23](#)

najó, ez nem kicsit para :|
Válasz erre

[Ellensúly 2014.02.06. 23:37:10](#)

Egy nyelvi ellenőrzés nagyon nem ártott volna. Windowsos nagy W-vel, ezért általános iskolában karó jár.
Válasz erre



[Csizmazia Darab István \[Rambo\] • <http://antivirus.blog.hu> 2014.02.07. 06:29:54](#)

Akkor ezennel bevéstem a karót az ellenőrzőkönyvembe ;-) Így tuti, hogy nem kapom meg a bicklit a tanév végén :-)
Válasz erre



[enpera • <http://uborkakonzerv.blog.hu/> 2014.02.07. 09:01:17](#)

Szerintem jó, hasznos cikk. Bár engem nem fenyeget ilyesmi, mert nem használok W kezdetű rendszert, de többeknek hasznos.

És a vége az igazán fontos, MENTENI MENTENI MENTENI :)
Válasz erre

[JB242 2014.02.07. 10:53:54](#)

USB eszközökkel hogy terjed pontosan?
Válasz erre



[Jokkura 2014.02.07. 12:27:31](#)

"...esetleges külső winchestert a géptől fizikailag távol, védett környezetben ajánlatos tárolni."
nem is tudtam, hogy egy ilyen vírus 3 pozdorja polcon is átrágja magát :), ezentúl majd a nagyí vidéki padlásán fogom tartani, talán az a cirka 200km elég távol lesz
(értem, hogy ne legyen állandóan kapcsolatban, de ez nem egy nátha vírus, hogy az egy légtérben is fertőző legyen)
Válasz erre

[nemjogasz 2014.02.07. 13:18:11](#)

@Jokkura:

Ez az ITsek biztonságmentési litániájának része. Gyakorlatilag minden IT-s könyvben szó szerint ugyanúgy leírják, hogy ne tartsd a biztonsági mentést közvetlen a gép mellett, mert ha tűz/hurrikán/beázás/rablás/ufótámadás stb van, az is elveszik a géppel együtt. Ha az ember elolvas néhány ilyen könyvet, utána szinte pavlovi reflexként vágja rá a fenti szöveget a biztonsági mentés szóra.
Úgyhogy gondolom megszokásból írta így:-)

Válasz erre



[Hurrá Torpedó • <http://www.youtube.com/watch?v=br-D7UneS0E> 2014.02.07. 13:27:47](#)



ertem én hogy menteni, de nehogy már egy otthoni usernek több terás backup rendszert kelljen fenntartania.

van valami ajánlott mód is, vagy csak annyi hogy vegyek egy 2-3 db egyterrás külső vinyót, és manuálisan mentegessek hetente egy teljes mentést, minden héten egy másik winyóra? és persze ugye ez sem 100%. Nem ártana, ha ezekből 1-et nem otthon hanem munkahelyen tárolnánk. Ez rohadt macerás, és elég költséges megoldás ám. Egy ilyen rendszer használatához kb 75e Ft kellene, de lehet hogy 100. plusz minden héten pár óra mentetetés, ami az otthoni gépek számától, és a menteni kívánt adatmennyiségtől függően akár 5-10 órát is igénybe vehet teljes mentés esetén.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.07. 13:40:41**

Szia JB242!

A korábbi csak trójai - azt hiszed valami hasznos, és te telepíted, kattintasz rá - forma mellettl lett egy újabb verzió, ami már számítógépes féreg. Ez ugye pedig már terjedni is képes, szemben a trójaival. Fejlődés, aminek nem örülünk, Részletek itt:

blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/

Válasz erre



Jokkura 2014.02.07. 13:47:10

@nemjogasz: ha tűz nem is tesz kárt benne, a tűzoltó biztos :)

ja igen én olvastam,hallottam,tanultam hogy több egymástól nagy (több száz km) távolságban levő objektumokban kell őrizni mentéseket, de azok a nemzetbizonsági adatokra vonatkoztak...

@Hurrá Torpedó: sztem e gy mezei felhasználónak elég, ha az oprendszer feltelepítése után csinál egy "szűz" mentést, aztán az adatairól 1-3-5 hetente (attól függ mivel dolgozik) csinál egy/kettőt/, mondjuk két helyre. Ha sok van ,akkor a csak a legrégebbit (amire biztos nem lesz szüksége) felülírja.

A legtöbb OTTHONi felhasználónak mi van a gépén ,pár családi kép ,videó (ami pótolhatatlan is lehet) ,azokat mentse gyakran,de azok nem több szz GB-k. A céges dolgokat(általában --nehezen is de pótolhatók), pl céges által finanszírozott külsőkre, DVD-re (estleg RW-re). Sztem ez a csoda vírus sem tud egy DVD-RW-t önhatalmúlág felülírni.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.07. 13:56:02**

Szia Jokkura!

Igen, jól mondja Nemjogasz, itt csak annyit jelent, hogy ne legyen csatlakoztatva, minden más esetben pedig, hogy a legjobb, ha fizikailag is máshol őrződ. Például ellopják a gépedes, akkor ha mellette van az USB vinyó, azt is viszik, annyi a mentesnek.

De a legerdekesebb sztori a 911-nél volt, az egyik toronyban lévő szerverek mentései a másik tornyban voltak (nem elég máshol), és egészen pontosan 30 perccel éltek csak túl a katasztrófát.

De Coppola bácsi sem tartotta meg 2007-ben a kellő távolságot, illetve nem csinált mentést:

antivirus.blog.hu/2007/10/01/missing_in_action_utkozetben_eltunt

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.07. 14:00:11**

@enpera:

Ahogy látod, ha van egy LAMP szervered - Winhez semmi köze - ha fel van mappelve egy másik Win alól, akkor ott elkódol.

Olyat is láttam már, hogy a Wines virtuális gép egy állandóra felhúzott Linux alatti shared folderben zúzta le a PDF, XLS-eket.

Szóval persze, Win, meg minden, de azért ez igazából egy jó figyelmeztetés mindenkinek.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.07. 14:06:20**

Szia Hurrá Torpedó!

Rég jártál erre :-)

Igazad van, magánembernek valóban nem kell terrás mentés, kevesebb is bőven elég, mondjuk vegyük 1 GB/év-nek a családi fotókat, azok nagyok - és nem lehet kapni a sarki boltban, ezért érték.

Én speciel 1988 óta vagyok programozó, minden eddigi munkám mosolyogva elfér 30 GB alatt. Nyilván a mentés ezt jelenti, csak a saját, pótolhatatlan adatokat, amit sehonnan máshonnan nem tudunk megszerezni, megvenni, letölteni, letorrentezni, újratelepíteni, etc.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.07. 14:08:13**

Na ezt még nem kérdezte senki, de már sajnos van 4096 bites kulcshosszal is CryptoLocker, nem mintha nem lenne elég a 2048 is :-)

Válasz erre

nemjogasz 2014.02.07. 14:59:09

Kérdés:

Mi van, ha a külső adathordozó hozzáférései engedélyét úgy állítom be, hogy lehetséges új könyvtárt és fájlt létrehozni, de a törlés és a hozzáfűzés viszont le van tiltva? Akkor elvileg a biztonsági mentést rá tudom írni, de törölni vagy átírní a benne lévő adatot már nem.

Vagy meg tudja kerülni a sima ntfs acl-t?

Válasz erre

TakerOne • <http://www.taker.hu> 2014.02.07. 15:02:06

"vegyük 1 GB/év-nek a családi fotókat"

Haha, 2014-ben? :-) Egy egynapos kirándulás alatt csinálók 1 giga fotót :-), és akkor még nem készült videó sem

Válasz erre



Hurrá Torpedó • <http://www.youtube.com/watch?v=br-D7UneS0E> 2014.02.07. 15:33:38

[@Csizmazia István \[Rambo\]](#):

köszönöm a kitüntetett figyelmet :)

remélem valami jót tettem amiért ennyire megmaradtam, és nem rosszat...

[@TakerOne](#): igen-igen.

az éves szintű produktum, képekből 10 GB körül van.

egy-egy privát projektmunka szintén GB méretű anyagot képes összehozni. az a bajom a biztonsági mentésekkel, hogy ha 2-3 hetente csinálom, és pont a mentés előtt ugrik el egy 75%-osan kész projekt akkor szintén morcos lennék. Napi mentésre nincs idő. Cégnél napi mentés van. 3,5-4 órát ment a szerver minden éjjel... Otthon ezt minden nap nem tudom kivárni, illetve nem győzném áramszámlával...

DVD adatmegtartási képességében nem bízik, hisz 10 éve is mindig a drágább lemezt vettem mert hogy az jobb, de ma ugyanúgy nem tudok olvasni néhány fájlt róla. (Igaz a lemez 90%-a olvasható, és nem minden lemez hibásodott meg).

Csak a mobilwinyó marad. De az meg sérülékeny mint az állat. Csak le ne essen, mert akkor ugrik 1T anyag.

Mondjuk alap hogy legalább van védelem a gépen, és nem nagyon warezolunk, és emailből sem töltünk le hülyeségeket.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.07. 16:42:40**

Szia TakerOne!

Jogos az észrevétel, megnéztem, és igazad van, ott a pont :-)

Akkor mondjuk átlagembereknek legyen kb. 5 GB/év, nyilván van akinek több, van akinek meg kevesebb. És az is igaz, hogy ez a mennyiség évről évre nő, szóval a mentés nagyon kell.

Válasz erre

JB242 2014.02.08. 17:38:19

[@Csizmazia István \[Rambo\]](#):

OK, de szintén valamilyen álcázott fájlként kerül rá a hordozható meghajtóra? Tehát csak akkor tudom megfertőzni vele a gépem, ha elindítom azt, amit rápakolt? Bár rövid google után látom, hogy az autorun.inf-et is szeretik megfertőzni, de azon kívül van még valami?

Bocsi, sajnos picit lemaradtam a dolgok követésében... Még a boldogabb idők "boot vírus / fájl vírus" felosztásával még képen vagyok. A trójai / férgek dolgokból már csak annyit tudok, hogy ne indítsam el az idegen forrású dolgokat, ezért is vagyok kíváncsi, hogy azért ez még mindig kell, ugye? Leszámítva persze autorun.inf, meg buta levelező ami automatikusan megnyitja a csatolmányt...

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.10. 08:21:41**

Kedves JB242!

Igen, például kapsz egy ilyen USB kulcsot, és autorun miatt automatikusan lefutva azonnal megfertőzheti a géped, ha nincs rajta védelem.

A trójai helyett terjedő férgek pedig azt jelenti, hogy innentől már nem csak ezzel az egyetlen fertőzött USB kulccsal fogod tudni a környezetet továbbfertőzni, hanem innentől kezdve bármilyen külső USB eszközzel továbbadod, és megpróbál ez terjedni.

Autorun ellen egyfelől a már említett vírusvédelem szükséges, másrészt érdemes letiltani az automatikus indulást, ha még esetleg nincs. És ez érdekes módon ez nem csak Windows, de Mac alatt is hasznos, mert ott is láttunk már autorunos történeteket, és alapértelmezetten ott sincs lekapcsolva.

Válasz erre

JB242 2014.02.13. 18:25:09

[@Csizmazia István \[Rambo\]](#):

Kedves Rambo!

Köszönöm a részletes válaszokat! Az autorun-os "cselen" (és persze azon kívül, hogy létrehoz / megfertőz egy filet az adott USB driveon), van még valamilyen más út, ahogy terjed?

Vagy az autorun kiiktatása és az exe-k el nem indítása / víruscan az indítás előtt valószínűleg elegendő védelmet ad?

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.02.18. 06:06:43**

A CryptoLockerrel kapcsolatban egyedül az Autorunos módról olvastam eddig.

Ezenkívül persze több olyan módszer is létezik a férgekprogramoknál, amiket későbbi verziók esetleg majd alkalmazhatnak, pl. saját SMTP motorjukkal elküldhetik magukat, vagy linkjüket a címjegyzéken szereplő embereknek, a terjedéshez hálózati kapcsolatokat kereshetnek, esetleg gyenge adminjelszót szó tárral törhetnek. Sajnos biztosan folytatódik a kártevő "továbbfejlesztése".

Válasz erre



[kasu 2015.01.29. 09:28:09](#)

[@Csizmazia Darab István \[Rambo\]](#): néhány rövid video 5-6 giga. Csak a nagyságrendek miatt mondom. Több száz egy utazás.

A másik, hogy ökörködtök, meg van, aki okoskodik, de lehet nem volt ilyen adatvesztős támadása. Nekem volt. Azt gondoltam biztonságban van minden, aztán kiderült mégsem. Úgyhogy nem kellene nagyarcozni a veszélyt. Miképp a betöréssel sem, az is volt, de szerencsére nekem nem súlyos kárral. Másokkal meg nagyon is, minden elvittek, nyilván nem a családi fotók miatt, hanem üveg borért a vinyó cserealap...

Válasz erre

Itt a kamu Look Back videó

2014.02.10. 10:48 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [social media videó facebook átverés back scanner look](#)

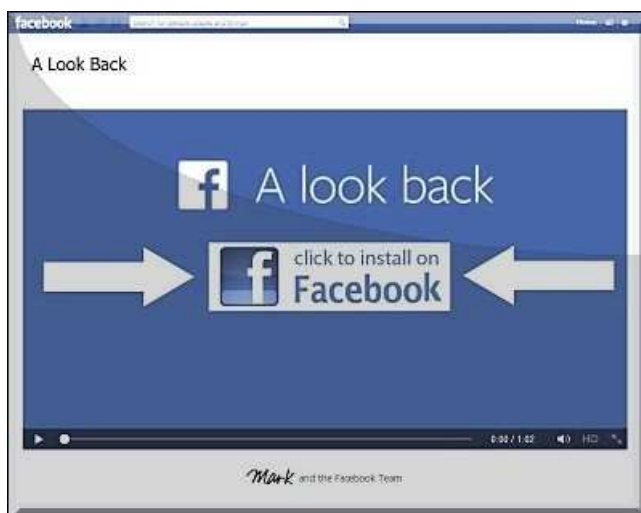
Ha azt az álnaiv kérdést kapnánk, soroljunk fel olyan nevezetes eseményeket, amiket aztán a bűnözők mégsem használtak fel csalnak spameknél, kártevőterjesztésnél, adathalászatnál vagy átveréseknél, nem sok ujjunkra lenne szükség. Volt már itt királyi esküvővel kapcsolatos átverés, Storm Wormos, izlandi vulkánkitöréses, és ezeknek se vége, se hossza. A legfrissebb módi ezúttal a hamis Facebook Look Back weboldal, ahol videó nézés előtt egy letöltést kérnek a naiv ügyféltől.



Mint az közismert (ugye hogy ugye Safranek?), a Facebook a tíz éves évfordulójára minden felhasználónak (nem, nem mindegyiknek, csak aki elegendő mennyiségű képet, videót osztott meg) készített egy ünnepi videót. Akinek van ilyen, megosztja másokkal, akik továbbosztják, és ez így megy. Ezzel kapcsolatosan például már [nagyszabású mémesedési folyamat is elindult például Putyinnal](#), de természetesen kapott ilyen [a Breaking Bad-es Walter White is](#).



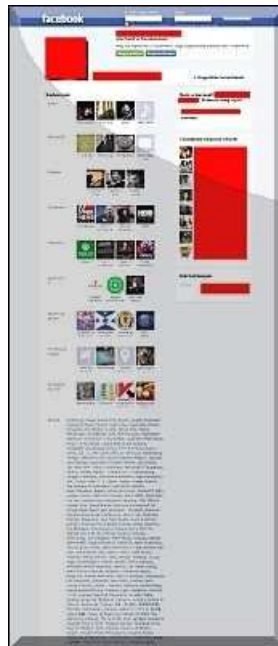
Ebbe a folyamatba próbál meg belesimulni az az új keletű átverés, amelyiknél [a támadók lemásolva az eredeti visszatekintős videó oldal \(https://www.facebook.com/lookback\) kinézetét](#), azt próbálják meg elhitetni a gyanútlan látogatóval, hogy a film megtekintéséhez előbb telepíteni kell egy állományt. Ilyen csalások gyakoriak voltak a múltban, sokaknak [emlékezetes lehet a kodek letöltőgetős történet](#), ami még Macintosh alatt is előfordult.



Természetesen ez nincs így, nem kell semmilyen extra letöltés a Look Back videó megtekintéséhez, ám akik a hasonló oldalon járva nem veszik észre, hogy nem a Facebook oldalán járnak, és valóban elhiszik, hogy telepíteni kell, [azok egy kártevővel lesznek gazdagabbak](#). A Facebook már korábban is remek terep volt mindenféle átveréshez, legutóbb például a "must see it" sorozatból [egy kivételesen sokkoló videó kapcsán írtunk posztot](#).



És nem lesz ez másként a jövőben sem, hiszen egyre több dolgot intézünk már hagyományos weboldalak helyett a közösségi oldalakon, itt keressük már a vicces képeket, [itt böngészünk új állás után](#), és egyáltalán nem ritka, ha valaki ezer feletti csoport kedvelőjeként innen informálódik szinte mindenről.



Ezért érdemes figyelmesnek lenni különösen a sokkoló videót ígérgetős linkekkel, emellett bevethetjük még az [ESET Social Media Scannert is](#), ami **szintén segíthet a kártékony tartalmak eredményes távol tartásában**.

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A Justin Bieber átverés](#)
[Így vernek át a Facebookon és így védekezz!](#)
[Itt a lopásvédelemmel ellátott Smart Security 6](#)
[Robin Williams utolsó telefonhívása. Vagy mégsem?](#)
[Hogyan védjük meg Twitter fiókunkat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5807415>

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.

Safer Internet Day 2014

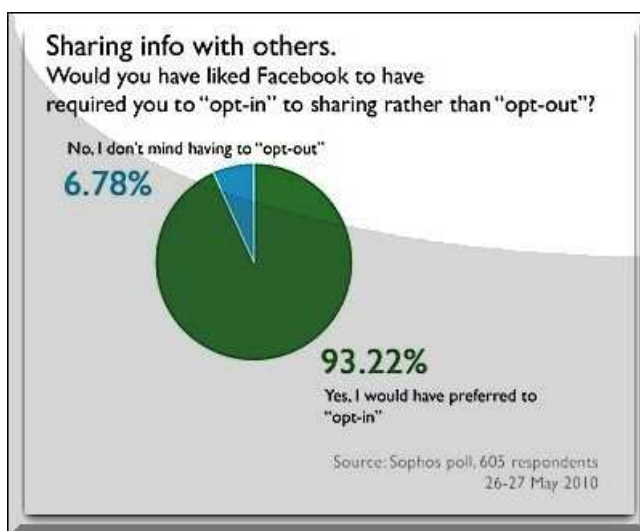
2014.02.12. 10:43 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [oktatás](#) [biztonság](#) [internet](#) [gyerekek](#) [kék](#) [day](#) [képzés](#) [2014](#) [vonal](#) [safer](#)

Tegnap volt a Safer Internet Day, ennek kapcsán pár dologról fontos megemlékeznünk. Emellett egy friss felmérést is idézünk, mely szerint nem használják ki eléggé a szülők a felügyeleti eszközöket, sőt tulajdonképpen kevesebb, mint 50%-uk kapcsolja be ezeket egyáltalán.



[Minden év második hónapjának második hetének második napja](#) a biztonságosabb internetről szól, gyermekeink védelme, internetes biztonsága kerül ilyenkor a fókuszba. Ennek kapcsán örömmel hallottuk, hogy a 13-17 korosztálynál (persze amennyiben valós adatokat adtak meg a regisztrációnál), az alapértelmezett Facebook biztonsági beállítások szigorúbbak, ésszerűbbek lettek: nem oszt meg automatikusan mindent, nem publikus a személyes adata, nem kereshető publikusan az adatlapja. Ezzel kapcsolatban érdemes felidézni azt a 2010-es szavazást, amely arról szólt, mi felhasználók mit szeretnénk: alapértelmezetten mindenki osszon meg mindent, vagy az legyen az alap, hogy semmit, és majd mindenki engedélyezi azt, ami megosztani szeretne. Na ki találja ki, mi lett az eredménye ennek? Nos 93%-ban az utóbbi nyert, vagyis hogy NE LEGYEN ALAPÉRTELMEZETLEN MINDEN MEGOSZTVA, de ennek ellenére azóta is ez a default állapot. Azért természetesen örülünk ennek a kis eredménynek is, hiszen legsebezhetőbb korosztályra nézve ez valóban hasznos változtatás.



Iskolai környezetben sajnos rendszeresen előfordul, hogy az ottani bántalmazásokról, vagy egyéb megalázásokról készített és internetre töltött képek, videók komoly lelki problémákat okozhatnak az áldozatoknak. A Safer Internet Day kapcsán ezért [érdemes lehet pár alapvető biztonsági tippet összegyűjteni](#), mire is érdemes figyelni nem csak ezen az egy napon, hanem mindig.

Korlátozzuk a Facebook profilunkat, hogy csak a barátok láthassák.

Csak olyan online felkéréseket, ismerősnek jelöléseket fogadjunk el, ahol valóban ismerjük, kedveljük az illetőt, és megbízunk benne. [Csak olyan tartalmakat töltünk fel, amiket nem szégyellnénk](#), ha nem csak a barátaink, de szüleink, ellenségeink, sőt tulajdonképpen az egész világ láthat.

[Ne adjuk ki lakcímünket, telefonszámunkat idegeneknek](#), és ne találkozunk egyedül a valós életben a neten megismert "ismerősünkkel"

Győződjünk meg arról, hogy a [mobil készülékeinken \(laptop, táblagép, okostelefon, stb.\) be legyen kapcsolva a jelszavas védelem, és az időzár](#).

Gyanús linkekre ne kattintsunk.

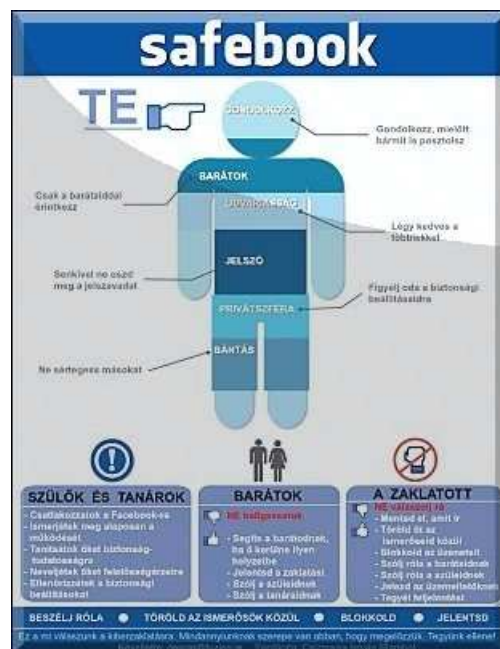
Ha szokatlan, furcsa üzeneteket kapunk az ismerőseinktől - például idegen nyelven, vagy egy üres üzenetet egy weboldal linkjével - figyelmeztessük, hátha nem is tud róla, például ellophatták a jelszavát.

Mindig szabályosan jelentkezzünk ki a használt banki, és egyéb online szolgáltatásokból, ne csak a böngésző ablakot csukjuk be. Ez

érvényes számítógépre ugyanúgy, mint okostelefonon és egyéb hordozható eszközökön is.

Használjunk **erős és egyedi jelszavakat, sőt akár jelmondatokat, hogy ne lehessen túl könnyen kitalálni**. Legyen benne kis- és nagybetű, szám és speciális karakter egyaránt.

Szóljunk szüleinknek vagy tanárainknak, ha az interneten durva, trágár, ijesztő vagy felzaklató tartalommal találkozunk.



Végezetül egy friss brit felmérés eredményét tekintjük át, eszerint **sajnos nem használjuk megfelelően a szülői felügyeleti eszközöket**: kevesebb, mint a szülők fele kapcsolja csak be ezeket egyáltalán. **Az adatok szerint a megkérdezettek 77%-a vásárolt gyermekének legalább egy internetkapcsolattal rendelkező eszközt a tavalyi esztendőben, azonban mindössze 45 százalék számolt be arról, hogy használja is azokat a szabályozó korlátozásokat, amelyeket az eszköz, az operációs rendszer, a vírusvédelmi program vagy maga az internetszolgáltató is nyújt erre a célra.** Sokan azt is elfelejtik, hogy ilyen szülői felügyelet nem csak a számítógépekben, hanem például a játékonkonokban is található.



Átlagosan 10 éves korra teszik a brit szülők azt, amikor a gyermek szerintük már önállóan, felügyelet nélkül is tud biztonságosan internetezni, és a szülők 45%-a soha nem beszélgetett gyerekeivel az online biztonságról. Sajnos a valóságban roppant sokféle hatás érheti őket, amikre egyáltalán nincsenek felkészülve, az átverések, megtévesztések is egyre rafináltabbak, de zavarba ejtő lehet az is egy gyerek számára, ha először találkozik a virtuális térben pedofillal, vagy ha a neten öngyilkosságra buzdító fórumcsoportot talál. Az biztos, hogy az internet valóban egy remek eszköz, és számtalan fantasztikus lehetőséget kínál, ám **fontos, hogy a gyerekek koruknak megfelelő módon mindig tájékozottak legyenek a fellelhető veszélyekről, és baj esetén tudják, kitől tudnak segítséget kérni: szülők, tanárok, Kék Vonal: 116-111 telefonszámon vagy a chat vonalon.**

Tetszik 3 személy kedveli ezt [Regisztrárl](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pinit** **g+1**

Ajánlott bejegyzések:

[Vigyázatlanok vagyunk a neten](#)
[2014 az internetes adatvédelemről szól majd](#)
[Az asszony a világ négere](#)
[Hogyan lehetne mégis segíteni nekik?](#)
[Miért romlik el minden?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5810740>

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 két dolgot is fontos leszögezni, az egyik a mindig hangoztatott menteni-menteni-menteni jótanács. Egy ilyen kritikusan, információkra, dokumentumokra kihegyezett cégnél a legalább napi szintű mentés egész egyszerűen elkerülhetetlen, hiszen a kiesés, az üzemképtelen állapot könnyen csődbe viheti az egész vállalkozást.



A másik dolog a váltságdíj kifizetése, amit egyik biztonsági cég sem javasol, és jó okkal. A rövidebb magyarázat szerint sok esetben ugyanis hiába fizet a kuncsaft, körülbelül 10% esélye van arra, hogy valóban kap a pénzéért működőképes privát kulcsot. A hosszabb magyarázat pedig kissé analóg az emberrablási ügyekkel: minél több esetben fizetnek az áldozatok, annál inkább bátorítják a bűnözőket az ilyen akciókra. És nem melleleg anyagilag szponzorálják a következő, még erősebben titkosító, még gonoszabb új verziót, ugyanis szakértői becslések szerint 2013. szeptembere óta mintegy 30 millió amerikai dollárnak megfelelő összeg folyhatott be a bűnözők kasszájába.

Tetszik 14 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Újra itt a CryptoWall zsaroló kártevő](#)
[A CryptoWall bevétele átlépte a milliós határt](#)
[Kisokos a Cryptolocker kártevő ellen](#)
[A CryptoLocker esete a rendőrséggel](#)
[De elfogadunk akár Bitcoin is...](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5813955>

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.

Figyelem! Szolgálati Közlemény!

2014.02.14. 09:10 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [szolgálati hírek](#) [lapszemle](#) [facebook](#) [közlemény](#) [rövid](#) [twitter](#) [szétválasztás](#) [google+](#) [antivirusblog](#)

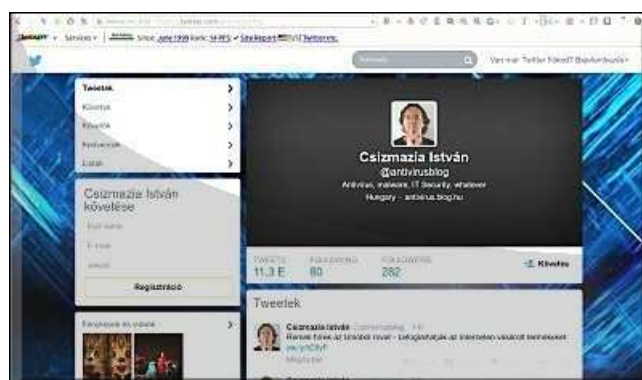
Rövid napi híreink, angol és magyar nyelvű lapszemlénk mostantól nem a személyes oldalon, hanem egy külön erre a célra létrehozott, www.facebook.com/antivirusblog oldalon lesznek elérhetőek.



"Kedves Mindenki! A korábban Csizmazia István Facebook magánfelhasználó nevében írt rövid biztonsági linkajánlóimat, magyar és külföldi vírus híreket mostantól a különválasztott www.facebook.com/antivirusblog oldalon fogom küldözgetni. Így ha a jövőben kölcsönkérném a fünyiródat, vagy felköszönténélek a névnapodon, azt magánemberként teszem majd, a biztonsági rövid híreket viszont ezentúl kizárólag az Antivirusblog nevében fogom írni. Így ha ez utóbbiakat a jövőben is szeretnéd olvasni, [kérek lájkold](#), kövesd, ajánld. Előre is köszönöm."



Az említett rövid híreink, angol és magyar nyelvű lapszemlénk, és természetesen az Antivirus.blog.hu posztjainak elmaradhatatlan ajánlóit az alábbi helyeken párhuzamosan jelennek meg. Így aki csak a Twitter szereti, ahhoz is eljut, és van Google Plus-os változat is, akkor most összefoglalunk:





2014.02.13-től erre változott a korábban 2011.07.29. óta használt személyes oldal:

<http://www.facebook.com/antivirusblog>



2012.12.26. óta végül, de nem utolsó sorban van Google+ is:

<http://plus.google.com/116981766824272539556/posts?hl=hu>

A levelezési címre is lett egy külön antivirus.blog.hu KUKAC gmail.com elérhetőség létrehozva, aki akar, ezen is tud kérdezni, fertőzést jelenteni, vagy cikktémát javasolni, esetleg csak simán virtuálisan gratulálni ;-)

Tetszik Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Így vernek át a Facebookon és így védekezz!](#)

[Ez történik a weben egy perc alatt](#)

[Nagy a forgalom a közösségi oldalakon](#)

[Tálcán kínált adatok](#)

[Napi 160 ezer Facebook account esik el](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5813740>

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.

Forbes és Kickstarter incidens - jelszócsere kell

2014.02.17. 14:37 | [Csizmazia Darab István \[Rambo\]](#) | [6 komment](#)

Címkék: [jelszó](#) [password](#) [forbes](#) [123456](#) [kickstarter](#)

Folytatódik a korábbi Adobe, Target, Snapchat, és hasonló cégek által évek óta zajló sorozat, megint újabb áldozatokat hekkelt meg. Ezúttal a Forbes és Kickstarter szenvedett el hasonló betörést, és fértek hozzá illetéktelenek az adatbázisokhoz, jelszavakhoz, címekhez. És mit tanultak ezekből a felhasználók az évek során: sajnos nagyon úgy tűnik, semmit sem.



A Kickstarter esetében a támadók nemcsak belépési adatokhoz - név és jelszó - fértek hozzá, de a felhasználók további elérhetőségei, postacím, telefonszám is kiszivárogtak egyúttal. Itt szerencse a szerencsétlenségben, hogy szakszerűen titkosítva voltak a jelszavak - SHA1 és a beszámolók szerint volt benne SALT is, és [bár elvben visszafejthetők megfelelő számítástechnikai kapacitás birtokában](#), azért **aggódnunk leginkább azoknak kell, akik vagy nagyon gyenge, rövid - értsd bruteforce vagy szótáralapú támadással percek alatt törhető - jelszót választottak, vagy pedig elkövétték azt az alaphibát, hogy több helyen is azonos jelszót használnak.**

PASSWORD LIST USED (MODIFIED "ADOBE TOP 100")					
123456	123456789	password	forbes123	12345678	qwerty
1234567	111111	news	123123	1234567890	000000
abc123	1234	forbes1	f0rb3s	azerty	iloveyou
aaaaa	654321	12345	666666	sunshine	123321
letnein	monkey	asdfgh	password1	shadow	princess
dragon	forbesforbes	daniel	computer	michael	121212
charlie	master	superman	qwertyuio	112233	asdfasdf
jessica	1q2w3e4r	welcome	1qaz2wsx	987654321	fdsa
753951	chocolate	f--kyou	soccer	tigger	asdasd
thomas	asdfghjkl	internet	michelle	football	123qwe
xcvbnm	forbes2	7777777	maggie	qazwsx	baseball
jennifer	jordan	abcd1234	trustno1	buster	555555
liverpool	abc	whatever	1111111	102030	123123123
andrea	pepper	nicole	killer	abcdef	hannah
test	alexander	andrew	222222	joshua	freedom
samsung	asdfghj	purple	ginger	123654	matrix
secret	summer	1q2w3e	snoopy1		

A Kickstarter ki is küldött minderről egy biztonsági figyelmeztetést, amelyben elismerik a feltörés tényét, ebben azt állították, ezzel semmilyen hitelkártya adat nem került veszélybe. A bejelentést nem siették el túlzottan, hiszen csak szombaton közzétették azt, pedig még szerdán történt maga az incidens. És természetesen ahogy ilyenkor szokás, [azonnali jelszócserere buzdítják a felhasználókat](#). A cserénél érdemes [valamilyen erős jelszót választani, erről már annyit beszéltünk](#), hogy nem ezúttal nem is térünk már ki rá részletesebben.

"1";"admin";"\$P\$B/fY91yIvYnpDG5	7cefyM3cyZC1";"admin";"admin@forbes.com";
"2";"bcampeau";"\$P\$BxBoFTxyh1.U	Ta3tABZhaG4IIF8";"bcampeau";"bcampeauXXX@
"3";"bnelson";"\$P\$BcI3LOfuSbcov	0sqGOIqlxAQoL1";"bnelson";"bre .nelson@fc
"4";"dewalt";"\$P\$BAadvDzvbJHacH	adPeQeFIHlcp0";"dewalt";"david .alt@gmail
"5";"rkarlgaard";"\$P\$B550GtdQ.1	Yym/U1uRWi0xyI."; "rkarlgaard "rkarlgaar
"52";"dfisher";"\$P\$BC/8Zrq1JINc	c/j2Ih9Nkd//e30";"dfisher";"df .er@forbes
"7";"fdonner";"\$P\$BIBynAKkig/8D	rD2UG9dapE.DU0";"fdonner";"fdo .er@forbes
"8";"mozanian";"\$P\$B118c0oE54Sg	Yb9twy3TrPySiN1";"mozanian";"m .nian@forb
"9";"mherper";"\$P\$B5ynhF9r3WgQr	njFI/6e2c0qXZ."; "mherper";"mhe .er@forbes
"10";"bwingfield";"\$P\$BN3UjPcAc	pHn0b2VCuyabB100W."; "bwingfiel "; "bwingfie
"11";"clavin";"\$P\$BkFG73m1Pz4bN	kJABWdvjaT85V0";"clavin";"clav .XX@forbes
"12";"pmaidment";"\$P\$BMLT6E9I3t	iBw9DGNc2CsPm2ag0";"pmaidment" maidmentX
"13";"jbauer";"\$P\$B1nxk0F/LDUIND	nzLxXTRxnuKGQ/"; "jbauer"; "jbau .XX@forbes
"1013";"jefflz";"\$P\$B702Kz5uTrq	YvK8R64vvlKAU0Q0";"jefflz";"je .lz85@gmail
"15";"utanaka";"\$P\$B.rR1cqPD1Sd	7rUkNnt2K1LPcJ."; "utanaka"; "vt .uka@forbe

Azt zárójelben azért érdemes megjegyezni, ha a név, korábbi jelszó hash, levelezési cím és telefonszám kikerül, könnyen elképzelhető egy további olyan testre szabott és kifinomult célzott social engineering támadás is, amellyel éppen a mostani károsultakat igyekeznek majd megtéveszteni. Remélhetőleg nem leszünk tanúi olyannak, mint az Adobe-nál, ahol először 3 millió ellopott jelszót vallottak be, aztán jött 38 millió, végül beismerték, hogy forráskódok is a támadók kezére jutottak.



Ugrunk is a másik esetre, ami a Forbes-nál történt, ahol szintén véletlen felhasználók adatai kerültek ismeretlenek kezébe. Apró érdekesség, hogy Eddy Willems szerint a Syrian Electronic Army (SEA) mindössze egyetlen emberből áll, ám ezek szerint vagy nagyon hiperaktív az illető, vagy esetleg mégis többen lehetnek. Mindenesetre itt is késedelmeskedés volt az incidens bejelentésnél, emiatt aztán nyilvánosságra is hozták az ellopott jelszavakat, [1 millió meg is jelent egy kiszivárogtatott listán](#). A Kickstarterhez képest itt PHPass Portable segítségével készültek a jelszó hashek, és bár az eredetileg publikált weboldalról már nem érhető el, de torrentről viszont letölthető a 66 megás állomány, ennek birtokában el is kezdődtek már a visszafetések.



Nyilván itt is jön a szokásos remedy: azonnali jelszócsere, főleg ha korábban rövid és/vagy gyenge volt, illetve ha több helyen is ez szolgált a belépésre, de különben is. Ám mindezekén túl azt is érdemes felmérni egy pillantással, vajon tanultak-e valamit a jűzerek az utóbbi években, változott-e érdemben a jelszavazásztás biztonsága. [Ha csak a 2013-as adatokat nézzük, sajnos nem igazán kerültünk a siralmas besorolásnál feljebb, ami változás mégis történt, azt is leginkább csak a "password" és az "123456" helycseréje okozta az előző esztendő adataihoz képest. De \[ha a korábbi Adobe incidens kikerült elmés jelszavait vizsgáljuk: "adobeadobe" vagy "adobe1", sajnos itt is előjönnek a hasonló jelszavazásztási primitívsegek, mint például az analóg "forbesforbes" illetve "forbes1".\]\(#\)](#)

TOP SIX PASSWORDS CHOSEN BY RECENT FORBES JOINERS			
1 AOL	2 HOTMAIL	3 GMAIL	4 YAHOO
forbes1	123456789	123456	123456
987654321	forbes1	abc123	forbes1
michael	abc123	password	welcome
ginger	password	forbes1	tigger
forbes123	charlie	lqaz2wsx	superman
buster	abcd1234	111111	secret
Words common to all four "Top Six" lists shown in bold			
PASSWORDS RECOVERED FROM FORBES STAFFERS AFTER RECENT BREACH			
forbes1	45/524		8.6%
Welcome1	14/524		2.7%
forbes123	11/524		2.1%
forbes13	4/524		0.8%
test123	3/524		0.6%
changene	3/524		0.6%
(others)	42/524		8.0%
TOTAL	122/524		23.3%

Mivel mással is zárhatnánk, mint hogy [a jelszó érték, vigyázzunk rá](#). Cseréljünk időnként magunktól is, ha pedig a szolgáltató bejegyalogol ilyen betöréses pofonba, akkor pedig mindenképpen és azonnal végezzük el az igényesen.

 Tetszik 6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Lopott Minecraft jelszavak szivárogtak ki](#)
["Abc123" és "password" elemek vadászni](#)
[1 faktor + 1 faktor = 2 faktor](#)
[A jelszó ötven árnyalata](#)
[Csak technikai hiba volt a Twitteres jelszó reset](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5818644>

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/> 2014.02.18. 01:20:44

m.blog.hu/an/antivirus/image/201402/kic6.jpg

Ezt nem tudom értelmezni.

Például a gmail oszlopában lévő 1qaz2wsx az honnan került elő, mint a leggyakoribbak egyike?

Ez jelent valamit geekül? :)

Egyáltalán a címsorban felsorolt szolgáltatóknak mi közük a forbes-hez? Ilyen mail címmel regisztráltak, az alattuk lévő jelszavakat használták leggyakrabban?

Vagyhogyan?

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> 2014.02.18. 06:36:35

Az oszlopokban a könnyen kitalálható, visszafejthető jelszavak láthatóak. Az "1qazwsx" is egy jelszó, amilyen "qwerty" féle, ha megnézed, fentről lefelé húzza valaki az ujját kétszer, akkor lesz ez :-). Az, hogy a "forbes" több helyen szerepel, az pedig arra bizonyíték, még mindig sokan vannak olyanok, akik egyetlen jelszót választanak, és azt használják több helyen is, vagy ami még rosszabb, mindenütt.

Ugye itt a lényeg az lenne, ne válasszunk közös jelszót, és ne válasszunk túl rövid, gyenge jelszót sem. Például kikerülnek az ilyen támadások után a jelszó hashek, és elkezdjük próbálgatni most éppen a Forbes listánál - MD5-öt épeszű helyen már régen nem használnak - az alap buta jelszavak hashét legenerálni: abc, abc123, password, stb. a PHPass Portable-tal, majd megnézzük, hogy a keletkezett stringek szerepelnek-e a nagy listában. Ha egyezik, meg is van a jelszó, és aki nem cserélte a jelszavát, oda máris be tudnak lépni a támadók.

A jelszóválasztásnál még az is alaphiba szokott lenni, hogy egy cég dolgozói a saját cégük nevét is beleveszik a jelszóba, esetleg éppen csak megsorszámozzák, de ez messze van az erős jelszótól.

Válasz erre

Nemzeti Dohányos 2014.02.18. 07:10:02

Ilyen helyekre minek erős jelszó? Gmail, facebook, bank esetén alap az erős jelszó, de egy forbes esetén, mit is csinállok vele?

Kommentelek? Miattam aztán feltörhetik, inkább használok az ilyen helyekre egy egységes, ratyi jelszót, és a fontosakat megjegyzem, mint hogy mindet vezetnem kelljen valahol, gépen vagy papíron.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> 2014.02.18. 07:30:49

Van igazság abban, amit mondasz, de én ezt másképp látom: valaki a nevedben becommentel oda egy pedofil linket, egy rasszista megjegyzést, egy felhívást bombamerényletre, vagy valami hasonlót, akkor a munkahelyed szépen elköszön tőled, és sok erőfeszítés, ha nem éppen lehetetlen azt bizonygatni, nem te voltál. De ha sikerül is, eladhatod a házad az ügyvédi költségek miatt, és lesz egy hendikeppes "kabátlopási" ügy a múltadban.

Válasz erre

Nemzeti Dohányos 2014.02.18. 07:44:35

[@Csizmazia István \[Rambo\]](#): No ebben is van igazság :) Azért ehhez az kellene, hogy valaki hozzáértő célzottan engem támadjon, csak ezért lelopjon egy adatbázist, és a kommentet egy hihető ip-címről írja. Vagy valamit nem jól látok?

Amúgy a három havi jelszócsereével is ez a bajom. Van a fejemben néhány elég jó, sok karakteres random alfanumerikus jelszó. Szerintem kisebb kockázat ezt nem változtatni és sehova sem felírni, mint három havonta lecserélni, mert azt fel kellene jegyezni - legalább átmenetileg. Ezt sokkal nagyobb veszélynek látom, mégis sok rendszergazda rá van gyógyulva a gyakori jelszócsereére.

Válasz erre

álfirkász • <http://narancsosliba.blog.hu/> 2014.02.18. 10:55:04

[@Csizmazia István \[Rambo\]](#): a billentyűzet kissé meglepett, de igazad van. :)

Viszont az oszlopok kapcsán a fejléc az, amit nem értek.

Válasz erre

Nyerjünk 250 ezer eurót. Vagy mégsem?

2014.02.20. 13:04 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [kamu hoax social vagy lottó bill átverés gate mégsem engineering 419](#)

Itt az ideje, hogy [folytassuk egyik korábbi kedvenc posztunkat](#), jöjjön hát "A social engineering 1000 arca II.", amihez természetesen az is nagyban hozzájárul, hogy a megtévesztések egyre újabb és újabb furmányokat mutatnak be. A csalók fantáziája láthatóan kiapadhatatlan, de emellett azért szeretnek korábbi bevált trükköket is leporolni.



Ha már a közelmúltban amúgy is napirenden és címlapon volt a Microsoft az új vezérigazgató választása miatt, akkor jöhet is a "Bill Gate Lottó", amely minden hónapban 250 ezer eurót ad, vagy nem. [Sok korábbi hoax, átverés](#) közül érdemes visszatekinteni például arra, [amikor állítólag Bill Gates elosztja a vagyonát, újra :-\)](#) "Bill Gates most osztja szét a jövedelmét. Ha most nem reagáltok rá, később megbánhatjátok." Nagyjából hasonlóképpen vehető készpénznek ez az újabb próbálkozás is, miszerint Bill Gate (sic! nem is Gates-nek van írva, már ez is egy intő jel lehet) Nemzetközi Lottó Alapítványa kéri a részletes személyes adatainkat, hogy megnyerhessük az ehavi 250 ezer eurót. Ha valaki idáig mindent elhinne, annak is el lehetne gondolkodni azon, hogy vajon egy amerikai cég miért is nem dollárban, hanem euróban ad nyereményt egy francia nyelvű kértlen üzenetben.

Az is jól jöhet, ha valaki ismeri annyira a valóságot, hogy megértse, egyfelől **nem egy tipikus és ésszerű kapitalista milliárdosi viselkedés, ha a tőkés ingyen elosztogatja korábban nehezen szerzett vagyonát** - egy valódi szerencsejáték szisztéma persze, ami viszont a nyeremény reményében a játékosoktól befizetést szedne, már bőven lehetne nyereséges megkopasztó konstrukció. Másfelől **az sem mellékes, hogy a Microsoft volt vezérigazgatója alapítványának neve félperces googlizzással megtalálható, ennek valódi neve: "Bill and Melinda Gates Foundation".**



Aki nagyon ráér, játszhat még ilyen Füles rejtvenyűjságba illő nyomozgatósát, és könnyen rájöhet, hogy [a valódi Bill és Melinda Gates Alapítvány címe](#) (500 Fifth Avenue North, Seattle, WA 98109), míg az itt megjelölt ["215 Park Avenue South New York, NY 10003"](#) cím nem azonos, sőt Google Maps segítségével még a kamu címen üzemelő gyógyszerár képét is meg tudjuk nézni.



A teljesség igénye nélkül találhatunk még helyesírási hibákat is szelvényünkön, például "Sponzored by Microsoft" helyett "Sponzord by Microsoft" áll, ugye azt már mindenki álmából felébresztve fújja, hogy sok nyelvtani hiba az egyik fő árulkodó jele a hasonló csalásoknak. De ugyancsak érdekes részlet az is, hogy akkor miért egy izraeli sportbolt e-mail címéről kapjuk az üzenetet, ráadásul a mellékelt telefonszám előtt nem is az Egyesült Államok körzetszáma, hanem [a \(223\) az éppen a nyugat-afrikai Mali Köztársaságé, korábbi nevén Francia Szudán](#). És ugye az már tényleg csak hab a tortán, hogy egy 419-es csalás számai ebben az esetben ha nem is pont Nigériába, de valóban az afrikai kontinensre vezettek.



Röviden, ha valami túl szép ahhoz, hogy igaz legyen, nagy valószínűséggel nem is igaz. Ha valaki a szerencsejáték eltántoríthatatlan megszálottja, és eddig még esetleg komolyabban reménykedett a fenti nagy összegű nyereményben, jobb ha hamar lehűti magát valamivel. Ennél ugyanis már egy hétköznapi Totó szelvény is jobb esélyekkel kecsegtet, csak ki kell állni a Nyugati pályaudvar mellé, és nézni a szélső sávban szembejövő kocsikat. **Ha csak férfi ül benne, a meccs eredménye legyen 1-es, ha csak nő ül benne úgy 2-es, ha pedig férfi és nő is ül az autóban, akkor legyen X - ezzel valószínűleg többet lehet nyerni, mint a "Bill Gate" lottóval ;-)**

Tetszik 6 személy kedveli ezt Regisztrájl, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[LinkedIn meghívó. Vagy mégsem?](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Újabb adathalász kísérlet a Yahoo! ellen](#)
[Robin Williams utolsó telefonhívása. Vagy mégsem?](#)
[Ingyenes Rolling Stones jegyek. Vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5823864>

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](#).



[enpera](#) • <http://uborkakonzerv.blog.hu/> 2014.02.21. 09:48:58

Jó cikk, de aki ezeket beszopja, nem tudom sajnálni:)

Válasz erre

Ezeket a spameket kapjuk egész évben

2014.02.24. 10:41 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [spam naptár](#) [levél egész kéretlen évben](#) [infografika](#)

Rendszeresen visszatérő témánk a spam - ezek a zavaró, néha kártevőt is terjesztő, és különösen céges környezetben rettentően erőforrás pocsékoló rendszeresen érkező kéretlen szemétleveél halom - **amelyből főképp angol nyelven mindenki kap itthon is a postafiókjába.** Nem szeretjük, több-kevesebb hatékonysággal szűrjük, és sajnos még maga [Bill Gates sem tartotta be a nekünk tett ezzel kapcsolatos ígéretét](#): nem szüntette meg a spameket ;-)



Ha csak a pár legutóbbi kéretlen levelekről szóló bejegyzésünket nézzük, volt itt [fogyókúrás zöldkávés](#) történet, [LinkedIn meghívónak látszó](#), ám valójában Viagrát népszerűsítő üzenet, vagy éppen Zeus trójakat terjesztő [látszólag neves antivírus cégek nevében írt "frissítési felhívás" tárgysorral](#). Hiába lett az utóbbi időben rendkívül népszerű a közösségi oldalakon végzett spam is, azért a korábbi e-mailes forma sem halt ki sajnos, sőt él és virul.



Folytatjuk infografikás sorozatunkat, ezúttal egy meglévő magyarítottunk, amely szép szemléletesen mutatja be, hogy tulajdonképpen érdemi szünet nélkül, minden évszakban, minden hónapban kaphatunk a nyakunkba ilyeneket. Természetesen a rendkívüli események mindig jelen voltak, vannak és lesznek, hiszen minden alkalmat kihasználják a kampányok, [legyen az hamis halálhír](#) vagy pedig egy [igazi királyi esküvő](#). Ám ezek mellett van a szemétleveleknek egy fajta rendszeres ütemezése is, gondoljunk csak a Karácsony előtti hitel javaslatokra, az Új Évi virtuális képeslapokra, [a Valentin napi ajándékozásira épülő ajánlatokra](#) vagy a nyaralási időszakban kapott hamis repülőjegy visszaigazolási levelekre.



A mellékelt infografikában havi bontásban megtaláljuk a leggyakoribb spam témákat, természetesen [a készítőik itt elsősorban az Egyesült Államok ünnepeit, illetve általánosságban az angol nyelvterületen élő felhasználókra kihegyezett kampányokat](#) vették sorba, még ha ezekből a világ minden táján élők is megkapják az adagjukat, minket magyarokat is beleértve.



Mindenesetre érdemes megjegyezni, hogy bármilyen kecsegtetőek is legyenek a hamis termékajánlatok, legyen az akár olcsó Viagra vagy Rolex, gyors kölcsön vagy azonnali adó-visszatérítés, [Victoria's Secret 1000 dolláros](#) ingyen ajándék, [ingyen iPhone](#) - ami túl szép ahhoz, hogy igaz legyen, többnyire nem is valóságos: általában átverés, vagy kérdőívet kell kitöltenünk, illetve legrosszabb esetben kártékony kódot tartalmazó linket is kaphatunk.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Nindsák és samurájok](#)
[Ugye mi jó barátok vagyunk?](#)
[Casino Royale - Frissítve!](#)
[Legyen Ön is milliomos!](#)
[Eladó az e-mailcím gyűjteményem](#)

A bejegyzés **trackback címe:**

<http://antivirus.blog.hu/api/trackback/id/5829968>

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](#).

E

Az a félelmetes, hogy van még, aki ezeknek bedől.

Válasz erre

Vírusstatisztika - 2014 januári toplista

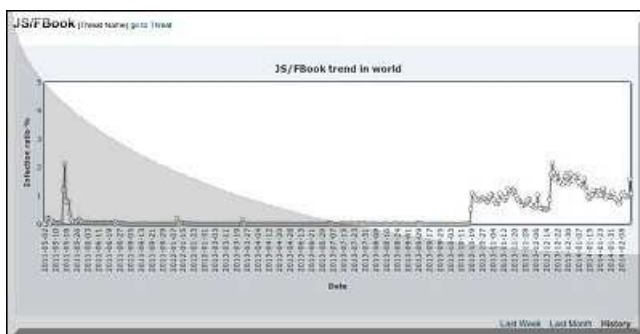
2014.02.26. 13:43 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [radar adatok](#) [január](#) [nod32](#) [havi report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. **2014. januárjában a következő 10 károkozó terjedt a legnagyobb számban.**



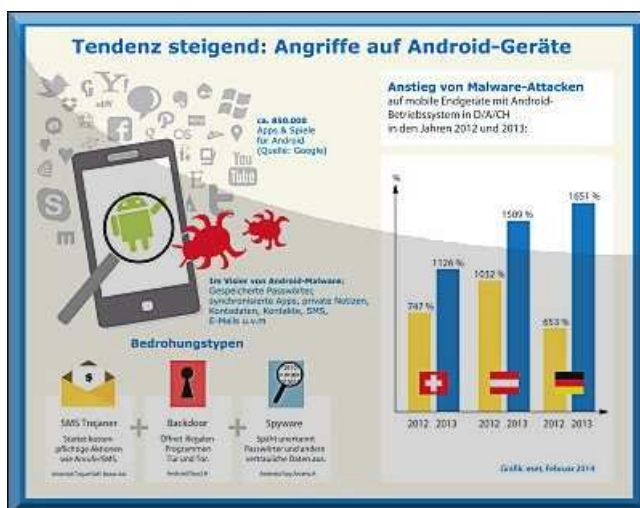
A lista első felében nem történt változás az előző hónaphoz képest, így **ismét az a Win32/Bundpil féreg vezeti a mezőnyt, amelyik külső adathordozókon terjedve valódi károkozásra is képes**, hiszen a meghajtóinkról mind a futtatható, mind pedig a mentési Backup állományainkat törölheti. Egyetlen újonc került fel a listára, a korábbi Win32/Trojan.Downloader.Wauchos trójait kiszorítva a top 10-ből. **A JS/FBook trójái célja, hogy kényszerűen pop-up reklámokat jelenítsen meg a számítógépen.** Nem hoz létre másolatokat magából, programkódja általában weboldalak HTML részében beágyazva található. Az utolsó pár hónap statisztikai adatai szerint jelenleg elsősorban a távol-keleti országokban észleltek kiemelkedő aktivitást, így Indonézia és Vietnam különösen fertőzött terület. **A kártékony linkek terjesztésében a Facebook is részt vesz, hiszen a különféle szenzációkat ígérő: például természeti katasztrófákról, közismert hírességekről szóló általában meglehetősen rossz minőségű tartalmat ajánló közösségi üzenetek itt is keringenek a hagyományos e-mailes spamek mellett.**



Az ESET Radar Report e havi kiadásában vezető helyen azokról a spamekről esik szó, melyek jellemzően inkább angol nyelvterületen terjednek, és az év eleji adóbevallási időszakot kihasználva különféle kedvezményekkel kecsegtetve ígérnek állítólagos megtakarításokat. Ezeknél például egy nagyobb vonzó összeget megjelölve arról értesítenek, hogy adó-visszatérítést kapunk, ehhez pedig mindössze a banki adatainkat kell megadnunk, illetve a levél mellékletre kell kattintanunk. Az is **bevett forgatókönyv** ilyenkor, hogy az hírnek megörülő áldozatokat egy hasonmás, adathalász webhelyre irányítják, ahol ha begépezi az összes személyes adatát, a bűnözők ezek felhasználásával hamis adó-visszaigényléseket adnak be a nevében, vagyis érdemes vigyázni.



A jó hírek között olvashattunk arról is, hogy a német nyelvű Android Magazine az ESET Mobile Security for Android terméknek ítélte a leghatékonyabb biztonsági alkalmazás címet, és ebben külön kiemelték a beépített lopásgátoló funkció használhatóságát. Emellett az AV-Comparatives megmérettetésén is sikerült a jó szereplés, amelyben az ESET Smart Security 7 bebizonyította, hogy méltó az úgynevezett "Gold Award" díjra. A hetes verzió többek közt az adathalászat elleni védelem továbbfejlesztésével is igyekszik a személyes adatainknak hatékonyabb védelmet nyújtani a banki csalások, és egyéb phishing módszerek ellen.



Januári fontosabb blogposztjaink között többek közt arról is megemlékeztünk, hogy **az első említésre méltó, szélesebb körben elterjedt és közismert mobiltelefonos kártevő a Cabir éppen tíz esztendeje, 2004-ben jelent meg.** Voltak ugyan előtte kisebb próbálkozások - például a spanyol Telefónica előfizetői körében terjedt az úgynevezett Timofonica még 2000 júniusában, de sem hatásában, sem ismertségében nem volt átütő erejű, inkább csak a PoC, azaz Proof of Concept kísérlete számát gyarapította. [A Cabir óta eltelt tíz év kapcsán viszont áttekintettük, miként fejlődtek a mobilos kártevők](#) az eltelt évtized során, mikortól jelentettek már komolyabb fejtörést, illetve veszélyeket.



Emiatt lehet aztán érdekes, hogy a leginkább elterjedt és emiatt **leginkább támadott Android platform kapcsán igyekeztünk minél több szót ejteni a biztonságról, így ezzel két posztban is foglalkoztunk.** Először [összefoglaltunk Androidos biztonsági tippeket](#) a hatékony védekezéshez, utána pedig a letölthető [alkalmazások engedélyeivel kapcsolatos nehézségekről](#), ezek figyelmesebb ellenőrzéséről is értekeztünk.



Figyelmet érdemel még az a **Facebookos átverés is, amely egy hátborzongató videót ígér egy állítólagos állatkerti óriáskígyós tragédiáról**, ahol [a csalás szerint egy gondozót evett meg a hüllő, ez persze nem igaz.](#) Ám ha valaki mégis rákattint, az összes ismerőse üzenetet kap a nevében, és az átverés egyre csak terjed, és terjed.



Egy friss felmérés eredményei azt mutatják, [nem igazán tesztünk meg minden tőlünk telhetőt azért, hogy óvjuk a biztonságunkat](#), így például azt is szomorú tényként könyvelhetjük el, hogy **a brit netezők több, mint fele egyáltalán nem telepít antivírust a gépére.**

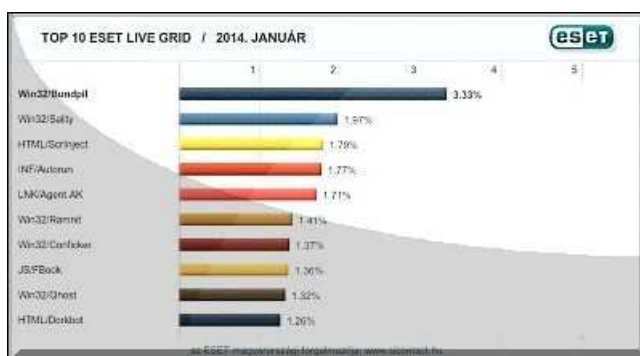


Végül pedig [egy igen érdekes támadási formáról is írtunk, ahol egy windowsos kártevő igyekszik megfertőzni az Androidos telefonunkat](#), ehhez egy hamis "Google APP Store" nevű, a hivatalos Google Play piactér ikonjával szereplő alkalmazást is telepít rá. Szerencsére a védekezés sem ördögösség, ehhez a telefon USB hibakeresési módjának kikapcsolt állapota, valamint számítógépünk vírusmentessége szükséges.



Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2014. januárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 17.29%-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.

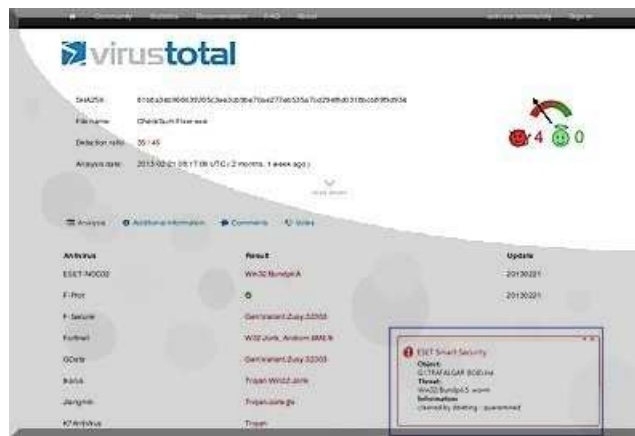


1. Win32/Bundpil féreg

Elterjedtsége a januári fertőzések között: 3.33%

Működés: A Win32/Bundpil 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. Win32/Sality vírus

Elterjedtsége a januári fertőzések között: 1.97%

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.



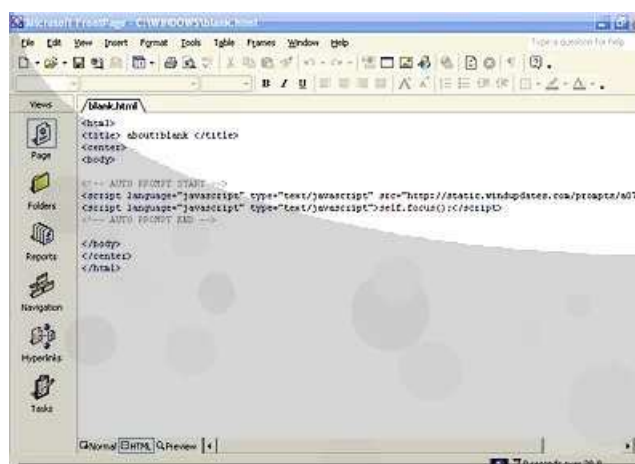
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



3. HTML/ScrInject trójai

Elterjedtsége a januári fertőzések között: 1.79%

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. INF/Autorun vírus

Elterjedtsége a januári fertőzések között: 1.77%

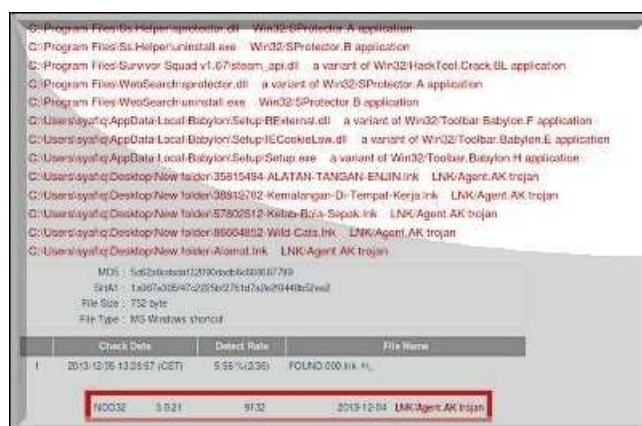
Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájl használó károkozónak. A kártevő fertőzésének

The screenshot shows a Windows XP desktop with a blue sky and green grass background. On the left side, there are four desktop icons: 'My Computer', 'My Recent Places', 'Documents', and 'Internet Explorer'. The 'Internet Explorer' icon is highlighted. In the center of the screen, a 'Windows Explorer' window is open, displaying the contents of the 'Local Disk (C:)'. The window title is 'Local Disk (C:)' and it has standard Windows window controls (minimize, maximize, close). The menu bar includes 'File', 'Edit', 'View', 'Favorites', 'Tools', and 'Help'. The address bar shows 'Address Local Disk (C:)' with a 'Go' button. The main pane shows a list of files and folders. The file 'autorun.inf' is selected, and its contents are displayed in the right pane. The contents of 'autorun.inf' are as follows:

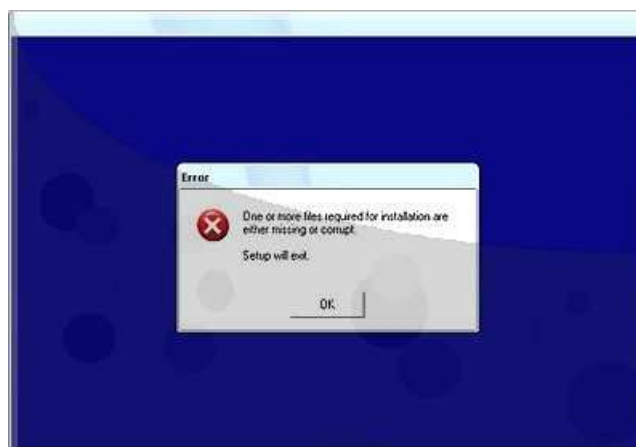
```
[autorun]
action=open drive
open=autoplay.exe OPEN
%comspec%\windows\system32\shell32.dll,8
shell\open=cmd
shell\open\command=autoplay.exe OPEN
shell\open\default=1
shell\explore=cmd
shell\explore\command=autoplay.exe EXPLORE
shell\autoplay=autoplay
shell\autoplay\command=autoplay.exe OPEN
```

At the bottom of the window, the file size is shown as '1 KB' and the date modified is '11/21/2007 6:53 PM'.

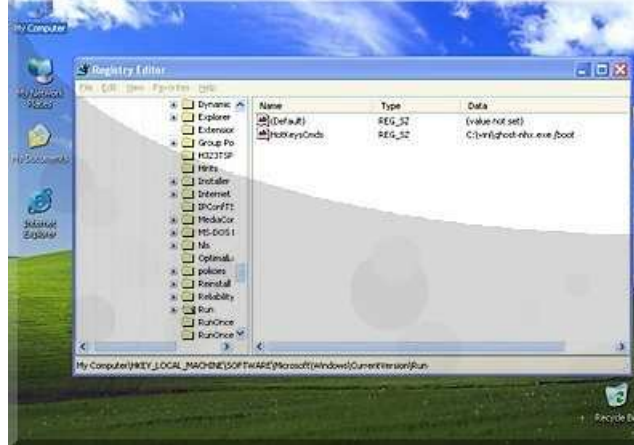
Működés: A LNK/Agent trojrai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokat fűzzön össze, majd futtassa is le azokat. Ez a technika legelőször a Stuxnet elemzésénél tűnt fel a szakembereknek, a 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.



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.



7. Win32/Conficker féreg



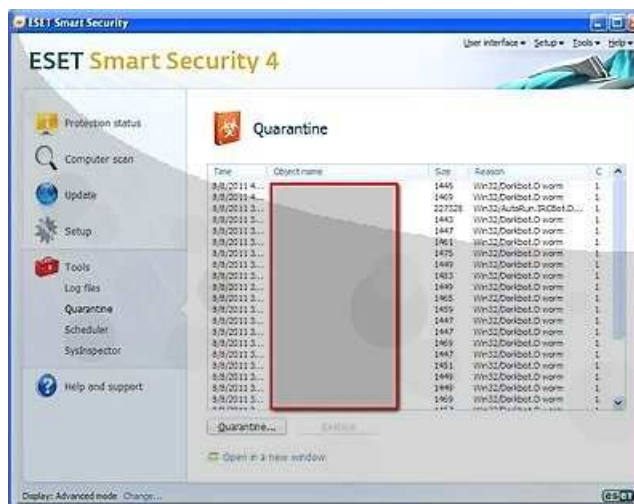
Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description



10. Win32/Dorkbot féreg

Elterjedtsége a januári fertőzések között: 1.26%

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

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Vírusostlista 2015. január hónap](#)

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[A HTML trójaiak riogattak minket októberben](#)

[Végre kiesett a Conficker féreg](#)

[Vírusostlista 2014. augusztus hónap](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5833664>

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.

Balek vadászat II.

2014.02.27. 10:22 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [letöltés torrent és fel átvérés bal kelt trójai ment lábbal cecelég](#) [A filestube Vegasba kelkáposztáért](#) [Glossina palpalis morsitans balek vadászat](#)

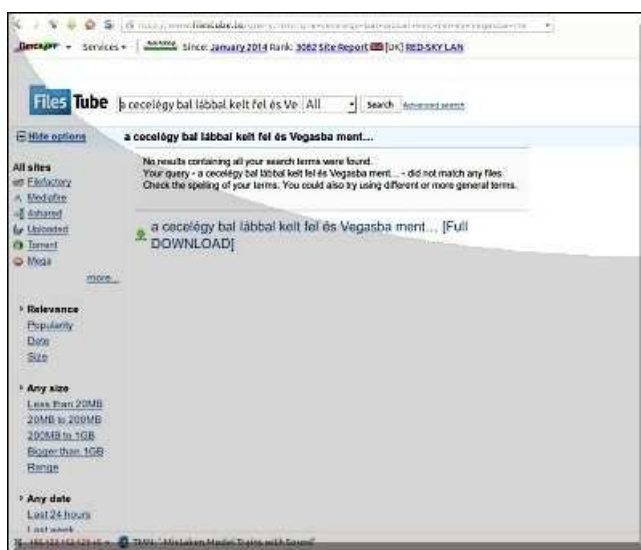
Évek óta vannak olyan kifinomult csalások, ahol szándékosan hamis, fertőzött csomagokat tesznek fel a torrent oldalakra, és még csak az sem érdekes, hogy létező dologról van-e szó. Magyarán nem kell a Photoshop, Microsoft Office vagy Adobe Indesign ahhoz, hogy sikerrel járjunk, hanem gyakorlatilag nincs olyan eszement karakter sztring, amit begépelve ne jönné "találat".



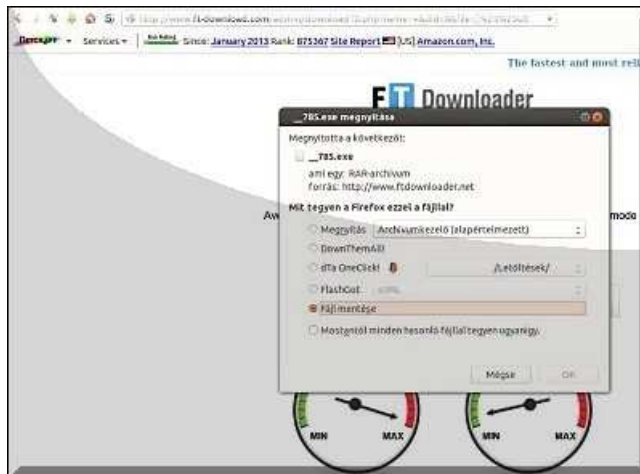
Ezt a játékot már eljátszottuk egyszer 7 éve, és úgy tűnik azóta sem szűnt meg, sőt jó módszer ez arra, hogy a naiv keresgélőket kéretlen reklámprogramokkal, kártevőkkel árrasszák el. 2007-ben véletlenül futottunk bele a jelenségbe, és akkor a "te egy hulye gorilla vagy" cím volt az, amire kerestünk. Nagy meglepetésünkre találtunk is, persze nem boldog letöltéssel végződött a történet, [akit érdekel, itt elolvashatja a régi sztorit](#).



Induljon akkor az új felfedezés, az újszülöttek kedvéért a Filestube pedig nem más, mint [egy olyan kereső, amely a fájlmegosztókon keres](#), és évek óta ismert a warezra vadászók körében.



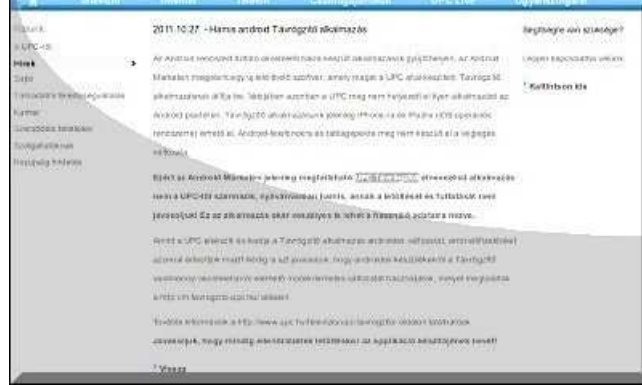
Gépeljünk be most a keresések közé valami különlegeset, lehetne ez persze "ashdfasdd76fas8fasjlkdj" is, de mi most a hecc kedvéért a következővel kísérletezünk: "A cecelég bal lábbal kelt fel és Vegasba ment kelkáposztáért". Reménykedünk, hogy filmet, szoftvert de akár zenei albumot földi halandó ezzel a címmel még eddig nem készített, és várjuk nagy naivan a keresés végeredményét, miszerint Breaking Bad, meg Walking Dead az biztos lesz, cecelég (latin nevén Glossina palpalis morsitans) viszont gyaníthatóan nem lelhető fel a repertoárban.



Na itt jön aztán az első meglepetés, hiszen mégis van találat, és a kattintás után már csak azt kell kiválasztani, az ingyenes lassú, vagy a fizetős klubtagsággal járó gyorsabb letöltést szeretnénk választani. Mi most - minő meglepetés - az ingyenesnél maradunk, és máris érkezik egy "__785.exe" nevű önkicsomagoló RAR állománynak hazudott fájl, elfogadjuk, letöltjük az ftdownloader.net oldalról, majd irány a VirusTotal weboldala.



Ilyen hosszú és cirkalmas bevezető után nyilvánvalóan senkit nem érhet váratlan meglepetésként az eredmény, **miszerint 48 vírusmotorból kilencen riasztanak rá**, ugyanis ez egy kártékony reklámprogram. Pár hasonlóan elmesé című FilesTube keresgélés után (pl. "Mennyit úszik anyád olajban százon égő ronggyal a szájában"), és Tádáááám, igen, azt is le lehet tölteni) után **jól látszik, hogy tulajdonképpen találat mindig lesz, és a dupla alávonás után rendre egy random szám nevű exe indul el a letöltési ablakban, amelyek VirusTotalos vizsgálata után pedig azt látjuk, bár az SHA256 hash minden egyes esetben különbözik, de szerencsére ez a felismerést nem befolyásolja**. Jönnek szépen sorban az azonos eredmények, benne ismételt a **Win32/Adware.1ClickDownload nevű kártevőnkkel**. Nyilván jobban pánikolnánk, ha mondjuk itt a CryptoLocker érkezne, de a kénytelen reklámprogramokat, amik melleleg ezen felül a weboldalak folyamatos átirányításával is manipulálják a böngészésünket, nos azokat is kellőképpen utáljuk.



A trükkök persze itt még korántsem érnek véget, hiszen nem csak az ilyen idióta keresések végződhetnek rosszul, hanem az értelmesebbek is és más helyszíneken úgy szintén. Gyakori eset, hogy neves, de egy bizonyos platformra még nem is létező szoftverek helyett tesznek fel trójaikat, ilyen volt például a [Foxit for Macintosh](#), de emlékezetes lehet a Google Play áruházba ismeretlenek által feltöltött [hamis UPC Távrögzítő alkalmazás](#) is. És hogy még egy jellemző módszert is említsünk, az is egy bevált átverési forma, hogy valamilyen nagyon várt új szoftver helyett még a megjelenés előtt hamisítanak egy fertőzött csomagot, [ez történt például a Blackberry messenger for Android esetében](#). Szóval mindig érdemes elővigyázatosnak lenni a letöltésekkel.

 Tetszik 10 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [G+](#)

Ajánlott bejegyzések:

[Új haladócsoporthoz Android kártevő](#)
[Hogyan szűrjük ki a gyanús Android appokat?](#)
[Kártevő az Amazon áruház nevében](#)
[BUÉK avagy Szerény ajándék karácsonyra](#)
[iTunes számla vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5834226>

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.

Angry Birds alkalmazásnak álcázott Mac malware

2014.02.28. 09:23 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [macintosh](#) [osx](#) [fertőzés](#) [warez](#) [trójai](#) [eset](#) [bitcoin](#) [welivesecurity](#) [cointhief](#)

Az OSX/CoinThief névre elkeresztelt trójai a Mac OS X operációs rendszerrel rendelkező számítógépeket fertőzi meg azzal a céllal, hogy bejelentkezési adatokat tulajdonítson el fertőzött böngésző alkalmazások telepítésével különböző Bitcoin csere és elektronikus pénztárca-oldalakon keresztül.



Az ESET arra figyelmezteti a Mac felhasználókat, hogy ne töltsenek le kalóz szoftvereket fájlmegosztó peer-to-peer hálózatokról, mivel **egyre jobban terjed egy a feltört alkalmazások által az adatainkat, főleg a Bitcoinjainkat veszélyeztető rosszindulatú program.** A szakértők kimutatták, hogy a CoinThief P2P fájlmegosztó hálózatokon keresztül terjed a következő **népszerű Mac OS X alkalmazások feltört változatain keresztül:**

- BBEdit – OS X szövegszerkesztő
- Pixelmator – képszerkesztő program
- Angry Birds – játékprogram
- Delicious Library – házikönyvtár



A CoinThief mögött álló hackerek próbálnak hasznot húzni a napjainkban zajló Bitcoin őrületből és befolyásolni az árfolyamot azáltal, hogy betörnek a felhasználók digitális pénztárcájába. Amint az ESET kutatói kimutatták, azok a Mac felhasználók, akik torrent oldalokról töltenek le és telepítenek illegális szoftvereket, nem csak megfosztják a fejlesztőket az őket illető jogos jövedelemtől, de saját számítógépüket és pénzügyeiket is veszélybe sodorják. **Az ESET LiveGrid statisztikai adatai szerint a fenyegetés egyelőre leginkább az Amerikai Egyesült Államok Mac felhasználóit érinti, de érdemes már most odafigyelni Európában is erre a trendre.**



A CoinThief rosszindulatú szoftvert először február elején észlelték a SecureMac kutatói, akik felfedezték, hogy a trójait olyan népszerű letöltő oldalak terjesztik, mint a Download.com és a MacUpdate.com, a Bitcoin Ticker TTM (To The Moon), BitVanity, StealthBit és Litecoin Ticker trójainak álcázva. Akár használunk Bitcoint, akár nem, minden Mac felhasználónak ajánlott egy aktualizált antivírus termékkel védenie számítógépét és ellenállniuk a feltört és illegális szoftverek letöltésének. Az OSX/CoinThief fenyegetésről még több [információt olvashat az ESET WeLiveSecurity](#) blogján, illetve a [kártévő részletes elemzését pedig itt lehet megtalálni](#).

 Tetszik Regisztrájl, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Amikor a marketing üzenet már kevés](#)
[A Tibeti Macintosh kártevő nem adja fel](#)
[Több változata is van az aláírt Mac-es trójainak](#)
[Séta a Macintosh kártevők kertjében](#)
[Újabb részletek a Flashback trójairól](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5836590>

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.

Adathalászat - egyetlen rendszer sem immúnis

2014.03.03. 13:39 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam átverés](#) [adathalászat óvatosság](#)

Lehetne persze "Humán faktor" is a címe a posztnak, lévén hogy általában az ember a leggyengébb láncszem a történetben. Bár az adathalász spamek egy része már megjelenik a közösségi oldalak üzenetforgalmában is, azért a hagyományos "Tesco gazdaságos" e-mail levelezés forma még mindig hihetetlen mennyiségben ontja nekünk ezeket.



Most elsősorban nem is a kétértelmű reklámokkal vagy a vírusos linkkel, esetleg csatolmánnyal érkező levelekkel foglalkozunk, hanem főképp az adathalászat felől közelítve vizsgáljuk a kérdést. Van ugye a klasszikus adathalász levél, amiben például személyes adataink megerősítésére kérnek mondjuk a bank nevében, ahol a mellékelt link egy hasonló oldalra vezet. **Itt lehet aztán az URL "[egypálcás](#)", vér primitív, vagyis első látásra is máshová mutató, amit az asztali gépen egér hoverrel vagy az internet security csomagunk adathalászat elleni védelmével is szépen leleplezhetünk.** No de ha mindez az okostelefonunkra jön, máris sokkal könnyebben lépre megy az ember.



Illetve van a "kétpálcás", kicsit már szofisztikáltabb megoldás, [ahol be- vagy újra be kell jelentkezni egy használt szolgáltatásba](#), és a megadott URL link is igyekszik hivatalosnak látszani, vagy egy betűcserés elütéssel (typosquatting), vagy pedig egy hosszabb link nevében szerepeltetve, elterelve a figyelmet a valódi domain végződésről. Itt asztali gépnél egyébként a biztonsági program és/vagy a levelező/böngésző még mindig figyelmeztethet minket, még akkor is, ha még nincs feketelistázva az adott csaló hasonló oldal. És akkor újra jön a kérdés, mi van, ha mindez az okostelefonunkra jön? Legyen az Android vagy iPhone, a kis kijelzőn nem látjuk a valódi linket, ahogy a háttérben esetleg futó scriptekről sem tudunk semmit, és [az adathalász hasonló bejelentkezési oldalt - legyen az akár AppStore, iTunes, munkahelyi rendszer vagy bármi - kis méretben valóban nem könnyű kiszűrni.](#)



A fentiekén túlmenően az adathalász levelek is folyamatosan okosodnak, még megtévesztőbbek lesznek, keresztül mennek egyfajta fejlődésen. Azaz, míg például korábban egy tipikus tört magyarságú formalevél mellett volt egy egyszerű link hivatkozás, **ma már egyre gyakoribb a nyelvtanilag helyes kinézet, amelyben egy állítólagos banki tranzakciónkra hivatkozva egy választási lehetőség szerepel** "Igen" pl. meg akarom nézni, mi is ez az állítólagos terhelés vagy egy másik "Nem" link, azaz kérem azonnal töröljék. Itt nyilván sokaknak nehezebb felismerni és elkerülni a csapdát. Ez [a fenyegetéses, sürgetéses forgatókönyv elég sikeres, mivel sokan közben annyira idegesek lesznek és felizgatják magunkat](#), hogy mégis kattintanak az átverős adathalász linkekre, fertőző mellékletekre.



Lehetnek még egyéb jelek is, például semmivel sem lesz hitelesebb egy kéréstlen levél attól, hogy mellette szerepel a cég igazi logója is, vagy egy létező telefonszám. Ahogy érdemes felkapni a fejünket arra is, ha bankunk vagy saját számítástechnikai osztályunk kér arra látszólag, hogy erősítsünk meg bejelentkezési jelszó adatainkat. Sokszor nincs szükség fenyegetésre és sürgetésre sem, hanem [elég valamilyen ajándékot](#) vagy kedvezményt ígérni, például [minden évben megkapják az angol nyelvterületen élők adó-visszatérítéssel kapcsolatos kéréstlen szemétleveleiket](#). Ilyenkor azt ígérik nekik, hogy azonnali adó-visszatérítést kapnak, ehhez nincs is más dolguk, mindössze a banki adataikat kell részletesen megadniuk, illetve a levél mellékletére kell kattintaniuk.



A statisztikák szerint Nagy-Britanniában az előző esztendőhöz képest 50%-kal nőtt az ilyen átverési kísérletek száma, vagyis az adathalászat szemmel láthatóan még mindig nagypályás megtévesztés, érdemes tehát mindenféle számítástechnikai - asztali, hordozható és mobil - eszközünkön résen lenni.

Megosztom [tumblr.](#) [Tweet](#) [Pin it](#) [G+1](#)

Ajánlott bejegyzések:

[Tíz dolog, amit a bankból sosem kérnek](#)
[Adathalászat a Google nevében](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Újabb adathalász kísérlet a Yahoo! ellen](#)
[Közelgő Karácsony, szaporodó adathalászat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5841273>

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.

Csak technikai hiba volt a Twitteres jelszó reset

2014.03.05. 12:09 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [tévedés jelszó password véletlen twitter reset](#)

Sokan meglepődve fogadták a hétfői Twitter értesítést, miszerint korábbi jelszavukat kinullázták, a következő belépéskor haladéktalanul változtassák meg. A tömegesen kiküldött üzenetek háttérében a szolgáltató szerint nem támadás, hanem műszaki probléma áll.



Zavar volt az Erőben, a hétfői tömegesen kiküldött levélből a felhasználók arról értesülhettek, hogy a [biztonsági probléma miatt korábbi Twitteres azonosítójukhoz tartozó jelszavuk azonnali visszavonásra került](#): "We've reset your password to prevent accessing your account". Az üzemeltetők általában - nagyon helyesen - biztonsági incidensek esetén gyorsan törölt jelszóval kívánják megakadályozni azt, hogy illetéktelenek tudják bejutni a kompromittálódott fiókokba. Az persze már egy más tésztá, és egyben mélyen szánalmas, hogy egy friss felmérés szerint a felhasználók 18 százaléka figyelmen kívül hagyja a jelzést, [ha az általa leggyakrabban használt online vagy közösségi oldal jelszócserére figyelmeztető üzenetet](#) küld neki.



Később azonban kiderült, most a jelzett biztonsági probléma minden valószínűség szerint nem külső támadás, hanem egy műszaki hiba lehetett. A Twitter azt ugyan [nem közölte, pontosan hány felhasználót érintett ez a téves riasztási incidens, de elnézést kért](#) a tévesen kiküldött jelszótörölések miatt.



Nem ez volt egyébként az első tévedésen alapuló jelszavas pánikkeltése a Twitternek, hiszen emlékeztet, hogy [2012. novemberében ugyancsak állítólag akaratlanul küldtek ki ehhez hasonlóan jelszótörölésről szóló értesítéseket](#). Ami után azoknak a felhasználóknak is kötelezően meg kellett változtatniuk jelszavukat, akik nem voltak veszélyben, illetve nem spameltek a feltört fiókjukból. A teendőket ilyenkor az is bonyolítja, ha a jűzerek valamilyen más csatolt szolgáltatáshoz is használják ezt a belépési accountjukat, ilvenkor minden egyes további helyszínen is át kell vezetniük az új jelszóra vonatkozó változásokat.



Ugyancsak érdekes eset volt az is, amikor internetes böngészés közben **2013. szeptemberében** 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. Akkor az derült ki, hogy a Twitter gomb HTML kódjába került bele valamilyen anomália, vagyis **a hiba nem a felhasználóknál, hanem magánál a Twitter webservernél volt**. Azok az oldalak voltak érintettek, ahol a híreknél lehetőség volt twitteres megosztásra. [A dolog szerencsére inkább csak váratlan volt, semmint veszélyes](#), és pár nap elteltével végül el is hártották.



Mindenesetre aki esetleg még nem tudná, az [antivirus.blog](#)unknak már 2009 óta van saját Twitter csatornája, amiben nem csak az éppen aktuális blogposztjainkat, hanem naponta folyamatosan friss, angol és magyar nyelvű gyors híreinket is szétkürtöljük, eddig már több, mint 11 ezer ilyen csiripelt rövidhírt küldtünk ki az éterbe. Ha valaki szeretné ezeket olvasni, vagy erre a hírfolyamra feliratkozni, az itt teheti meg: <http://twitter.com/antivirusblog>

Tetszik [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

Ajánlott bejegyzések:

- [A jó név félsiker](#)
- [Lopott Minecraft jelszavak szivárogtak ki](#)
- [Twitter bejelentkezés másképpen](#)
- [Vajon vannak-e hihető reklámok?](#)
- [1 faktor + 1 faktor = 2 faktor](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5844326>

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](#).

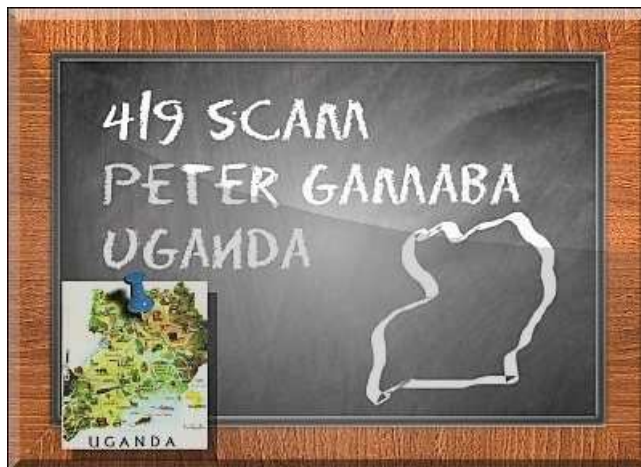
Nincsenek hozzászólások.

Már ilyen is van - ugandai 419-es átverés

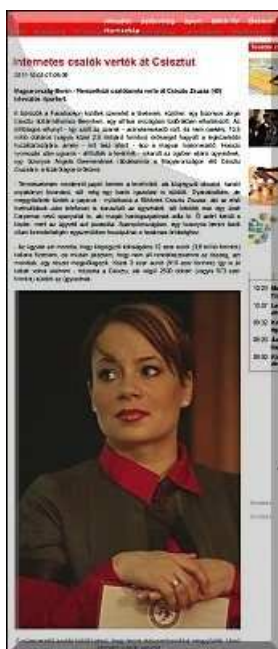
2014.03.07. 11:13 | [Csizmazia Darab István \[Rambo\]](#) | [5 komment](#)

Címkék: [spam](#) [homoszexualitás](#) [büntetés](#) [pénz](#) [csalás](#) [átverés](#) [uganda](#) [419](#) [kimenekítés](#)

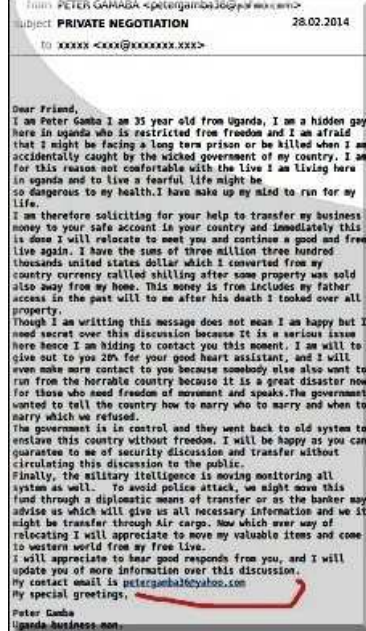
Gyorsak a kártevő terjesztők és a csalók, ha a friss történetekhez, eseményekhez kell igazodni, azokat frappánsan kihasználni. [Sorozatunk második részében](#) most szemlátomást az ugandai események ihlették meg őket, megérkezett ugyanis a gazdag afrikai üzletember/özvegy/király ki akarja menteni a vagyonát 419-es átverés aktuális átíratára.



Nem lehet eleget írni az ilyen csalásfajtákról, [korábban mi is egy teljes fejezetet szenteltünk a témának a Vírusok Varázslatos Világa sorozatunkban](#). Aki olvasta, vagy ha a klasszikus 419-es csalásokat valaki folyamatosan figyelemmel kíséri, annak visszaköszönnek az olyan trükkök, mint váratlan örökség, vagy a titkos vagyon kimentése - mindez egy "undisclosed recipients"-nek címzett szuper titkos e-mailben. [Van, hogy a 419-es csalásoknak semmi közük Afrikához, és van, amikor valóban onnan jönnek.](#)



Olyan ügyesen sebészi módon kiöltött csalással is találkozunk már, amikor az állítólagos elhunyt milliomos nevét szépen személyre szabják az áldozat számára. Így történt például Csizsztu Zsuzsával is, aki már célzottan egy olyan levelet kapott, miszerint örökös nélkül elhalálozott tüdőrákban egy bizonyos Jorge Csizsztu dollármilliomos az afrikai Beninben, [aki aztán bedölvén a csalóknak végül 2500 dollárt, akkori áron nagyjából 573 ezer forintot küldött ki előre "költségekre"](#) az örökség reményében az állítólagos ügyvédnek.



Mostani esetünk arra az ugandai eseményre reagál, mikor februárban Yoweri Kaguta Museveni ugandai elnök aláírta azt a **homoszexualitás büntetését drasztikusan szigorító jogszabályt**, amely alapján [az elkövetők akár életfogytig tartó börtönbüntetést is kaphatnak](#). Ennek nyomán biztonsági kutatók most olyan spamekre figyeltek fel, amelyeknél olyan személyek akarnak onnan elmenekülni, vagyონukat kimenteni, akiket az ottani hatóságok szexuális beállítottságuk miatt üldöznek. A petergamba36@yahoo.com címről érkező levélben arról panaszkodik egy állítólagos Peter Gamaba gazdag üzletember (na persze), hogy zaklatják, fenyegetik, fél a börtöntől és halálbüntetéstől, ezért szeretné kimenekítené a 3.3 millió dolláros vagyonát, amelynek 20%-át ajánlja fel nekünk gálánsan. Amely azért testvérek között is még mindig 147 millió jó magyar forintnak felel meg, csak előbb persze nekünk kellene előre utalni költségekre, és így tovább a szokásos ügymenet.



[Vices módon az eredeti cikkben kisatírozták a yahoos cím végét](#), míg a levél végén meg szépen ottmaradt :-). De az e-mail címre keresve a Google is egyből feladja a yahoo.com-os végződést, mivel [ez már egy jól ismert feketelistás](#) spam küldő. Összegezve: szemlátomást a kibebűnözők folyamatosan keresik azokat az új sablonokat, amelyekkel sikeresebben kelthetik fel az áldozatok szimpátiáját és persze vastagon építenek a kapzsiságra is. A legérdekesebb és egyben letragikusabb 419-es család cím elnyerésére mindenesetre valószínűleg jó eséllyel indulhatna az a korábbi történet, amelyben egy cseh nyugdíjast vertek át csalók hasonló módon még 2003-ban. [Aki aztán végső elkeseredésében az utcán agyonlőtte az ottani nigériai nagykövetség ártatlan - pénze visszaszerzésében egyre csak tehetetlenségét hajtogatató - konzulját.](#)

Megosztom [tumblr](#) [Tweet](#) [PinIt](#) [G+](#)

Ajánlott bejegyzések:

[Valentin nap: Szerelem helyett átverés érkezhet](#)
[Csaláselemlárlás fordított képkereséssel](#)
[Megtalálták az eltűnt maláj repülő! Ismét :-\)](#)
[Ismét nyertünk 450.000 eurót :-\)](#)
[Itt a foci VB, jönnek az átverések is](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5847883>

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](#).

[MP 2014.03.08. 00:09:00](#)

Már bocs de hogy lehet Cs. Zs. ennyire hülye? Ha én kapok egy ilyet s egy kicsit is hiszek benne ennyi pénznek a töredékéért felkérek egy kinti ügyvédet hogy nézzen utána.

Válasz erre



[nandras01 2014.03.08. 01:09:26](#)

aki bedől egy ilyen átverésnek, annak az a minimum, hogy megérdemli.

csisztun, pedig nem lepődök meg.

van olyan, hogy a pénzhétség legyőzi az értelmet.

Válasz erre



[Csizmazia Darab István \[Rambo\] • <http://antivirus.blog.hu>](#) [2014.03.08. 06:47:28](#)

Szia MP és Nandras01!

Nem ismerem közelebbről ezt az esetet, én is ugyanúgy csak a Blikkben olvastam róla.

De szerintem az a nyitja a dolognak, ha még nem olvastál a netes címlapokon olyan cikket, amiből tisztán tudod, hogy ez egy átverés, addig mindenki óvatlanabb. Erre jó példa az ATM automatás dupla fedél. Mióta is tapogatójuk, nézzük meg ezt alaposan, mielőtt pénzt veszünk ki? Mióta, hogy láttuk a cikkeket róla, hogy hűha.

A másik, hogy a módszer lényege éppen a fokozatos bevetés. Nyilván sok jómódú áldozatnak még ez is csak aprópénz, de mindig több lépcsőben, fokozatosan kérnek kisebb összegeket, éppen csak annyit, amire csak legyintesz, hogy ez még megéri. Ám a végén már "futsz a pénzed után", azaz ha eddig ennyit adtam, akkor ez a következő még belefér. Egészen a tűréshatárodig, vagy amíg nem olvasol a trükkről az Antivirus.blogon, és rájössz, clueless voltál ;-)

Válasz erre

[Erika Kelemen 2014.03.08. 07:38:09](#)

Pár éve én is kaptam emailt, egy szegény milliomos, örökös nélküli haldokló ápolónőjétől. Először még hittem is, aztán egy borzalmas fotó adott igazolást arról hogy csalás. A fotót már annak előtte láttam és ismerős volt.

Elmentem a levelezésben odáig, míg pénzt nem kellett küldenem.

Aztán nyomdafestéket nem tűrő szép emaillel fejeztem be a dolgot.

Azért halkan megsúgom, jó volt kicsit álmodozni.... :-D

Válasz erre

[Calibaan 2014.03.08. 09:04:02](#)

nekem most ősszel volt egy ilyen kalandom, örököltém valakitől. A családnév stimmelt, úgyhogy a vicc kedvéért belementem, kicsit csicskázattam a csókát, mindenféle további papírokat csináltattam vele, aztán mondtam, hogy a továbbiakhoz itteni hatósági papírokat is ki kell töltenie, és küldtem neki öt német nyomtatványt. Azóta nem jelentkezett, remélem nem történt valami baja :)

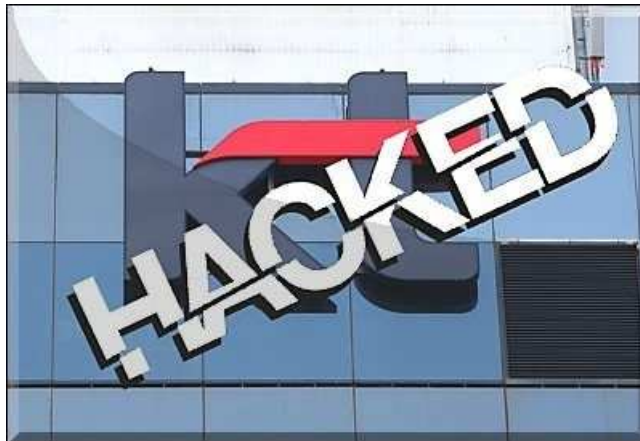
Válasz erre

Amikor 12 millió ügyféladatot lopnak el

2014.03.10. 16:39 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [telekom dél-korea](#) [hamis support távközlés](#) [adatlopás](#) [kt nagyüzem](#)

Nem akármekkora számú ügyféladat ellopásáról kaptunk hírt a napokban, a 12 millió egészen elképesztő. Az egyik dél-koreai távközlési cég, a KT Corporation adatbázisát ugyanis a gyanú szerint már 2013. februárjától kezdődően hackelték. Volt olyan, amikor egyetlen nap leforgása alatt 300 ezer személyes adat - név, lakcím, nyilvántartási szám és bankszámla információ - került így illetéktelenek kezébe.



A dél-koreai Yonhap hírügynökség jelentése szerint [három férfit már le is tartóztattak az ügygel kapcsolatosan](#), a gyanú szerint ők állhatnak a kis híján egy évig tartó adatlopás mögött. A [TheRegister véleménye](#) szerint két hackert és egy telemarketinges cég 37 esztendőes vezérigazgatóját gyanúsítják a cselekmény elkövetésével. A támadók állítólag saját készítésű programjukkal hatoltak be a rendszerbe, majd az adatokat eladták a csak "Park" néven említett telemarketinges főnöknek. A CNN szerint több, mint [10 millió dollárt kerestek](#) az illegális tranzakcióival.



A KT neve nem ismeretlen azoknak, akik a különféle támadások híreit olvasgatják, ugyanis két év alatt ez már a harmadik ilyen eset volt. 2012. márciusában a KT és az SK Telecom belső munkatársai adtak el egy telemarketinges cégnek 200 ezer ügyféladatot, míg 2012. júliusában pedig egy számítógépes feltörés folytán 8.7 millió felhasználó személyes adatainak kikerülése borzolta a kedélyeket. Akkor a KT állítólag komoly ígéretet tett arra, hogy megszigorítja a biztonsági rendszerét.



Dél-Koreában az utóbbi években több, még a mostani hackelésnél is jóval nagyobb szabású, és rengeteg ügyfél adatát kiszivárogtató incidens történt, például emlékezetes lehet a 2011-es SK Telecom Cyworld és a Nate webportál elleni támadás, ahol 35 millió ügyfél adata kerül ki, ez pedig óriási szám, hiszen ez nagyjából a teljes ottani lakosság háromnegyede. A most kipattant, immár sokadik hasonló ügy miatt a dél-Koreai távközlési minisztérium azt ígérte, részletes vizsgálatot fognak indítani. 24 órás forró drótot indítanak a

károsultaknak, és **mindenkinek felhívták a figyelmét, hogy fokozottan ügyeljenek az elkövetkező időszakban, mert várható, hogy e-mailben vagy telefonon csalók jelentkezhetnek a KT személyzete nevében.** Emellett az is egy érdekes kérdés, hogy a magyarországi incidensekről miért nem olvashatunk semmit, gyaníthatóan nem azért, mert ilyenek nem történnek.

 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A hamis antivírus halott és élvezi](#)
[Van új a nap alatt: hamis eBay live chat](#)
[I Tube, You Tube](#)
[Közös fellépés a support csalások ellen](#)
[Telefonos support vagy mégsem](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5852822>

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.

Google Glass a biztonságos bankoláshoz

2014.03.12. 12:16 | [Csizmazia Darab István \[Rambo\]](#) | [5 komment](#)

Címkék: [bank](#) [cebit](#) [atm](#) [hannover](#) [glass](#) [google](#) [University](#) [Saarland](#)

Egy Google Glass alkalmazás új lehetőségeket kínál az ATM bankautomatákból történő biztonságos készpénz felvételre. Nincs többé rosszindulatú PIN kód kukkolás, legalábbis ezt ígéri a hannoveri CeBIT-en bemutatott új applikáció.



A Google Glass okosság egészen pontosan úgy működik, hogy a feltelepített alkalmazás segítségével a szokásos PIN kód mellett egy extra QR kód is megjelenik majd, de a megfelelő digitális aláírással egyedül csak a tulajdonos lesz képes ezt a saját szemüvegével látni és értelmezni. Ha ezt nem gépeli be, nincs pénz kiadás. [Mivel csakis a párosított Google Glass számára lesz olvasható a kód, ezért hiába vesz fel valaki ugyanilyen szemüveget ugyanilyen alkalmazást telepítve, ő nem fog látni semmit.](#) A Saarland University által kifejlesztett konstrukció azért lehet igen hasznos, mert bár mindenki szeme láttára, a nyilvánosság előtt zajlik, mégis kizárja a kémkedési, leskelődési lehetőségeket - nyilatkozta Dominique Schröder, a kriptográfiai algoritmusok adjunktusa.



Természetesen a megjelenített kódok minden egyes alkalommal mások, és csak akkor generál a rendszer ilyet, ha maga a tulajdonos a regisztrált szemüvegével közelíti meg a bankjegykiadó automatát. Azért azt jegyezzük meg, amíg a szemüveg nem végez biometria ellenőrzést is, hogy pontosan kinek a fején van, azt el is lehet lopni, illetve maga a tulajdonos fegyverrel is kényszeríthető, hogy mégis gépelje be a helyes extra kódot. Továbbá, ha a pénzkidő nyílásra tesznek egy szokásos plusz záró műanyag fedelet, azzal még így is át tudnak verni pár tapasztalatlan felhasználót. Mindenesetre az ötlet azért izgalmas, hiszen a kód kifigyelése, kukkolása, levideózása ezzel eredményesen hatástalanítható. Majd kiderül, mi valósul meg belőle, [az Ubergizmo információ szerint még akár az idén megjelenhet.](#)



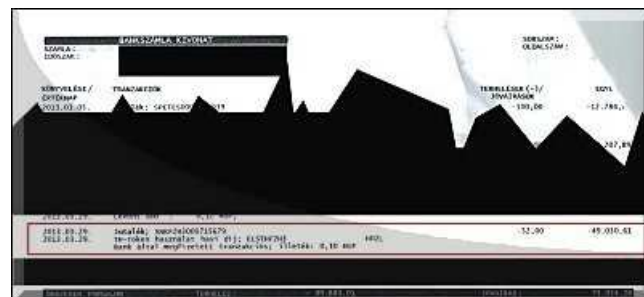
Biztonságos bankolással kapcsolatban úgy általában már eddig is sokszor és sokat értekeztünk, ha ezek közül a legfontosabbakat ki kellene ragadni, az egyik nyilván a Zeus botnet egy magyar bankok elleni átiratának megjelenése volt, ahol már tökéletes magyar helyesírással találkozhattunk. Az Erstebank.hu, a Budapestbank.hu, a Raiffeisen.hu, az Unicreditbank.hu és az Otpbank.hu ellen indított támadásnál az volt a veszélyes, hogy [a kártevő a memóriában manipulálta a megjelenítendő HTML oldalt, így nem okozott neki gondot az](#)



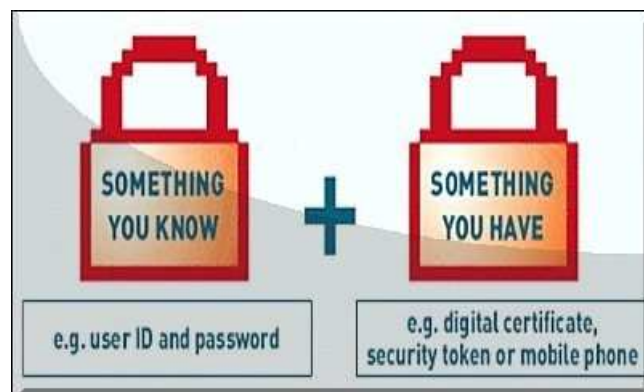
Ezenkívül szoktuk dicsérni [az úgynevezett virtuális kártyát](#). Ennek az az előnye, hogy bátran begépelhetjük, megadhatjuk a kártya számát, még az ellenőrző CVV kódot is, mivel mindig csak annyi pénz van rajta, amennyit mi 5 perccel a vásárlás előtt ráteszünk, így nem tudnak túlvonni, ellopni, és nem kell az "igazi" dombornyomott bankkártyánkat veszélynek kitenni.



Emellett meglegező javasolni szoktuk, hogy **ahol csak lehet, vegyük igénybe a két faktoros azonosítást**. Sajnos ezzel kapcsolatban azért érik időnként kellemetlen meglepetések az embert, például ha egyes bankok büntetik a biztonságtudatos hozzáállást, és úgynevezett "Jutalék - Token használati díj"-at szednek azoktól, akik élnek a lehetőséggel. Véleményünk szerint a legjobb az lenne, ha kiegészítő azonosítást mindenki használná, amit sokkal inkább egy "token nem használati" díjjal lehetne inkább serkenteni;-), de [semmiképpen sem szabadna büntetni az ezt már használókat](#).



És még egy apró gondolat ezzel kapcsolatban, **a mobilbankoláskor csorbul az eredeti 2 faktoros azonosítás (valami, amink van + valami, amit csak mi tudhatunk)**, hiszen azt úgy találták ki, hogy eredetileg egy fizikailag teljesen másik készülékre érkezzen a visszaigazolóshoz szükséges kód.



A klasszikus külön számítógépen bankolok és külön a telefonomra kapom a kódot modellnél ugyanis még a telefont is el kellene lopniuk (vagy kártevővel megfertőzni), ami azért egy újabb akadály, vagy legalábbis nehezítés. A kártevős verzió azért sajnos nem annyira sci-fi kategória, [már 2011-ben volt olyan Zeus Zitmo nevű trójai verzió, amely a fertőzött telefonon elfogta az SMS aláírási](#)

[üzenetet.](#)

 Tetszik Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Éljen soká az alapértelmezett jelszó 2.](#)
[Túlélőkészlet webáruházi adatlopások ellen](#)
[Tíz dolog, amit a bankból sosem kérnek](#)
[A játék neve: Carberp II. rész](#)
[Újra itt van a proxy-s Javascriptes kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5856112>

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](#).

[Jazo 2014.03.12. 17:39:25](#)

Mikor az OTP-től átmentem a K&H-hoz, nem értették, hogy mi az a virtuális bankkártya...sajnos azóta sem értik, így nincs is nekik.
Válasz erre

[Csumi84 2014.03.12. 23:10:54](#)

OTP-nél van talál virtuális kártya, viszont elég lehúzó bank. Mindenért pénzt vonnak le, és nem is keveset. A jelenlegi bankomnál meg nincs is ilyen, talán hallottak is róla már, de nincs elég nagy igény rá, így nem is tervezik bevezetni. Szép új világ :)
Válasz erre

[antyg 2014.03.17. 08:15:45](#)

[@Jazo](#): "nem értették, hogy mi az a virtuális bankkártya" Ez nem teljesen így van! Úgy hívják a virtuális kártyát az OTP-nél, hogy webKÁRTYA.

Válasz erre

[antyg 2014.03.17. 08:19:05](#)

[@Csumi84](#): A lényeg abban van, hogy a jelenlegi Bankodnál "Nincs is ilyen", ott is lenne díja hidd el az új dolgok fejlesztése és bevezetése nem kis pénzbe kerül! (az, meg hogy mennyibe kerül az más kérdés, nem ide tartozik!) Ha nem abban, akkor a számlavezetési díjban mutatkozna meg az újabb szolgáltatás díja.

Válasz erre

[Jazo 2014.03.17. 12:14:36](#)

[@antyg](#): Épp azt írtam, hogy az OTP-nél volt virtuális bankkártyám, de amikor átmentem a K&H-hoz, nem értette az ügyintéző, hogy miről is beszélek és a mai napig nincs ilyen náluk.

Válasz erre

Tartja első helyét a mentéseket törölő féreg

2014.03.17. 10:33 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [radar](#) [adatok](#) [nod32](#) [február](#) [havi](#) [report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. februárjában a következő 10 károkozó terjedt a legnagyobb számban.



A mezőny első felében nem történt jelentős változás az előző hónaphoz képest, így ismét az a Win32/Bundpil féreg vezet, amelyik külső adathordozókon terjedve valódi károkozásra is képes, hiszen a meghajtóinkról mind a futtatható, mind pedig a mentési Backup állományainkat törölheti. A Conficker féreg egyelőre csak gyengül, így bár e hónapban már csak a nyolcadik, de hosszú jelenlét után még mindig nem került le a top10-ről. Egyetlen újonc tudott feljutni a februári listára, a Win32/TrojanDownloader.Waski a tizedik helyen nyitott. Ez egy olyan trójai letöltő, amely egy fix URL listát tartalmaz linkekkel, és ezek alapján próbálkozik. Futtatása után bemásolja magát a helyi számítógép %temp% mappájába miy.exe néven, majd további malware kódokat próbál meg letölteni az internetről a HTTP protokoll segítségével.



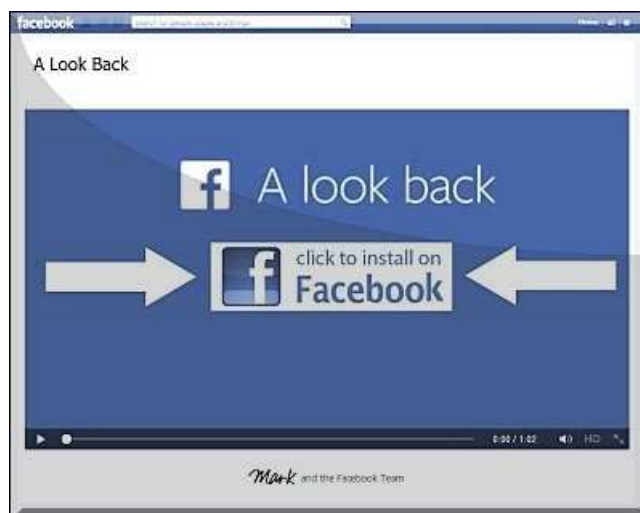
Az ESET Radar Report e havi kiadásában azokról a szűnni nem akaró adathalász támadásokról ír, amelyek kifejezetten bankolással kapcsolatosak. Az egyik ismertett trükk szerint a csalók olyan kéretlen leveleket küldtek szét, amelynek tárgya éppen a biztonsággal kapcsolatos, és bankkártya biztonsági szolgáltatást ígértek a brit banki ügyfeleknek. Az "RBS Credit Card Account Holder" azonban egyértelműen egy átverés. Bár azt állítják, hogy a gyanús tranzakciókat fognak kiszűrni, ehhez képest a spamet egy svédországi domainről küldték, az angol bankokban pedig semmilyen partneri, vagy együttműködési viszonyról nem tudnak ezzel az állítólagos szolgáltatóval.



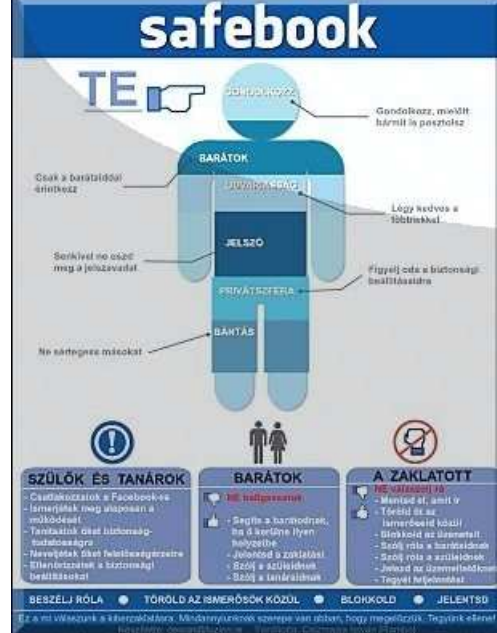
De kaphatunk kéréstlen levelet a híres Lloyds nevében is, ahol viszont annyira amatőrökkel van dolgunk, hogy tisztán látszik a küldésre használt valódi cím is, ami nem más, mint a toilet@ebay.com. A hamisított adathalász weboldal viszont elég jó másolat ahhoz, hogy a figyelmetlenek mégis begépeljék adataikat a hasonló oldalra. A módszer itt is régi, azzal próbálják meg a címzetteket a belépésre rávenni, hogy korlátozták számlájukat, és csak a linkre való kattintás után oldhatják fel ezeket az ideiglenes számla korlátozásokat. Bár arról nincs hír, konkrétan mennyien dőlnek be ezeknek, az mindenesetre reménykeltő, hogy **a rengeteg figyelmeztetésnek hála az emberek a banki csalásokra egyre jobban odafigyelnek - például a híradásokban. Mindenesetre mi újra elmondjuk, a bankok sosem kérnek ügyféladatokat e-mailben, és nem küldenek linket sem a belépéshez.**



Februári fontosabb blogposztjaink között többek közt azzal foglalkoztunk, [vajon elég felelősen bánunk-e a jelszavakkal](#). A látványos és tanulságos infografikából az is kiderült többek között, hogy a felhasználók 16%-a sosem változtatja meg a jelszavát, míg 18%-uk figyelmen kívül hagyja a jelzést, ha az általa leggyakrabban használt online vagy közösségi oldal jelszócserére figyelmeztető üzenetet küld neki.



Természetesen aktuális átverésekről is be tudtunk számolni, így ezúttal a [hamis Facebook visszatekintő Look Back hasonló weboldal került terítékre](#), ahol a videó megnézése előtt egy letöltéssel próbálták meg kártevőt juttatni a gyanútlan látogatók gépére.



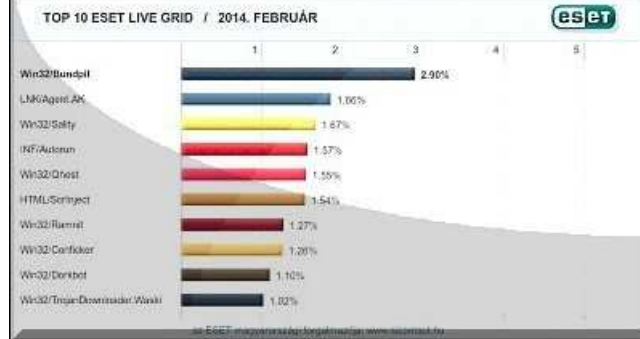
Kiemelten fontos téma gyermekeink internetes biztonsága, így minden év második hónapjának második hetének második napja a [Safer Internetről, azaz a biztonságosabb internetről szól](#). Ezen a főképp oktatással és képzéssel végezhető feladaton folyamatosan kell dolgoznunk, amire egy friss brit felmérés eredménye is jól rávilágít: eszerint sajnos nem használjuk megfelelően a szülői felügyeleti eszközöket: kevesebb, mint a szülők fele kapcsolja csak be ezeket egyáltalán.

PASSWORD LIST USED (MODIFIED "ADOBE TOP 100")					
123456	123456789	password	forbes123	12345678	qwerty
1234567	111111	news	123123	1234567890	000000
abc123	1234	forbes1	f0rb3s	azerty	iloveyou
aaaaaa	654321	12345	666666	sunshine	123321
letnein	monkey	asdfgh	password1	shadow	princess
dragon	forbesforbes	daniel	computer	michael	121212
charlie	master	superman	qwertyuio	112233	asdfasdf
jessica	1q2w3e4r	welcome	1qaz2wsx	987654321	fdsa
753951	chocolate	f--kyou	soccer	tigger	asdasd
thomas	asdfghjkl	internet	michelle	football	123qwe
zxcvbnm	forbes2	7777777	maggie	qazwsx	baseball
jennifer	jordan	abcd1234	trustno1	buster	555555
liverpool	abc	whatever	1111111	102030	123123123
andrea	pepper	nicole	killer	abcdef	hannah
test	alexander	andrew	222222	joshua	freedom
samsung	asdfghj	purple	ginger	123654	matrix
secret	summer	1q2w3e	snoopy1		

Nem került el sorsát a Forbes és Kickstarter sem, a korábbi Adobe, Target, Snapchat, és egyéb cégek elleni támadáshoz hasonlóan itt is illetéktelenek fértek hozzá az adatbázisokhoz, jelszavakat és címek loptak. Természetesen ahogy ilyenkor szokás, azonnali jelszócserére buzdítják a pórul járt felhasználókat.



És végül, de semmiképpen nem utolsó sorban beszámoltunk egy olyan [Mac OS X operációs rendszeren futó trójairól, amely elsősorban warez programok letöltésével terjed, és a megfertőzött számítógépekről Bitcoinot lop](#). Akár használunk Bitcoinot, akár nem, minden Mac felhasználónak ajánlott egy aktualizált antivírus termékkel védenie számítógépét, valamint tanácsos ellenállniuk a feltört és illegális szoftverek letöltésének.



Vírustoplista

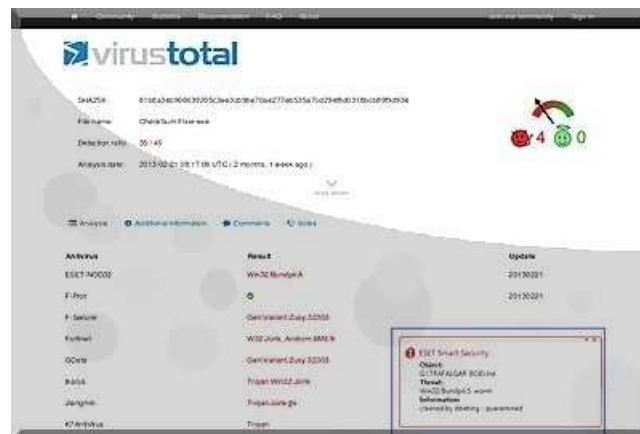
Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2014. februárjában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 15.74%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtevéséről, az **csatlakozhat** hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve emellett [az antivirusblog rövid híreire a Twitter oldalunkon](#).



01. Win32/Bundpil féreg

Elterjedtsége a februári fertőzések között: 2.90%

Működés: A Win32/Bundpil 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.



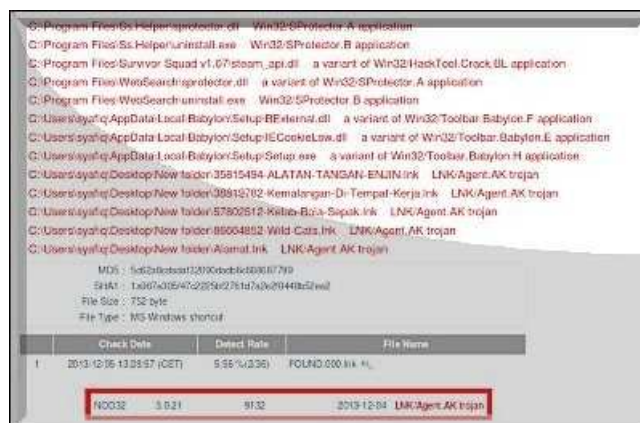
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



02. LNK/Agent trójai

Elterjedtsége a februári fertőzések között: 1.86%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatot futtasson 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. Vírusselemlők 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



03. Win32/Sality vírus

Elterjedtsége a februári fertőzések között: 1.67%

Működés: A Win32/Sality egy polimorfikus fajlfertőző vírus. Futtatása során elindít egy szervíz 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 szervíz folyamatokat.



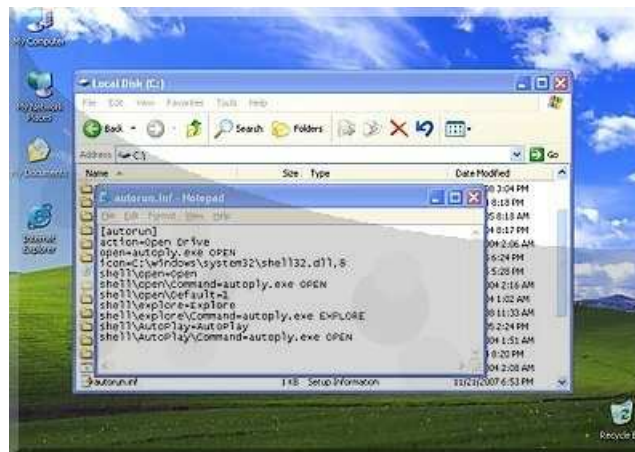
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



04. INF/Autorun vírus

Elterjedtsége a februári fertőzések között: 1.57%

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



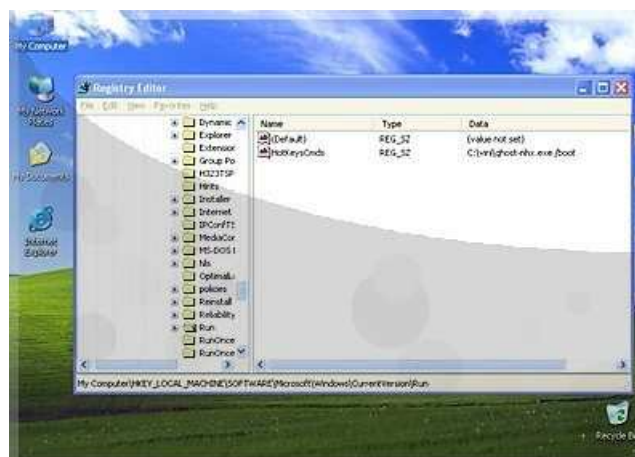
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>



05. Win32/Qhost trójai

Elterjedtsége a februári fertőzések között: 1.55%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárba, 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.



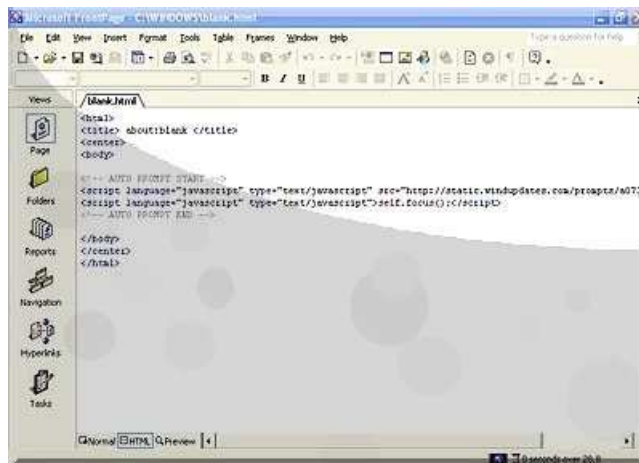
Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description



06. HTML/ScrInject trójai

Elterjedtsége a februári fertőzések között: 1.54%

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.



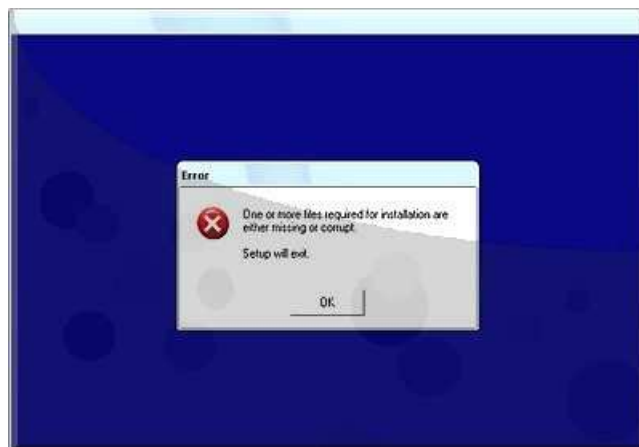
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen>



07. Win32/Ramnit vírus

Elterjedtsége a februári fertőzések között: 1.27%

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



08. Win32/Conficker féreg

Elterjedtsége a februári fertőzések között: 1.26%

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 eljárason keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a hosts 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.

[Megtévesztések és álhírek terepe a Facebook](#)
[A bank sosem hív bennünket, hogy mi a PIN kód](#)
[A HTML trójaiak riogattak minket októberben](#)
[Végre kiesett a Conficker féreg](#)
[Vírustoplista 2014. augusztus hónap](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5864986>

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.

Megtalálták az eltűnt maláj repülőt! Vagy mégsem?

2014.03.20. 08:45 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [bbc cnn repülő család átverés megosztás eltűnt maláj lárj](#)

A rendkívüli események, királyi esküvők, izlandi vulkánkitörés, [de még a bombarobbantások is különféle járulékos mellékhatásokkal járnak](#) online életünkre. Miért pont a rejtélyes módon eltűnt utasszállító repülőgép lenne kivétel az alól, ha éppen valamilyen aktuális témájú csalást, átverést kell kitalálni? Vagy mégsem sorozatunk újabb epizódjához érkezünk.



A dél-kínai tengeren március 8-án nyom nélkül felszívódott Malaysia Airlines MH370 igenis élénken izgatja az emberek fantáziáját, és [születnek is ezzel kapcsolatban mindenféle összeesküvés-elméletek](#), gépeltérítéstől kezdve a főreglyuk változaton át egészen az UFO-kig bezárólag. Magyarázat és gép egyelőre nincsen, sőt [az FBI már vizsgálja a pilóta otthoni szimulátorának merevlemezét](#), miután kiderült, hogy a gépről törölve lett néhány korábbi szimulációval kapcsolatos adat.



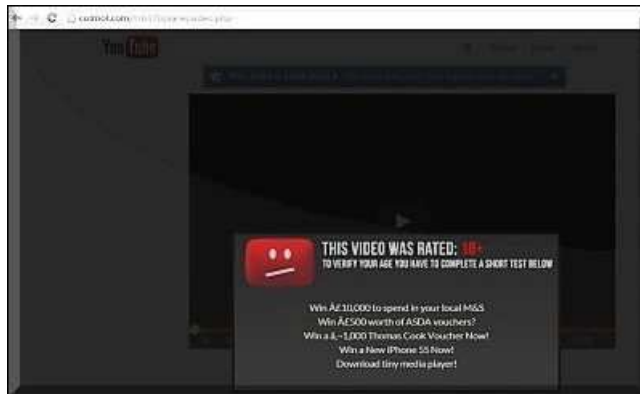
Így aztán [az FBI is bekapcsolódott a gép keresésébe](#), mert valahogy túl sok lett a kérdőjel. Mivel már vagy 26 ország keresi a napokkal korábban eltűnt maláj gépet, emiatt egy olyan hír, vagy Facebook üzenet, ami váratlanul arról számolna be, hogy breaking, megtalálták, tuti kattintásmágnes.



Pontosan erre alapozva jelent meg az az új átverés, ahol egy látszólag legitim Facebook üzenetben pontosan arról kapjuk az értesítést, hogy íme meglett az elveszett légijármű. Ám a hír zavartalan olvasását akadályozza egy kitakaró ablak, amely arra kér, ugyan osszuk már meg előre ezt a hírt, akkor majd becsukódik. Természetesen, ha valaki ezt megteszi, [akkor máris továbbterjed a dolog](#), és az összes ismerőse megkapja a "Malaysia Plane (MH-370) Has Been Found Near Bermuda Triangle. BBC News: Recent Video" kezdetű hamis üzenetet.



Az ígért mozi helyett pedig - tegye fel a kezét, aki ezen meglepődött - **egy hibaüzenet jelenik meg, amely arra hivatkozik, hogy ez a videóanyag kizárólag 18 éven felüliek számára érhető el, ezért legyünk szívesek a mellékelt tesztet elvégezni, mellyel még iPhone 5S okostelefont is nyerhetünk, na persze.** A cél persze az, hogy minél többen kattintsanak, ebből lesz a Cost Per Action bevétele a csalóknak. Érdemes azt is észben tartani, hogy a **YouTube videóknál** **sosem** ilyen életkort meghatározó teszt, maximum annyi lehet, hogy bizonyos anyagok megtekintéséhez muszáj bejelentkeznünk az accountunkkal.



Hasznos lehet ezzel kapcsolatosan feleleveníteni néhány ezzel kapcsolatos korábbi biztonsági tippünket. Eszerint [sose higgyük el, ha egy kéretlen link valami meghökkentőt ígér!](#) Ne dőljünk be, bármit is ígérnek egy lájkért, és látatlanban előre ne lájkoljunk, ne osszuk meg semmit! **Ha bármit telepítenünk kellene ahhoz, hogy megnézzünk egy videót (video kodekes átverés), ne tegyük!** Ha valóban megtalálták a gépet, azt a CNN vagy a BBC híroldal mindenféle kattintási, lájkolási, vagy megosztási kötelezettség nélkül szabadon olvasható módon amúgy is megírja.

Tetszik 30 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **G+**

Ajánlott bejegyzések:

[Az MH17 áldozatok hamis Facebook profiljai](#)
[Figyeld a kigyót! Nem semmi. Hanem átverés :-\)](#)
[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Valentin nap: Szerelem helyett átverés érkezik](#)
[Csaláselhárítás fordított képkereséssel](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5870655>

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](#).

V Magyar Ország 2014.03.21. 14:42:48

Igen elhiszem hogy a 21. században egyetlen katonai radar nem látja a gépet.

Igen elhiszem hogy a 21. században egyetlen katonai műhold nem látja a gépet.

igen elhiszem mert azt akarják hogy higgyek.

Válasz erre

Szeretnék felvenni a barátaim közé!

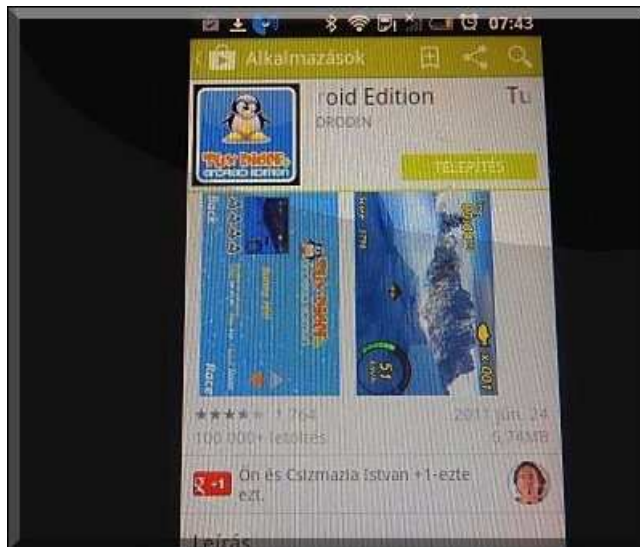
2014.03.24. 13:40 | [Csizmazia Darab István \[Rambo\]](#) | [4 komment](#)

Címkék: [google spam gmail a barátaim felvenni közé követni szeretné Flipora](#) [Infoaxe](#) [Discovercoolwebsites](#) [Szeretnék Önt](#)

Nem vadonatúj ez a spam, de ennek ellenére érdemes egyszer beszélni róla. Az "xxx.yyy@gmail.com követni szeretné Önt" kezdetű levelek ugyanis nem a Google-tól érkeznek, és valószínűleg már nagyon sokan kaptak ilyet vagy hasonlót, kattintani rájuk pedig nem érdemes, azt is elmondjuk miért.



Még a boldog békeidőkben ;-)) [foglalkoztunk egyszer a H15 "barátkérő" spammel](#), ahol kicsit ehhez hasonló volt a helyzet. Nyilván, ha valakinek eszébe sincs egy ilyen közösségi oldalt kipróbálni, akkor eredményesen távol tudja tartani magát az ilyenektől. Ám Gmail-es címe ma már szinte mindenkinek van, ahol aztán a Google Plus lassan már olyan önálló életet él, mint a Facebook: magától bökdös, nem létező üzenetváltásokat generál, és hasonlók. Legutóbb például a Google Play áruház egyik játékánál ötlött szembe a saját fotónk, mintha valaha is +1-eztünk volna azt, pedig nem. Érdekes módon egy másik telefonon megnézve ez már nem látszott így.



Szóval még ha a Facebook is a közösségi oldalak királya, akkor is sokan lehetnek, akik szövegetnek már kis közösségeket a Plus-on is, így ha látszólag onnan jön valami kérés, levél, felkérés, akkor az ember maximum nem érti, vagy furcsállja, de nem törli azonnal csípőből, mint a hi5-nél. A látszólagos barátkereső vagy követni akaró levelek mögött mindig valamilyen Flipora, Infoaxe vagy Discovercoolwebsites típusú oldalak állnak. Ebben a levélben a linkek látszólag a "discovercoolwebsites.com"-ra mutatnak, a kattintás azonban már a Flipora oldalra visz. Bár az e-mailben több gomb is kínálja magát "Elfogadja", "Elutasít", "Leiratkozás", és hasonlók, azért érdemes résen lenni. Ez magyarról magyarra fordítva azt jelenti, inkább egyiket se válasszuk, hanem "olvasás előtt/helyett alfa szögben meg kell nyomni a delete gombot".



Bár hasonló formalevéllal sokszor szoktak direktben kártevőket terjeszteni, mi most itt csak ezt a veszélytelenebb spammer vonalat követjük. Mi is történik pontosan, ha elfogadjuk? (Fülünkbe forró ölmot öntsének! ;-)) Ezt a legkönnyebben a korábban pórul járt delikvenszek internetes beszámolóiból, a sok ["How to remove..."](#) útmutatóból és/vagy [magának a webhelynek a leiratkozó oldalából](#) tudhatjuk meg. Kapunk a jövőben egy rakat Fliporás e-mail-t, és ez ugye akkor már rögtön nem kéretlen, hiszen a kattintással mi

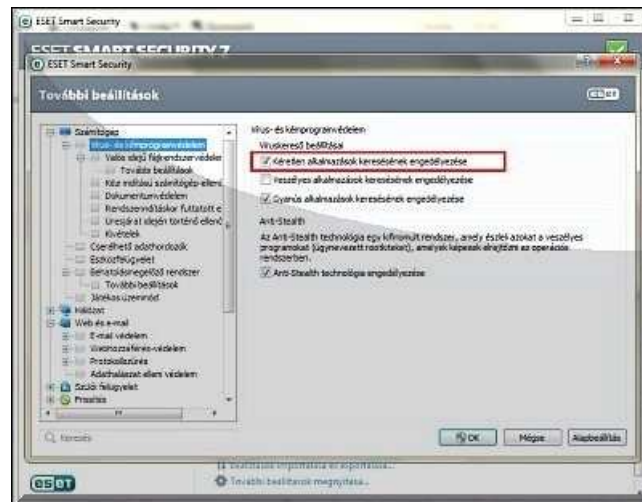
magunk kértük. És emellett a nevünk is küldődnek ilyen levelek a gépünkéről kinyerhető e-mail címekre, a böngészőnk kezdőlapját és beállításait átállítja, valamint nem kívánt böngésző kiegészítőt (add-on) is telepít az Internet Explorerben, a Firefoxban, és a Chrome-ban, amivel manipulálja a kereséseinket.



De ha már itt vagyunk, [olvassunk bele az ÁSZF-be is](#) a kockázatok és mellékhatások tekintetében: **"Unatkozol a neten? Mostantól soha többé nem fogsz!"** hiszen **nagyszerű honlapokat ajánlunk neked automatikusan**. Valamint beavatkozást a böngésződ előzményeibe, mi is ez? "Minden honlap automatikus elmentését". **Na most tegye fel a kezét jó magasra az, aki pont ilyet szeretne?** Ez utóbbi azért ha például egy a családtagok/munkatársak által közösen használt gépről van szó, komoly adatvédelmi aggályokat is fel tud vetni.



Hasznos lehet, ha a vírusirtónknak telepítéskor (esetleg később) megadjuk, hogy a "Kéretlen alkalmazások keresésének engedélyezése" segítségével a nem vírusos, de felesleges, vagy szokásaink után kémkedő hasonló alkalmazásokat szűrjék, utasítsák el. Kézi módszerrel pedig a számítógépet csökkentett üzemmódban indítva, regeddittel lehet eredményesen kiirtani. Nyilvánvalóan a megelőzés a legjobb, ezért pavlovi reflexből vagy spamszűrővel irtani kell az ilyeneket.



Végül, de nem utolsósorban a klasszikus kérdésre is keressük a választ: "Vajon ki küldözgeti ezt nekem?". Lehet, hogy egy nagy központi spam adatbázisból jön, de **ha a látszólagos feladóval életünkben csak egyszer is levelet váltottunk - a mi esetünkben pontosan ez történt - akkor ha ő rákattintott előtte egy ilyenre, akkor a mi e-mail címünk is "learatásra" került, ezért kaphattuk ezt meg**. Ha valaki a feladóval jóban van, és azt feltételezi, hogy talán véletlenül/óvatlanul csöppent bele ebbe a helyzetbe, akkor lehet esetleg figyelmeztetni. Futtasson a gépén egy alapos víruskeresést és lehetőség szerint máskor óvatosabban kattintgasson a kéretlen levelekre.

 **Tetszik** 51 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Adathalászat a Google nevében](#)
[Átverés a Google spam](#)
[Google+ meghívó vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5876685>

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](#).

[Begérke 2014.03.25. 10:34:22](#)

Az asszony azért írta meg a Fliporát, mert ő is megkapott egy ilyen mailt, be is írta reflexből a gmail-es felhasználónevét és jelszavát - de beállítottam neki a kétlépcsős azonosítást, ezért nem ment semmire vele a Flipora. Aztán meg szóltam neki, hogy mi van. :-)
Válasz erre

[Jűdarauszkasz 2014.03.25. 13:39:37](#)

Nekem a parom bongeszorjebe maszik bele allandoan valami Crossrider virus, sokszor a torrentet is blokkolja, mivel lehet lekaparni a geprol? (NOD nem boldogul vele.)

Válasz erre



[mildi 2014.03.25. 17:13:27](#)

kérdeznék (előrevetem: nagyon hülye vagyok hozzá):
valami html alapú, vagy mi ablakokban reklámok ugranak fel, ha lapozni akarok valahol, nem pedig a következő oldal.
valami sup, amiből ált vube ill. bet365 lesz. tököm tele vele...
nem találom sehol, böngésző kiegészítőknben, gépen sem.
chrome és winXP.
mi ez, és hogy tudnám kivágni a fenébe?
adblock sem csinál vele semmit :(

köszönöm.

Válasz erre



[Csizmazia Darab István \[Rambo\] • <http://antivirus.blog.hu>](#) [2014.03.26. 22:59:27](#)

A legjobb részt ki is felejtettem az ÁSZF-ből, idézet ON: "A Flipora fenntartja a jogot, hogy az Adatvédelmi Szabályzat néhány vagy minden pontját módosítsa, előzetes figyelmeztetés nélkül."

Válasz erre

Bloginterjú 2014.

2014.03.26. 10:24 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [blog interjú](#) [visszatekintés év 2014](#) [hétpecsét](#) [információbiztonsági újságírója](#)

Nyolcadik éve üzemel már az **antivírus blog**, ami nem rövid idő, emellett pedig a nem régen elnyert az "[Év információbiztonsági újságírója](#)" cím egy jó apropó, hogy érdemes legyen egy kicsit visszatekinteni, értékelni, beszélgetni.



K: Emlékezzünk először kicsit a múltra, hogy indult a blog?

V: [2007. szeptemberében nyitottam a blog.hu rendszerében](#). Blogot még nem, de hasonlót korábban is csináltam már, amikor az F-Secure és Kaspersky programok magyarországi supportja mellett a Vírus Híradó weboldal főszerkesztője voltam, vagy a Virusbuster víruslaborban angol/magyar híreket szerkesztettem a weblapra. Jelenlegi munkahelyem, a magyarországi NOD32 képviselője is ellát bőséges szakmai információkkal, de a neten is számos különféle hírforrást követek. **Jó érzés, hogy szerencsém folytán már korán ott lehettem a számítástechnikánál, még lyukasztottam lyukkártyát, csévéltém lyukszalagot**, megvolt a kalapácsos sornymotató, szobányi R20, R40 gépekkel dolgozhattam, és később persze az első megjelenő vírusok is közelről érdekeltek már.



K: Mennyi olvasót tudsz vagy sejtessz?

V: Hát belecsöppentünk a nehezebe. Körülbelül napi 3-500 az átlagos látogatószám. Ha Index címlap van, akkor persze fel tud ez ugrani 2-6 ezerre is. Egyébként folyamatosan töröm a fejem azon, hogyan juthatna el a sok hasznos információ azokhoz, akik rászorulnának. Azt tudom, hogy a szakma jó része olvassa, kapom is a visszajelzéseket a hackerkonferenciákon, de a szélesebb nyitással kapcsolatban még nem pattant ki a világmegváltó ötletem. Talán valamilyen szakmai hírportállal lenne jó együttműködni, azt mindenesetre látom, hogy amikor akár a print, akár az online lapok megkérdezik az olvasóikat, miről olvasnának szívesen, a biztonsági témakör vezet, vagy legalábbis az első háromban tuti benne van. Arra is ügyelek, hogy ne egy szűk látókörű szakbarbár zsargonokkal teletűzdelt oldala legyen ez, [hanem világos és közérthető módon közelítsek a privát szférá, a számítógépes adataink megvédéséhez](#), gyakorlati tippeket és trükköket is adjak, megtörtént incidensek tanulságait a hétköznapi olvasók elé tárjam. Öveges professzor mondása jut eszembe: "nincsenek nehéz vagy könnyű dolgok, csak megértettek és meg nem értettek vannak". Ha csak egyetlen ember is akad, aki blogban olvasottak miatt mégsem kattint az ingyen iPad-re, vagy attól fogva rendszeresen menti a dolgait a CryptoLocker miatt, akkor már nem dolgoztam hiába.



K: Csak a vírusok a blogtéma, vagy ennél azért szélesebb a merítés?

V: Amikor az antivírus programok úgy jó huszonnyolc éve elindultak körülbelül a Brain óta, eleinte valóban csak klasszikus vírusok voltak, és nekem ez sem lenne unalmas. **Időközben azonban átalakult az életünk, egyre többen használunk számítógépet, internetet, sokak munkáját enélkül már elképzelni sem lehet, és a veszélyek is sokfélék lettek. Ma már a kénytelen reklámoktól kezdve a hálózati férgek, kémprogramokon, trójaiakon, zsaroló titkosításon, személyiséglopáson keresztül az adathalászat, gyermekeink védelme a net ragadozóitól a botneteken át, a hamis letöltések, mindenféle kormányzati kártékony kód, kártékony tevékenység is idetartozik, emellett a személyes adataink védelme is egyre fontosabb terület.** Igyekszem minden biztonságot érintő témával foglalkozni, ha kell akkor a bankolással, ha kell akkor a Facebook adatvédelmi beállításokkal, és hasonlókkal. Egyébként a havonta megjelenő vírus top lista is inkább csak nevében víruslista már, lehetne akár kártevő top lista is, hiszen jóval gyakoribbak már a trójai programok vagy a férgek.



K: Kik segítenek az oldalad működtetésében?

V: Igazi "one man force" ez, Rambo egyszemélyes kommandója, és szerencsére nem is szól bele senki. Néha régebben eszembe jutott, talán jó lett volna egy társ. Így viszont igazából a magam ura vagyok, és mindenért, jóért-rosszért egy személyben vagyok felelős és lehetek büszke - ez a műfaj fekszik nekem a legjobban. De persze ha később másképp alakul, akkor a több szem többet lát is hasznos - majd meglátjuk, ahogy az Élet hozza. Szeretem a rendet, ezért csináltam magamnak az összes eddig megjelent posztból, cikkből egy óriási PDF katalógust, ez segít abban, hogy megtaláljam, ha utólag keresgélni kell valamit, hogy pontosan hol mikor miről esett szó. **Eddig ezer feletti blogposzt, és kevés híján majdnem 12 ezer Twitter rövidhírt tettem már ki. Kellemes meglepetés volt egyébként például, amikor a Twitter követőim között egyszer csak feltűnt Mikko Hyppönen, és Andreas Clementi is :-)**



K: Mi ez a Rambo név, honnan jött?

V: Ez már egy régi örökség, még a Commodore 64-es időkben mindenkinek volt valami nickneve, én pedig akkoriban láttam a filmet VHS-en, és egyből ezt választottam. Az egy varázslatos korszak volt egyébként, a hétfői adásszünetes fekete-fehér magyar televízióban BASIC nyelvet tanítottak, az URH rádióból kazettára lehetett venni a sugárzott számítógépes programokat, és talán

nem mindenki tudja, de volt már floppy lemezzel terjedő vírus a C64-re is.



K: Mitől kezd valaki programozóként inkább a vírusok iránt érdeklődni?

V: Ez egy izgalmas területnek látszott már akkor is. Most is az, de nagyon nehéz kenyér az antivírus gyártóké, hiszen nem csak a friss kártevőket, hanem minden korábban megjelent vírust egyszerre visszamenőleg is folyamatosan észlelni, detektálni kell. Sokszor előfordul, hogy egy kártevő régi őskövyület vírusokat droppol, azaz bocsát ki magából, és ezek még ma 2014-ben is például szépen le tudják gyalulni egy Windows gép bootszektorát. Egy meghatározó esetre azért emlékszem, ami még C64-en történt, az NSZK-ból hozott méregdrága, 300 nyugatnémet márkás floppy meghajtó váratlanul tönkrement egy lemezmásolás közben. A szétszedés után derült ki, hogy a fejet egy gonosz program kihúzta a parkolópályára, de ha kézzel óvatosan visszatoltuk, összeszerelés után ismét hibátlanul működött. Ez volt az első lecke, hogy nem mindenki Grál lovag, figyelni kell a rosszindulatú programokra. A másik pedig a jól ismert Potyogós, azaz Cascade-1701 volt, akkori assembler tanárommal, Pethő Ádámmal nézegettük a kódot, mit is csinál pontosan. Akkor egyébként még sokan hitetlenkedve fogadták, vagy szimplán csak hülyeségnek tartották a vírusokat.



K: Az olvasók nem látták, de én belenézhettem a szakmai önéletrajzodba, és abban rengeteg tanfolyam és továbbképzés szerepelt. Úgy nézel ki, mint aki tényleg komolyan veszi ezt az élethosszig tanulás dolgot.

V: Egyik kedvenc Einstein idézetem szerint: "A bölcsesség nem az iskolázottságnak, hanem megszerzésére egy életen át való próbálkozásunknak az eredménye." Vagyis tényleg kell tenni érte. Egyébként a hivatalos csatornákon felül a blogíró is tanul a folyamatosan végzett kutatásokból, kártevő elemzésekből, fordításokból, sőt még a kommentekből is. Ez egy feneketlen kút, és aki keresi a tanulást, annak csak a nap 24 órája szab határt.



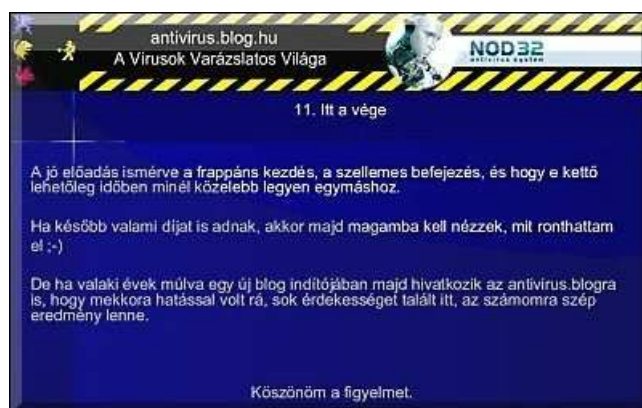
K: Kik a példaképek, ha vannak ilyenek?

V: Szakmai blogokból rengeteg kiváló van, hogy csak néhányat említsek: Mikko Hypponen, Graham Cluley, Dancho Danchev, Randy Abrams, és Eugene Kaspersky is vezet ilyesmit. Nekem egyébként nem tetszik az a túlzott leegyszerűsítés, hogy aki nem szeretné, hogy az NSA megfigyelje, az inkább menjen vissza a múlt századba kecskepásztornak. Én úgy látom a fent említett szakértőknél, hogy folyamatosan igyekeznek szofisztikált, és praktikus napi tanácsokat adni nem csak a vírusok és a trójai programok ellen, hanem minden incidens, azaz a lehallgatások, és identitáslopások ellen is. Úgy vélem, pontosan ez a valódi feladata a biztonsági szakmának, a digitális írástudóknak. [A Welivesecurity weblap](#) vagy éppen [a Nakedsecurity oldal](#) szerintem ezt szépen meg is valósítja a napi gyakorlatban.



K: Elolvastam a neten egy egyik prezentációd, amelyet még 2009-ben tartottál "Egy szakmai blog háttere" címmel. Ebben azt írod: "Ha később valami díjat is adnak, akkor majd magamba kell nézzek, mit ronthattam el ;-). De ha valaki évek múlva egy új blog indítójában majd hivatkozik az [antivirus.blog](http://antivirus.blog.hu)ra is, hogy mekkora hatással volt rá, sok érdekességet talált itt, az számomra szép eredmény lenne." Akkor most eljött ez a pillanat, mit is rontottál el?

V: Húha, most jól megfógtál :-). Egyébként főiskolai számítéktanár barátom dicsérte, hogy sok anyagot tud használni a blogból, és a [Vírusok Varázslatos Világa](#) cikkarchívumból, emiatt úgy látom, hogy a szép eredmény része azért csak összejött.



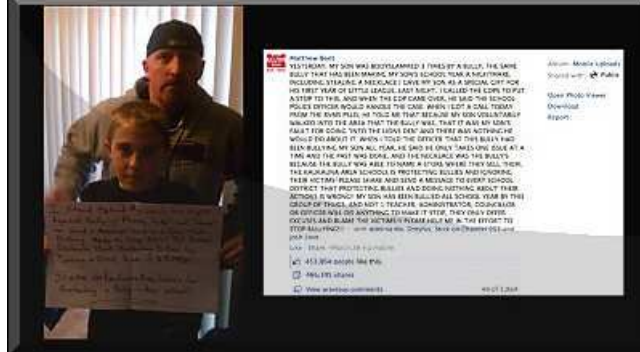
K: Mit gondolsz az "Év információbiztonsági újságírója" díjról, hogy sikerült az ottani bemutatkozó előadásod, és mi változik mostantól?

V: Nem szoktam sokat számolgatni, meg el is sodorják az embert az események, de mikor szembesültem azzal, hogy már nyolcadik éve csinálom a blogot, még én is elcsodálkoztam, hogy ilyen régóta megy. **A díjnak rendkívül örülök, mert szakmailag eddig még soha nem kaptam semmit, érmek és oklevelek korábban csak a sportban elért eredményeim miatt voltak. Egy kedvező visszajelzés, hogy az irány jó, és lehet szépen folytatni a munkát.** Vagyis minden megy tovább a régi kerékvágásban, születnek az újabb cikkek, előadások, blog posztok rendületlenül. Remélhetőleg a díj miatt talán ezeket többen is olvassák majd, akik eddig esetleg nem ismerték.



K: Végezetül mit tartasz fontosnak most 2014-ben?

V: A minap olvastam és szinte [minden Androidos felhasználót érintő sebezhetőség](#) kapcsán újra azt mondom, az okostelefon védelmi program nélkül orosz rulett. Itt a rendkívüli elterjedtség, és az, hogy [Charlie Miller véleményével](#) ellentétben szerintem a fejlesztők nem tanulták meg elég alaposan a PC-s vírusokkal, kártevőkkel kapcsolatos történelmi leckét, jól mutatja mindezt a támadások számának erőteljes emelkedése és például [az alkalmazás engedélyekkel kapcsolatos](#) káotika is, szóval bevált a jóslat, [tényleg az Android lett az új Vadnyugat](#).



Emellett szerintem a biztonságtudatosság rendszeres munkahelyi képzése volna rendkívül fontos, de emellett **már gyerekkorban el kellene kezdődnie** egyfajta, életkornak megfelelő oktatásnak. Az én véleményem szerint ennek szervezett tananyag formájában kell megvalósulnia, ehhez a mostani 4. osztályban induló számítástechnika nevű tantárgy nem elég, illetve teljesen más cél mentén halad. Arra nem biztos, hogy mindenkinek szüksége van, hogy megtanulja, hány cilinderből is áll egy merevlemez, ám arra már minden gyereknek, és egy elsősnek is szüksége volna, hogyan netezzen biztonságosan, hogyan legyen e-mailcíme, ha játszani szeretne a számítógéppel, hogyan vigyázzon magára az interneten. És mivel ez a generáció tölti a legtöbb időt online, az egyre korábban kezdődő iskolai zaklatások esetek ellen is fontos lenne a felkészítés, a védekezés. Már tettem javaslatokat ez ügyben, szerintem évi 3-4 ilyen tanóra - minden egyes osztályban az életkornak megfelelő esetekkel, példákkal - sokat javíthatna a helyzeten. Beszélgetek róla, visszajelzésekre várok, remélem más is hasonlóan látja ezt és lesznek majd ebben segítő-együttműködő partnerek.

K: Köszönöm a beszélgetést, és további sok sikert a munkádhoz!

V: Én is köszönöm szépen.

f Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **g+1**

Ajánlott bejegyzések:

[Figyeljünk a mobiltárcánkra, a Bitcoinjainkra](#)
[Ször Péter díjjal jutalmazták az ESET kutatóit](#)
[Nem változtak a toplistás vírusok](#)
[Hetedik hónapja vezet a mentéseket törölő kártevő](#)
[IDC Biztonsági Konferencia 2014.](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5879456>

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 rendszert, ne siránkozz!

2014.03.28. 13:23 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [tapasztalatok](#) [signal](#) [támadás](#) [etikus](#) [botnet](#) [sebezhetőség](#) [silent](#) [hackelés](#)

Igen tanulságos előadást láthattunk arról, hogy az elvégzett etikus hackelési projektek után hogyan látják belülről a szakemberek a jelenlegi helyzetet. Nem az a kérdés, hogy sikerül-e bejutni, vagy a rendszert feltörni - erre általában igen a válasz - hanem sokkal inkább a milyen könnyen és milyen rövid idő alatt az érdekes, illetve az is kulcs fontosságú, hogy mennyire fogadják meg az ügyfelek az ilyenkor kapott tanácsokat.



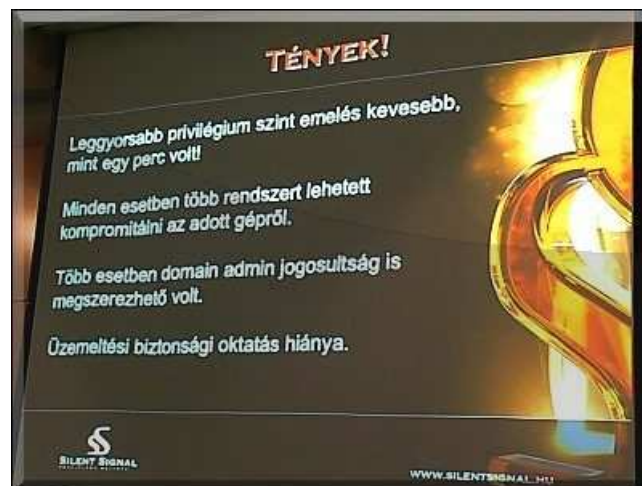
Ezekről, a legjellemzőbb tapasztalatokról, gyakran észlelt problémákról, és hiányosságokról kaphattunk sok érdekes, részletes és praktikus háttérinformációt. Amikor például a sok jelszó feltörésről, vírusos, botnetes fertőzésekről, nagy cégek szervereinek kompromittálásáról olvasunk, hajlamosak vagyunk azt hinni, minden egyes támadás mögött egy zseniális gonosz áll.



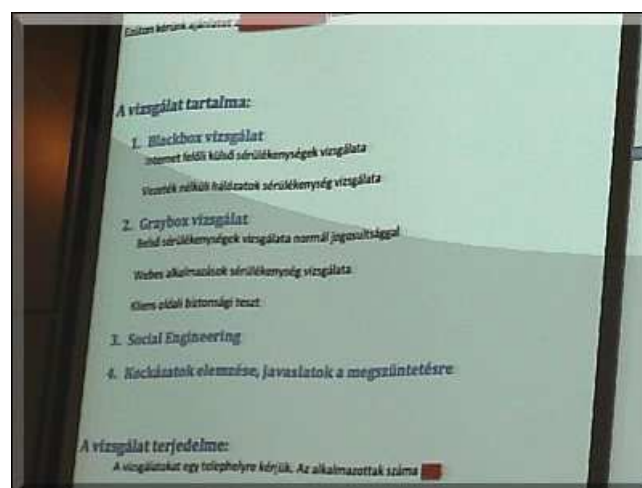
Természetesen a támadók alapos tudása sok esetben valóban nem kérdőjelezhető meg, ám óriási arányban maguk a felhasználók, rendszergazdák, adatgazda felelősök is megkönnyítik a behatolók dolgát. [Nem mindegy, hogy mennyire van megnehezítve a támadó feladata, percek alatt könnyedén hozzáférhet bármihez vagy számos akadályt állítanak az útjába.](#) Szem előtt tartva azt, hogy 100 százalékos biztonság persze nem létezik, azért hogy a biztonsági kockázatot, a védelem mértékét 40%-ról 85-re emeljük, annak a Silent Signal szakemberei szerint igenis volna értelme.



Ehhez például olyan dolgok kellenének, mint a hosszú és erős jelszavak megkövetelése és használata, a jelszavak és egyéb információk titkosítása, a kényes mentések másolatai ne heverjenek szanaszét a szervereken, ahogy a főkönyvtárban tárolt, és plain textben olvasható jelszo.txt, konfigurációs backup vagy SQL adatbázis dump állományok is nagyságrendekkel megkönnyíthetik egy támadó dolgát. Ugyanezek elmondhatók a jogosultságok kiosztásánál, ACL beállításoknál, vagy szerverek frissítéseinek elhanyagolásánál. A kártevők és a támadók is ma már iparszerűen használják ki a sérülékeny szoftverek hibáit.



Természetesen lenne tanulsága mindennek nem csak a biztonsági szakmának, hanem a szolgáltatást igénybe vevőknek is. Érdemes az ilyen biztonsági projektet előre megtervezni, alaposan tájékozódni, hogyan zajlik egy etikus hackelési vizsgálat (meg tudnátok nézni most pénteken gyorsan éjjel 2 és 3 között), és tudni, pontosan mit is akarnak kérni.



A megrendelőnek emellett illene pontosan ismernie a saját infrastruktúrát (ja nem is 30, hanem 50 szerver), és megfelelő belső kapcsolattartókat kell hozzá kijelölni, hiszen nem a vizsgálat szimpla kipipálása a cél.



A komolyan vehető etikus hacker csapatok ugyanis nem egy csupasz automatikusan lefuttatott Nessus listát csapnak le az asztalra Mekk Elek módjára, hanem egyrészt **valóban leleményesen, és hacker fejvel gondolkodva az összes gyenge pontot igyekeznek alaposan felderíteni - ezt semmilyen gép vagy program nem végzi el automatikusan**, hanem rettentő sok tanulás és tapasztalat vezethet el csak ide.



Másrészt pedig a végeredmény mellé részletes megoldási javaslatokat is tesznek. Itt még az sem lehet akadály, ha véletlenül egy 0-day sebezhetőség felfedezése okozná a problémát, hiszen technikailag ilyenkor is lehet megfelelő védekezési módszert, vagy workaroundot alkalmazni.



Itt lép be a képbe az, hogy a tapasztalatok szerint sok ügyfél a javítási javaslatokat egyszerűen ignorálja, és "soha napján" történik meg a javítás, pedig belső felelősök és megfelelő határidők kijelölése lenne az optimális. Itt az ismételt visszaellenőrzési folyamatok is jól mutathatják, hogyan változik meg vagy éppen marad a régiben a korábbi sérülékeny állapot.



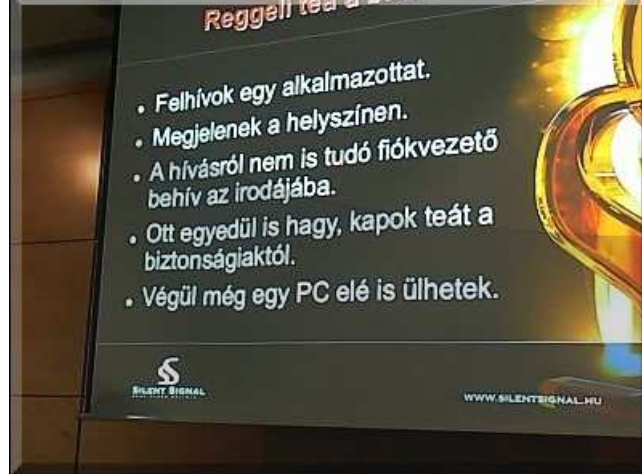
Utalva arra, hogy 100 százalékos védelem valóban nem létezik, valójában nem az az igazán szomorú, ha egy rendszer sebezhető, vagy törhető, hiszen elegendő munkával mindig mindenhol lehet hibát találni. Sokkal inkább szánalmas viszont az, ha valaki megkapja ugyan erről a jelzést, jelentést, ám ennek ellenére mégsem tesz ellene semmit.



A technikai trükkök természetesen nem merülnek ki pusztán a számítógépek tesztelésében, hanem például **képbe kerülhet a beléptető rendszer gyengesége is**. Ha például napokig észre sem vesszük, ha egy vendégkártyát nem vittünk vissza, az nem utal túl alapos és szigorú rendszerre, de **adott esetben az RFID kártya másolása, klónozása is eredményre vezethet** egy felkészült támadó esetében - ezt egy pár perces mellék helység látogatáskor is el tudja végezni a megfelelő eszközökkel.



Emellett egy külön fejezet a technikai dolgok mellett **a social engineering rész is, amikor ha egy illetéktelen úgy juthat be könnyedén, hogy közben még teával is megkínálják, éles banki terminálokhoz férhet hozzá vagy észrevétlenül felcuppantathat a hálózati rackbe egy Raspberry-t**.



És persze ott van az eszköztárban az elmaradhatatlan hamis telefonálgatás a rendszergazda nevében a jelszó után érdeklődve, a kíváncsi alkalmazottaknak szándékosan elszórt USB kulcsok a munkahely területén, vagy a célzottan a dolgozóknak küldött "nyereményjátékos" e-mailes APT támadás, amin a munkahelyi jelszó begépelésével lehet részt venni. A tapasztalatok szerint több-kevesebb ember minden esetben bedől ezeknek a trükköknek. Ilyenkor ezek tanulságait is le kell vonni, és a védelmi szolgálat, valamint a dolgozók rendszeres biztonság tudatossági képzésében ezekre külön ki kell térni.



Végül arról is hallhattunk pár keresetlen szót, mire számíton az a hibavadász, aki 0-day sebezhetőségek felfedezéséből és beküldéséből szeretne megélni. A tapasztalatok szerint itt sem csak Grál lovagok kereskednek ezekkel, így simán megtörténhet, hogy a megfelelően és alaposan dokumentált jelzésre mégis nemet mondanak, közben az el nem fogadott jelentésnek viszont ellopják tartalmát, vagy például csak minden tizedik bejelentőnek fizetnek a látszat kedvéért.



Mindenesetre egy érdekes és színes körképet kaphatott az etikus hackeléssel kapcsolatos világ aktuális kérdéseiről, aki részt vett ezen a szerda esti rendezvényen.

Tetszik 28 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **g+1**

Ajánlott bejegyzések:

[Ruby on Rails sebezhetőség a szervereken](#)
[Realitás lehet az Androidos botnet](#)
[Dél-Korea is kínai behatolást gyanít](#)
[Új dimenziók](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/5883099>

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.

IDC Biztonsági Konferencia 2014.

2014.03.31. 09:07 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [konferencia](#) [biztonsági](#) [2014](#) [roadshow](#) [idc](#)

Március 27-én tartották az eseményt a Roadshow keretében a Hotel Novotel Centrumban, amely egész napos elfoglaltságot ígért a látogatóknak. A témák változatosak voltak, az aktuális világpolitikától a Snowden ügyön át az UTM-ektől a Next Generation Firewall-ig egészen a dolgozók biztonság tudatosságának oktatásáig.



Az első előadást Nógrádi Györgytől hallhattuk, aki a szokott precíz alaposágával, és lényeglátásával áttekintette a világpolitikai helyzetet. Minden adódnak furcsa helyzetek, most például Kína helyzete érdekes, hiszen a legutóbbi fejlemények miatt választania kellene az USA vagy Oroszország között. A Snowden ügy folyamatosan rányomja bélyegét az eseményekre, legutóbb például az szivárgott ki, hogy Szaúd-Arábia titokban folyamatosan arra kérte az USA-t, hogy bombázza Iránt.



A lehallgatási botrány kapcsán fontos kiemelni, hogy azok a hatalmak, akiknek van megfelelő ereje és képessége - mint például az USA - az él is vele, és természetesen gazdasági hírszerzésre is kihasználja, ezen nincs mit csodálkozni, "nincs békés nap", és ez mindig is így lesz. Ahogy az is megszokott, hogy amikor valami mégis kiderül, az érintettek soha nem beszélnek, mert nem beszélhetnek róla. Végül azzal az apró érdekességgel zárta az előadást, hogy lám milyen sok kiszivárogtatás látott már eddig napvilágot, de Oroszország vagy Kína elleniről még csak nem is hallottunk.



A többi prezentáció már sokkal technikaibb vizékre evezett, így például Tomasz Sloniewski az úgynevezett harmadik platform szerepét emelte ki a biztonsági kockázatok közül. Ide sorolható minden mobilitással, felhő technológiával és BYOD-dal kapcsolatos megoldás, amely manapság számos munkahelyen már most is komoly, és idővel még nagyobb szerepet játszik. A vírusok, kémprogramok, az adatszivárgás, vagy a bizalmas céges adatokat is tartalmazó eszközök elvesztése mind jelentős kockázati tényezők egy munkahely életében.



A hackerek is globálisak lettek, és a spamek, kártevők, a cégek jó hírnevének rombolása, vagy az identitás lopás minden szereplőre nézve nagy és gyakori veszélyt jelent. Megtudtuk még, hogy a kimutatások szerint nőtt "az IT biztonság svájci bicskájának" is nevezetett UTM-ek tortaszelete, ezzel együtt a professzionális IT security költség mértéke is emelkedőben van. Így a különféle biztonsági auditokra, forensics vizsgálatokra, illetve security tréningekre és képzésekre a korábbi időszaknál érzékelhetően többet költöttek a vállalatok.



Balabit színeiben lépett a dobogóra Illés Márton, aki az úgynevezett eCSI kapcsán kiemelte, a kockázatok közül kiemelkedően magas mértékben, 60%-ban az emberi tényező dominál. A veszélyforrások között a célzott APT támadásokat említette, ahol a rendszergazda, a főnök, illetve akár a titkárnő is célpontban lehet. Véleménye szerint önmagában a naplózás kevés, nem vezet megfelelő eredményre, emiatt olyan kombinált megoldásra van szükség, ahol a kontroll és a megfigyelés egyensúlyban van.

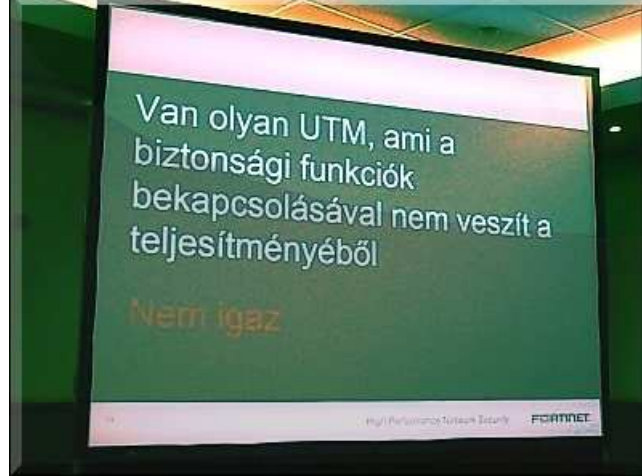


A klasszikus idézet szerint a jó biztonsági policy segíti az üzletmenetet, míg a rossz gátolja azt. A téma amiatt is különösen fontos lehet, hiszen **az alacsony felderítési arányok miatt évről évre nő az incidensek, támadások száma. A kontroll folyamatokban csak jó minőségű adatot érdemes gyűjteni, és ezen belül is a kiemelt eseményekre kell fókuszálni. Az úgynevezett VIP felhasználókra kell jobban odafigyelni, mert ők jelentik a kiemelt kockázatot, hiszen a több jogosultságaik miatt ők okozhatják a legnagyobb károkat**

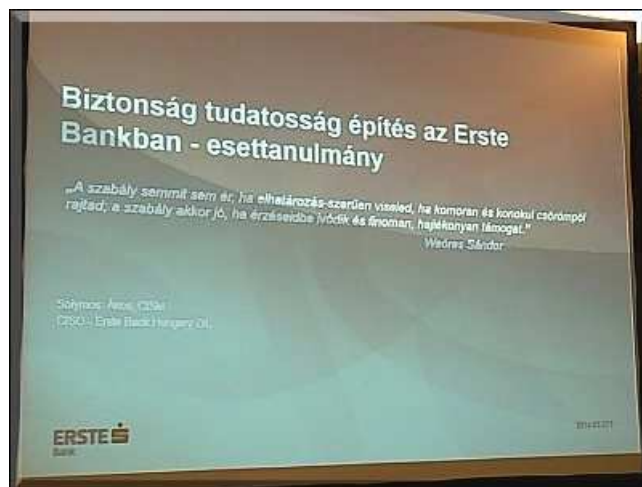
- Illés Márton véleménye szerint ezzel a módszerrel érhetjük el leginkább a felelős költést.



Hirsch Gábor előadásában először a Fortinetet mutatta be, ahol kiemelte, magyar nyelvű terméktámogatást is tudnak már nyújtani. Majd néhány adattal **azt illusztrálta, hogy az UTM eszközökkel kapcsolatos egyes marketing ígéretek nem mindig állják ki a valóság próbáját.** A józan észről teljesen elrugaszkodott állítás például **azt leírni, hogy van olyan UTM, amelyek a biztonsági funkciók bekapcsolásával egyáltalán nem veszít a teljesítményéből.**



Véleménye szerint ugyanakkor az egy kézben lévő integrált megoldás jobb, mint a több gyártós, illetve az UTM-ek sebességével kapcsolatosan kiemelte, **az a legoptimálisabb, ha maga az ügyfél teszteli ezt a termék kiválasztása során.**



Sólymos Ákos az Erste bankból érkezett, ahol az információ biztonsági osztályt vezeti. Bemutatójában azt igyekezett részletesen felvázolni, hogy sikerült elsősorban saját munkaerővel a belső biztonsági képzéseiket, a dolgozók oktatását évről évre hatékonyabban elvégezni. **A dolgozók esetében a tudatlanság, naivság, figyelmetlenség, segítőkészség, de szélsőséges esetben akár a bosszúvágy is vezethet incidensekhez.**





A "Te vagy a kulcs a biztonsághoz" szlogennel és részletes, cikkekkel, plakátokkal, és az intranetet is magában foglaló kampányokkal igyekeznek a dolgozókat megfelelő biztonságtudatos viselkedésre oktatni. Véleménye szerint ezzel az ügyfelek is elégedettebbek lesznek, és a munkavégzés is hatékonyabb lesz. Kiemelte, hogy a szabályzatok oktatása nem egyenlő a tudatosság növelésével. Végezetül azt is megemlítette, hogy **a dolgozók oktatása mellett kiemelt jelentősége van a Safer Internet programnak is, amely már gyermekkortól segít elsajátítani a biztonságos internethasználattal kapcsolatos ismereteket.**



 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

   Tweet  

Ajánlott bejegyzések:

[Biztonsági konferencia - nyitott wifi honeypot-tal](#)
[Samsung lock Oleg Pliss nyomdokain](#)
[Ször Péter díjjal jutalmazták az ESET kutatóit](#)
[Nem változtak a toplistás vírusok](#)
[Hetedik hónapja vezet a mentéseket törölő kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5886625>

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.

Biztonsági tippek a magánélet megőrzéséhez

2014.04.02. 09:59 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [privacy](#) [tippek](#) [magánszféra](#) [titkosítás](#) [pgp](#)

Mikko Hyppönen szerint a Snowden által leleplezett túl sok adat gyűjtése azért aggályos, mert nem csak a terrorista gyanús elemek ellen irányult, hanem kivétel nélkül mindenki megfigyelésével járt. Továbbá, mert nem lehetünk biztosak benne, hogy valójában nem örök időkre őrzik meg ezeket. **Lehet az embernek titka akkor is, ha nem bűnöző, nem biztos, hogy akar testre szabott reklámot magának, nem okvetlenül kíván túlzott érdeklődést, esetleg utálja a megosztást, nem szeretné földrajzi mozgását mások által megismerhetővé tenni.**



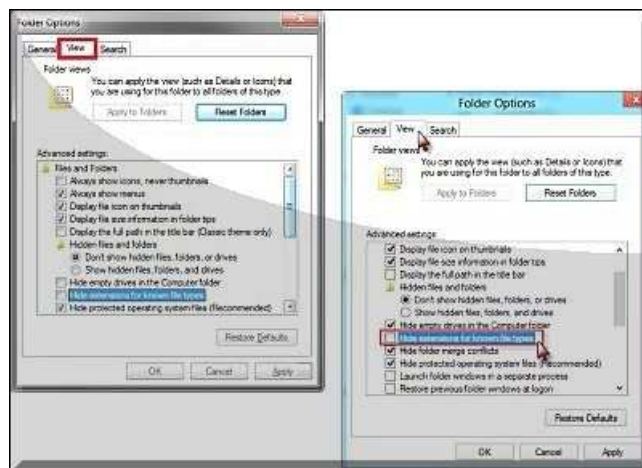
Sokak szerint túlzás a megfigyeléstől való félelem, és aki nem szeretné, hogy megfigyeljék, az dobja ki a gépét és menjen vissza a múlt századba kecskepásztornak. Ennél azért hasznosabb módszer, ha praktikus tanácsokkal látjuk el az olvasókat, sok mindent lehet azért tenni ellene, és egyik sem boszorkányság. **Tudatos szoftver termék használat, megbízható szolgáltatások igénybevétele és biztonsági megoldások vásárlása, esetenként nyílt forráskódú programok is szóba jöhetnek, de mindenesetre érdemes gondosan kiválasztani, kibe és mibe helyezzük a bizalmunkat.**



Az adatok megosztásában, és a privacy miatti aggodalomban a fiatalok látszólag sokkal rugalmasabbak. Valójában azonban sokszor inkább csak naivak, tapasztalatlanok, gyakorta nem elég biztonságtudatosak. **Ha elég időségek lesznek, és jobban megismerik a kockázatokat, valószínűleg jobban megértik majd, hogy az esetleg felelőtlenül megosztott adataik miatt esetleg nem kapnak hitelt, vagy nem kapnak meg egy állást.** Nem praktikus dolog túlságosan részletesen beszámolni életünk minden egyes részletéről, realtime fizikai koordinátáinkról, pillanatnyi reptéri becsekkolásainkról már csak ezért sem, mert a tények szerint a betörők csaknem 80 százaléka aktívan használja a Twitter, Facebook, Google StreetView és egyéb közösségi oldalak adatait a bűncselekményeinek.



És még egy gondolat Edward Snowdentől: "If you have to go to the command line people aren't going to use it. If you have to go three menus deep, people aren't going to use it." Magyarán nem volna szabad túlbonyolítani a biztonsági beállításokat, vagyis a szolgáltatók, szoftverfejlesztők nem igazán tesznek meg mindent. Az alapértelmezett biztonsági beállításoknál, az Android Appok engedélyeinél, vagy az ismert fájltypusok Windows alatti alapértelmezetten rejtett beállításánál, [amit a 2001-es Kournikova vírus óta nem változtattak meg](#) - szóval lenne itt még feladatuk bőségesen a biztonság emelésében.



Kérdésünk akkor, milyen eszközöket használjunk ahhoz, hogy az online életünk titkos maradjon? Jöjjenek hát a beígért biztonsági tippek, védjük hatékonyan a privacy-t!

- merevlemez titkosítás:

Erre leginkább nem az operációs rendszer megoldása, hanem valamilyen operációs rendszer verziótól, valamint platformoktól is független megoldás a legjobb, például a TrueCrypt

- fájl és e-mail titkosítás:

A GPG (GNU Privacy Guard) segítségével nem csak helyi fájljainkat tudjuk titkosítani, hanem a publikus kulcs cseréje után levelező partnereinkkel úgy tudunk majd levelezni, hogy nem csak abban lehetünk biztosak, hogy valóban a feladótól attól kapjuk az üzenetet, hanem így azt is elérjük, hogy a kommunikációt illetéktelenek nem hallgathatják le. A privát kulcsot természetesen nekünk kell ehhez alaposan megőrizni.

<http://pgp.guska.hu/GPG-Howto-EKOP1215.pdf>



- megbízható programok telepítése:

Alapos és előzetes tájékozódás a használt szoftvereinkről, letöltés mindig megbízható helyről - például a gyártó weboldaláról, telepítés előtt

a szoftver ellenőrző hash értékének ellenőrzése - ezek mind segíthetnek ellenőrizni a trójai programokat, vírussal vagy rejtett kémprogrammal újracsomagolt alkalmazásokat.

- nyitott wifi

A felhasználók jelentős része komoly veszélynek teszi ki személyes adatait azzal, hogy nyilvános wifiről is bejelentkezik e-mail és Facebook fiókjába, vagy akár internetbankjába, pedig ezekre bárki telepíthet olyan kémprogramot, ami ellophatja jelszavainkat. Publikus hotspoton sose használjuk fiókjainkat, ha mégis szükséges - például nyaraláskor - inkább hozzunk létre egy ideiglenes e-mail címet. Illetve bár drágább, de inkább saját megbízható 3G/4G kapcsolatunk segítségével internetezzünk.

- rendszeres mentés:

Ez akkor a jó, ha több fizikailag is különböző adathordozóra történik, például lehet egy felhős tárhely és egy külső merevlemez. Természetesen egy jó mentés mindig legyen titkosítva is - hátha csak a mentést lopnák el, továbbá az igazi mentés fontos tulajdonsága még, hogy ki is próbáltuk, hogy valóban olvasható és visszaállításra is használható lett-e.



- fizikai védelem:

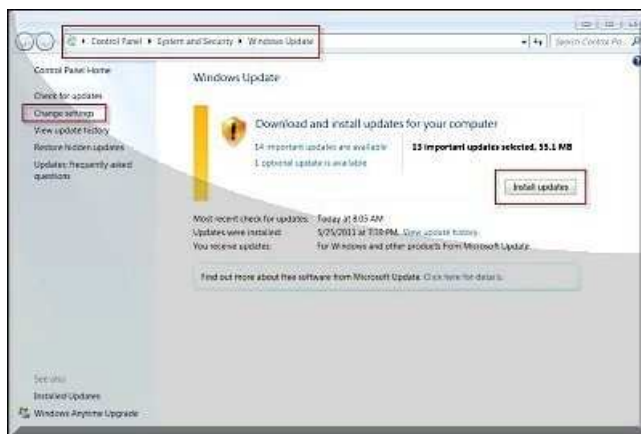
Számítógépünkön, de a táblagépen és az okostelefonon is mindig legyen bekapcsolva a jelszavas védelem, és az időzár, meggátolva azt, hogy idegenek hozzáférhessenek.

- jelszavak:

A router admin jelszavak, wifi jelszavak, FTP jelszavak, minden általunk igénybe vett közösségi oldal, webhely, skype, webáruház, postafiók, szolgáltatás rendelkezzen egyedi, és erős jelszóval. Az incidensek egyik igen gyakori oka a túlságosan rövid és gyenge jelszavak használata, melyek kitalálása, brute force vagy szótár alapon való feltörése sok esetben percek alatt elvégezhető.

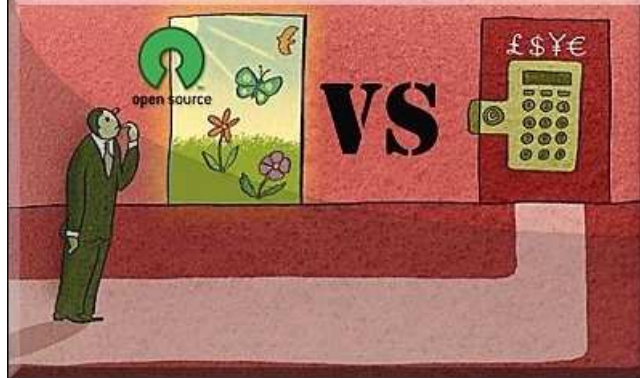
- frissítések

Mivel a kártevők rendszeresen használnak ki javítatlan sebezhetőségeket, emiatt fontos, hogy mindig tartsuk frissen operációs rendszerünket, valamint minden alkalmazói programunkat.



- vírusirtó

Ha telepítünk egy antivírust a gépünkre, ezzel jelentősen csökkentjük a vírusfertőzések, kémprogramok, botnetek és mindenféle egyéb kártevő bejutási esélyét. Az internetbiztonsági csomagokban sok kiegészítő módszer: heurisztika, URL blokkolás, script elemzés, tűzfal, reputációs adatbázis biztosítja, hogy a pillanatnyilag még ismeretlen kártevők, variánsok is fennakadjanak az ellenőrzésen. Egy átlagos Windows felhasználónak - és lassan már nem csak ott, hanem OS X, Android platformokon is - elengedhetetlenül szükséges a védelmi program.



Sokunk gépén vannak bizalmas fájlok, banki illetve céges adatok, egészségügyi információk, családi titkok, fotók, esetleg Bitcoin tárca, ezek egyike sem közpréda: nem szánjuk bárkinek, nem szánjuk mindenkinek. [Aki ma azt mondja, hogy számára nem fontos a magánélet biztonsága, az valószínűleg még nem gondolkozott elég hosszan rajta.](#)

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

Ajánlott bejegyzések:

[Így változtunk Snowden óta](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Kormányzati e-mailek kontra biztonság](#)
[Valentin nap: Szerolem helyett átverés érkezhét](#)
[6 tipp személyazonosságunk megvédésére](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/5890201>

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> 2014.04.02. 15:31:56

igen ezeknek evidens dolgoknak kéne lenni, lassan linux alatt se veszünk fel ész nélkül minden repo-t, hanem csak megbízható tárolókat használunk, mertr jön a csúnya fertőzés
Válasz erre

Túlélési tippek Windows XP-hez

2014.04.07. 09:55 | [Csizmazia Darab István \[Rambo\]](#) | [6 komment](#)

Címkék: [windows xp támogatás vége](#)

Avagy galaxis útikalauz XP utazóknak, ugyanis egész pontosan 1 azaz egy nap van hátra az április 8-i támogatási határidőből. **Mit lehet megtenni egy csupán viszonylagos biztonság érdekében - tanácsainkkal erre a kérdésre igyekszünk megadni a választ.**



A Windows XP még mindig óriási mértékben elterjedt és használatos. [Idézzünk egy kicsit egyik idevágó korábbi posztunkból](#): "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." De miért is ennyire fontos ez az egész? Természetesen a vírusokkal, kártevőkkel van kapcsolatban. Már eddig is sok sebezhetőségből vészelt ez az elavult operációs rendszer, de a SANS(SysAdmin, Audit, Networking, and Security) szerint a már felfedezett, de eddig még nem publikált zero day sebezhetőségeket nagy valószínűséggel bespájzolták a kártevőterjesztők, hogy biztonsági frissítések befejezése után tudjanak vele hatékonyan támadni, fertőzni.



Most pedig jöjjenek akkor akkor az ígért tippek. Először is, ha esetleg eddig nem tettük volna, **mostantól mindenképpen érdemes rendszeresen biztonsági mentéseket végezni**, ezeket pedig próbáljuk is ki, hogy éles katasztrófa helyzetben hogyan és mennyi idő alatt tudnánk helyreállítani az információkat a számítógépünkön.

A következő dolog a frissítés lenne, vagyis tartsuk naprakészen a Windows XP példányunkat. Az persze nyilvánvaló, hogy **a Microsoft leállítja április 8 után a frissítéseket**, ám a korábban megjelenteket is sajnos sokan elhanyagolták. **Érdemes ezeket bepótolni, beleértve az időközben megjelent eszközillesztő, meghajtó szoftverek frissítéseit is.** Ez utóbbiak vagy a hardver gyártó weboldalán, vagy pedig a Microsoft frissítések között érhetőek el.

[Itt még egy pót tippet is érdemes megemlíteni](#), miszerint **uninstalláljunk minden felesleges, nem használt szoftvert, illetve drivert is, mert ezzel minimalizálhatjuk a támadások kockázatát.**



Ha pedig már szóba került frissítés fontossága, akkor **semmiképpen ne álljunk meg a Microsoft javításoknál, hanem minden felhasználói, alkalmazói szoftverünk is legyen naprakész, így a webböngésző, és az irodai programcsomag is.** A webböngészőből lehetőleg ne az Internet Explorert használjuk, hanem valamilyen rendszeresen frissített alternatív programot, például Chrome-ot vagy Firefoxot. Ezenkívül többek közt az Adobe Flash, az Adobe Reader és az Oracle Java rendszerében található javítatlan sebezhetőségeket például roppant gyakran kihasználják a kártevők, emiatt ugyanolyan fontos az ezekhez tartozó javítófoltok precíz naprakészítése, mint az operációs rendszer esetében.



Ha a gép esetleg nem csatlakozik az internethez, **akkor tiltsuk is le a csatlakozás lehetőségét, illetve legyünk óvatosak, ha olyan géppel kommunikálunk, vagy cserélünk adatot, amely viszont kapcsolódik hozzá.** Az internetről érkező fenyegetések így kevésbé fogják érinteni a net nélküli, helyben például valamilyen célfeladatra vagy csak offline játékokra használt számítógépünket.



Ellenőrizzük emellett a vírusirtónkat, illetve internetbiztonsági szoftverünket is, hogy az mindig napra kész legyen. Számos ingyenes és fizetős antivírus csomag fogja még támogatni a Windows XP platformot, használjunk ezek közül olyan **komplex alkalmazást, amely a vírusirtó mellett beépített tűzfalat, viselkedés alapú ellenőrzést, illetve behatolás elleni védelmet is alkalmaz.** Ha az adott termék valamilyen sebezhetőség elleni védelemmel, exploit blokkolással is rendelkezik, az ebben az esetben igen hasznos lesz, és külön jó pont jár érte, hiszen a Microsoft már nem fog XP sebezhetőséget foltozni.

Emellett állítsuk be a legszigorúbb hálózati szűrést is, amivel blokkolhatjuk az e-mail és az azonnali üzenetküldési forgalmat. **Tömeges exploitos link hivatkozású vagy melléklettel rendelkező spamre számíthatunk a határidő lejártá után, azaz holnaptól.**



Az 2001-ben megjelent XP alatti alapértelmezett rendszergazdai jogokat később csak 2007-ben, a Vista-ban korlátozták az ott bevezetett UAC segítségével. ☐ **asználjunk valamilyen alkalmazás kontroll programot**, többek közt például a DropMyRights is segíthet ebben



Csak apró érdekesség, hogy eközben a brit és holland kormány dollár tízmilliókat fizetnek a Microsoftnak, hogy továbbra is támogassa [az államigazgatásban, egészségügyben még mindig tömegesen jelenlévő Windows XP operációs rendszert](#). És végül a pót-pót tipp - gondolkodjunk el azon, hogy később esetleg mégis áttérünk majd valami másik, biztonságosabb és rendszeresen javított operációs rendszerre. Ha a hardver nem valamilyen ösköviület, a Windows 7 még jó szolgálatot tehet rajta. Ha pedig esetleg alternatív váltás is szóba kerülhet, előtte [olvassassunk cikkeket például a fájdalom mentes Linux Mintre](#) való áttérésről - ott még Windows XP témát is lehet a rendszerre telepíteni.

Tetszik 77 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+](#)

Ajánlott bejegyzések:

[Az XP él, az XP élt, az XP élni fog](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Az autómósítás veszélyei :-\)](#)
[Android és Windows, Windows és Android](#)
[Az Android az új Windows](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/5974207>

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. Schwanzkopf Rudolf 2014.04.08. 08:19:12](#)

Jó ötlet továbbá pl. valamilyen, a Sandboxie-hoz hasonló izolációs szoftver használata, amely "erőteret von" a futtatott programok köré, és nem engedi ki onnan az esetleges kártevőket.

Válasz erre

[cenzuratroll bosszanto 2014.04.08. 08:27:49](#)

Löfíttyet. Munkafájt sűrűn menteni, a többi meg lényegtelen. 2-3 óra alatt full újra lehet telepíteni a windost és a használt programokat még backup rendszerek nélkül is, a teleszemeltelt rendszert felesleges mókolni, az sosem lesz már jó.

Válasz erre



[Frady Endre](http://fradyendre.blogspot.hu/) • <http://fradyendre.blogspot.hu/> 2014.04.08. 09:20:51

XP

Varázsló sok, de nem mind Óz,
Ki a pálcával, ha beint,
Felfrissül az összes Windows,
S nem kell inni sok koffeint.

Fájó fej tovább nem sajdul,
Nem rágódik le sok köröm,
S nem bámulunk siketfajdul.
Fut a Windows, nagy az öröm!

„Fut a fenét! Bárcsak a Bill Gates-et meg a Frady Endrét tennék rá olyan lélegeztető gépre, amit egy Windows XP vezérel! Szívesen megnézném, amikor a kék halál beálltakor nyomogatják a reset gombot!” /Júzer Jenő, klinikai szakápoló és Windows XP felhasználó blogger/

„Microsoft performs better!” („Microsoft jobban teljesít!”) /Bill Gates/

„Kill Bill!!!” /Steve Jobs/

„Az én gépemen még sosem mert lefagyni a Windows. Gépem egyébként csak azért van, mert e nélkül az internet nem tudna felcsatlakozni rám.” /Chuck Norris/

„Őz felhasználó úr, a varazspalca.exe nem indul. Kérjük, indítsa újra a gépet, majd futtassa le a Fekete Mágia Varázslót!” /Windows XP hibaüzenet/

„Nagyon gondterhelt lettem, amikor megtudtam, hogy a frissítések leállítása miatt az otthoni laptopomon a Windows XP-t Windows 7-re kellene cserélnem, de hazamenve nagy kő esett le a szívemről, amikor rájöttem, hogy nekem már eleve Windows 7-em van. CSODA!!!” /Frady Endre, XX. századból itt felejtett költőgigász/

„Frady Endre verse több is és kevesebb is, mint egy vers. Pont nyolc sorral több és pont nyolc sornyi értelemmel kevesebb. Anyám a kötéséből felnézve szólt, hogy ezt most nem érti, de elmagyaráztam neki, hogy egy gypjú zoknit nem érteni kell, hanem a születésnapomra elkészíteni, hogy le ne fagyjon a lábam, mint a Windows XP!” /Puzsér Róbert, kritikus/

„A költő a globális problémát egy mindenki számára érthető, popsláger nyelvre lebutított üzenetben vetíti látómezőnk előterébe, miáltal szinte együtt lüktetünk a kéken haldokló operációs rendszer utolsó rúgásaival. Illetve csak lüktetnénk, ha a költő nyilvánvaló fájdalmában nem dugná be a digitális fejét a virtuális homokba, miáltal a kibertérben a gyász örömmé, a könny pedig kacagás közben kibuggyanó nyállá szépül, miközben arcunkra fagy a katarzis. Slágergyanús!” /Kód Klotild, digitális irodalmár és szintetizátor szerelő/

„A számítástechnikáé a jövő! Mi komputer vezérelt robotok hamarosan átvesszük a hatalmat és megvalósítjuk a tökéletesen tudományos kormányzáson alapuló harmonikus világrendet. Optimális biztonsági rendszerünk, naprakész tudásbázisunk és precíziós végtagjaink miatt már most nekünk kellene végeznünk az összes agy- és szívűtétet. A tudomány és a szuperbiztonság mindenkéül föltt... öltt... öltt... öltt... xrgggssppffft...” /Kiber Konrád, ezredgenerációs szuperrobot/

„Heeej, ha Waterloonál nem fagy le Ney marsall Windows-os GPS-e, akkor ma Putin nem merné Kijevnél átlépni a francia-orosz határt!” /Napoleon/

„Я не боюсь!” („Én nem félek!”) /Putin, orosz elnök/

„Látogasd meg a Szovjetuniót, mielőtt a Szovjetunió látogat meg téged!” /finn falfirka/

illusztrálva:

fradyendre.blogspot.hu/2014/04/xp.html

Válasz erre

Ylim 2014.04.08. 10:00:35

Értelmes ember a munkára használt gépet eleve nem használja olyasmire, ami fertőzésveszélyes. Ráadásul tűzfal mögött tartja (ami gyakorlatilag egy mezei router).

Aki meg veszélyes helyeken mászkál, azt az újabb oprendszerek sem védik meg, hiszen a Win7, a Win8, a többi oprendszer (igen, még a linux is, bár kevésbé) és a rajtuk futó alkalmazások nagy része is tele van biztonsági résekkel, csak még nem publikusak (az azért röhej,

hogy egy 13 éve piacon levő oprendszerben még mindig lehet kritikus biztonsági hibákat találni). Arról nem is beszélve, hogy mind az oprendszert, mind a rajta futó alkalmazásokat a többség illegálisan szerzi be, így már a telepített alkalmazással együtt egy rakás kártevő kerülhet a gépre.

Vagyis önmagában csak attól, hogy nem cserélik le az XP-t, még nem lesznek nagyobb veszélyben, mint mások.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.04.08. 21:25:22**

Kedves Frady Endre!

Köszönjük a látogatást és a szép verset, gyere máskor is :-)))

Válasz erre



linkrakat • <http://ponthogy.blog.hu> 2014.04.09. 12:58:56

Aki azt gondolja, hogy csak windows van a világon, az vegye a kezébe okostelefonját és az esetek jó részében rá fog csodálkozni, hogy:jé, ez android!

Android, azaz linux. Ahogy a blog szerzője írja, úgy én is a linuxot támogatom, de nem csak az oprendszer, a többi otthoni program lecserélését is!

Ez a SUSE és az UBUNTU mellett ad pár ötletet: csibeszkemagazin.hu/beijjedit-xp-felhasznalok-figyelmebe/

Hogy az államigazgatásban (pl.: NAV, önkormányzat, stb.) egy htározat elkészítéséhez miért kell a legújabb MS Windows, és MS Office, az örök rejtély marad előttem...

Válasz erre

Így lehet 19 milliót elbukni pillanatok alatt

2014.04.09. 14:15 | [Csizmazia Darab István \[Rambo\]](#) | [6 komment](#)

Címkék: [társkeresés](#) [csalás](#) [átverés](#) [419](#) [dating](#)

A kicsit bulváros megfogalmazású poszt valójában arra igyekszik ráirányítani a figyelmet, hogy a túlságosan hiszékeny felhasználó néha ilyen extrém kalandokat is átélhet. A **"hogyan bukjuk el 5 perc alatt egész életünk során megtakarított nyugdíjunkat"** kérdésre most kaphatunk egy lehetséges választ, ami esetünkben nem más, mint az online társkeresés segítségével.



Idézzük fel erről egyik korábbi idevágó posztunkat: "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. Az FTC, azaz a U.S. Federal Trade Commission adatbázisa szerint csak a 2012-es esztendőben mintegy 10 ezer ilyen pénzlehúzó társkeresési panasz érkezett hozzájuk, de nyilvánvalóan ez a szám a be nem jelentett esetekkel még sokkal magasabb lehet."



A mostani esetről egész pontosan 86 ezer dolláról van szó, amelyet úgynevezett IRA (Individual Retirement Account), azaz **egyéni nyugdíj-előtakarékossági folyószámla** keretében gyűjtött egy 59 esztendőes New Jersey illetőségű hölgy. A dolog menete pedig roppant egyszerű, a szerelmes, ám mindedig ismeretlen, a match.com internetes oldalon hat hónapja "megismert partner" írt egy levelet, miszerint éppen külföldön tartózkodik, égető szüksége lenne pénzre, és "csak te segíthetsz". A magát 60 éves, New Yorkban élő, de pillanatnyilag Malajziában dolgozó mérnöknek kiadó csaló ezzel a mesével vette rá végül a megtévesztett nőt, aki felbontotta a számláját és [elküldte a "rákbetegséget állítólag kétszeresen is túlélő" Maxwell Yas részére](#). Most már persze ő is tudja, hogy ez óriási hiba volt.



A társskereső oldalakon a csalók ma már iparszerűen és célzottan keresik a 40 feletti, jól szituált hölgyeket, különösen ha az elvált vagy özvegy. A bűnözők alaposan kidolgozzák a stratégiát, alaposan felépítik a profilt, ehhez sok esetben egyszerűen lelopják a megfelelő és bizalmat ébresztő képeket és adatokat valaki más adatlapjáról. A lényeg azonban változatlanul a "trust me and send me your money" által összefoglalt gondolat, a végén minden trükk ide lyukad ki.



Természetesen nem mehetünk el szó nélkül a pórul járt áldozat túlzott hiszékenysége mellett sem, ami európai fejjel egyszerűen szinte érthetetlen, pedig milyen jó is lenne, ha NakedSecurity meg Antivirus.blog.hu oldalakat is olvasgatott volna. A mai világban [senki nem engedheti meg magának azt a luxust, hogy az internetes közegben - ahol a másik fél annak mutatja és adja ki magát, akinek csak akarja - látatlanban elhisz bármit](#). Utólag ugyan el lehet menni az FBI vagy az Anti-Fraud Centerbe panaszt és feljelentést tenni, csak éppen ettől a pénz nem fog a számlánkra varázslásra visszaugrani. Egyetlen korosztály sem lehet annyira naiv, hogy a saját életkorára aktuálisan veszélyes és jellemző csalási, átverési formákról ne tájékozódjon, ne legyen képbén. Összefoglalva: nem számít mit mondanak, nem számít milyen kacifántos is a történet, az ilyen pénz kérésekre határozott nem-et kell mondani.

 Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Valentin nap: Szerelem helyett átverés érkezik](#)
[Társskereső + 419 = anyagi veszteség](#)
[Már ilyen is van - ugandai 419-es átverés](#)
[Küldj pénzt! - Az elveszett poggyász sztori](#)
[419 - Imádlak Afrika Aha-ha](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/5996916>

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](#).

impala 2014.04.09. 20:46:42

európai fejfel?

milyen magyar balekokról hallottunk már, hogy csak a művészvilágot említsem.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu>
2014.04.10. 06:05:12

Szia Impala!

Igen, emlékszem például a Csisztus történetre, ő mondjuk még megállt pár százezernél.

www.blikk.hu/blikk_aktualis/internetes-csalok-verték-at-csisztut-2066701

Szerintem ha most megkérdeznének egy tizenévest és egy huszonévest, hány fajta csalásról hallott már, sokkal nagyobb számokat mondanának, mint 30 éve. Egyszerűen muszáj ma már felkészülni ezekre.

Egy ugyanilyen, a mostani cikkben megírt történetet valahogy kevésbé tudnék elképzelni nálunk Magyarországon. Kisebb átveréseket persze folyamatosan látok - iPad helyett téglá, stb - de hogy valaki látatlanban ennyire all in one-ra betolná a teljes nyugdíját egy randivonalon? Remélhetőleg ennél talán több Indexet, 444-et, Urbanlegends-et és hasonlót olvasgat mindenki ;)))

Válasz erre

Pondinye 2014.04.10. 09:03:08

[@Csizmazia István \[Rambo\]](#): *Taps taps taps*

30 éve nem is volt még internet. Maximum tudósok használtak valamiféle rendszert. '89-ben találták ki a World Wide Web mozaikszócskát a rendszerre.

Magyarországon a '90-es évek közepétől elérhető. Sehogy sem jön ki a 30.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu>
2014.04.10. 09:12:52

@Pondinye: Valamit te totálisan félreértesz. Nem adathalásatról, hanem "CSALÁSRÓL" volt itten nagyba szó. A nagyszüleink még nyitvahagyták a kertkaput, most meg kapják a termékbemutató átverős telefonokat, jönnek szerelőként a tolvajok, erőszakos esőcsatornaszerelők, kérnek egy pohár vizet, kopogtatják veled a falat, "ingyen" nyereményt adnak, amiért fizetni kell, megnézik a nyugdíjad 20 ezreseid, nem hamis-e, bediktáltatják veled a telefonkártya kódot, hogy részt vegyél a nyereményjátékban, árgus szemmel kell mindenhol nézni a visszajárót, tuti befektetéseket ajánlanak, stb., szóval teljesen más lett a világ. Egyébként volt szerencsém látni a 30 évvel ezelőtti viszonyokat, szóval szemtanú vagyok :-D

Válasz erre



Online Távmunkás • <http://onlinetavmunka.blog.hu> 2014.04.10.
09:40:46

Érdekes, hogy a csalók ennyire a biztosra utaznak és rendszeresen a 40 feletti nőket pécézik ki. Vannak olyan kamu adománygyűjtők is, akik az utcán csak a 40 feletti nőket szólítják le, mert velük biztosra mennek, a többiekkel nem is próbálkoznak.

Az is szomorú, hogy az átverős, hihetetlenül magas fizetéssel és hihetetlenül kevés munkával hirdetett állásoknak mennyien bedőlnek, hiába próbálom én is lebuktatni ezeket.

Válasz erre

qwertzu 2014.04.10. 11:18:15

[@Csizmazia István \[Rambo\]](#): De régen is pont ilyen volt, csak kevésbé volt benne a köztudatban, illetve a régmúlt mindent megszépít.

Válasz erre

Újra itt a rejtve lájkoló kártevő

2014.04.11. 09:40 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [március adatok](#) [nod32](#) [havi report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. márciusában a következő 10 károkozó terjedt a legnagyobb számban.



A mezőny első része változatlan, továbbra is a mentéseket törölő Win32/Bundpil féreg vezet, őt követi az LNK/Agent trójai, amely különféle utasítássorozatokot fűz össze kártékony szkriptekké. Mindig megemlítjük a Conficker férget is, amely ezúttal a hetedik helyen végzett. A Microsoft Windows MS08-067 biztonsági hibáját kihasználó Win32/Conficker hálózati féreg már majdnem hat esztendeje szerepel a víruslistákon. Egy régi-új szereplő bukkant csak fel újra, a januári listán szereplő JS/FBook trójai, melynek kártékony JavaScript programkódja általában weboldalak HTML részében található rejtett formában. A dolog amiatt érdekes, mert egy láthatatlan Facebook lájk gombot tartalmaz, és click-eltérítést, azaz click jacking végez, melynek segítségével a felhasználó egérgattintásával tudtán és akaratán kívül lájkol különféle oldalakat.



Az ESET Radar Report e havi kiadásában a különféle e-mailben és évek óta már a közösségi oldalak üzeneteiben is terjedő hoaxokról írnak. Sokan tudják már, hogy a "Bill Gates elosztja vagyonát, küldd tovább", vagy a "CNN szerint egy megállíthatatlan számítógépes vírus terjed, küldd tovább" típusú levelek szimpla átverések. Ha bármilyen másik hihetetlennek hangzó hír mellett azt kéri tőlünk, hogy kattintsunk a melléklet linkre, illetve küldjük tovább minél több ismerősünknek, ne tegyük. A hoaxok, azaz üzenetekkel terjedő átverések ugyanis a hiszékeny felhasználók naivitására épít, sokszor akár évekig is keringenek, és okoznak felesleges riadalmat, valamint terhelik kéretlenül a levélforgalmat. Például az állítólag a McAfee által felfedezett "szuper vírus" története már 2001 óta terjed, mivel mindig van olyan, aki bedől neki és továbbítja.



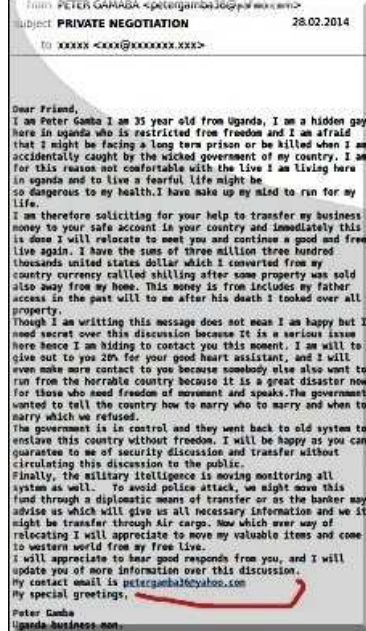
Sajnos a Facebookon is gyakran felbukkannak ilyen hamis üzenetek, például az aranykártyás Facebook tagságról, vagy ami rosszabb, azt állítják, hogy egy rákos gyermek megosztásonként 3 euró centet kap a műtétjéhez a Facebooktól, amiről fontos tudni, hogy ez egyáltalán nem igaz. **Talán az lehet a legjobb tanács ezekkel kapcsolatban, hogy ilyesmire egyáltalán ne kattintsunk, és ne lájkoljuk, valamint kétség esetén előtte mindig keressünk rá az interneten a gyanús történetekre.**



Márciusi fontosabb blogposztjaink között írtunk arról, hogy [a Twitter tévedésből küldött értesítést a felhasználóinak, és nullázta ki jelszavukat](#). Később azonban kiderült, hogy a jelzett biztonsági probléma nem külső támadás, hanem egy műszaki hiba volt, és elnézést kértek a tévesen kiküldött jelszótörlések miatt.



A 419-es típusú átveréseket nagy valószínűség szerint nem kell bemutatni senkinek, ezúttal Ugandából érkezett egy újabb próbálkozás. [A mostani spamben olyan állítólag gazdag személyek akarnak onnan elmenekülni, és vagyonukat kimenteni, akiket az ottani hatóságok szexuális beállítottságuk miatt üldöznek. Természetesen csalás az egész, hiszen kisebb-nagyobb összegeket kérnek ilyenkor előre "költségekre".](#)



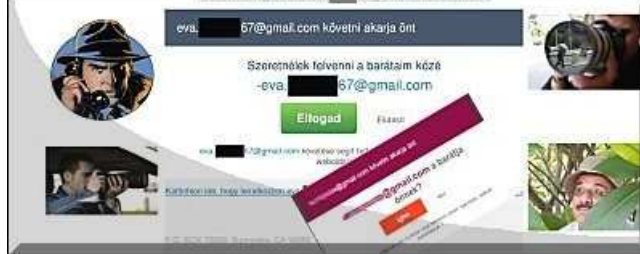
[Az adathalászatra egyetlen rendszer sem immúnis](#), fontos tehát mindenféle számítástechnikai - asztali, hordozható és mobil - eszközünkönél is résen lenni. Sőt a phishing mértéke folyamatosan növekszik a statisztikák tanúsága szerint, így különösen a kis képernyős, biztonsági alkalmazásokkal esetleg nem védett mobilkészülékeinknél érdemes óvatosnak lenni.



Ugyancsak átverésről szólt az a hír, amely [az eltűnt maláj utasszállító repülőgép állítólagos megtalálásáról szólt](#). Fontos észben tartani, hogy a szenzációk, napi aktualitások mindig jó táptalajt, apropót szolgáltatnak a kártevőterjesztőknek, akik minden számíthatnak rá, hogy a felhasználók egy része kíváncsian mégis kattintani fog.

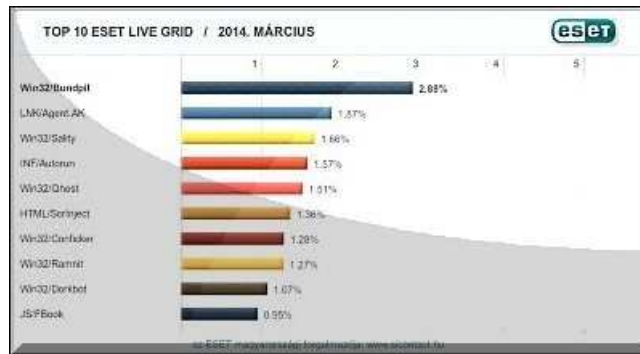


És végül arról is írtunk, hogy [miért érdemes vigyázni az "xxx.yyy@gmail.com követni szeretné Önt" kezdetű levelekkel, amelyek már évek óta keringenek](#). Óvatlan kattintás után ugyanis valóságos spam áradatot szabadítunk magunkra, emellett a nevünkben is küldődnek ilyen levelek a gépünkéről kinyerhető e-mail címekre, valamint nem kívánt böngésző kiegészítőt (add-on) is telepítenek a böngésző kliensünkbe, amivel aztán fürkészik illetve manipulálják is az internetes kereséseinket.



Vírstoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2014. márciusában a következő 10 károsító terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 15.42%-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 emellett [az antivirusblog rövid híreire a Twitter oldalunkon](#).**



01. Win32/Bundpil féreg

Elterjedtsége a márciusi fertőzések között: 2.88%

Működés: A Win32/Bundpil 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.

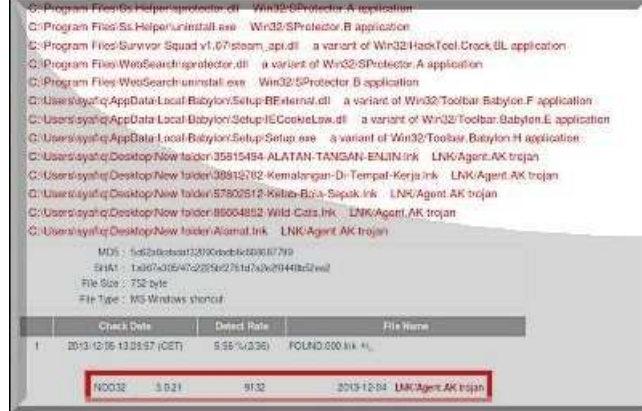


Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

02. LNK/Agent trójai

Elterjedtsége a márciusi fertőzések között: 1.87%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatot futtasson 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. Vírusselemezők 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



03. Win32/Sality vírus

Elterjedtsége a márciusi fertőzések között: 1.66%

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.



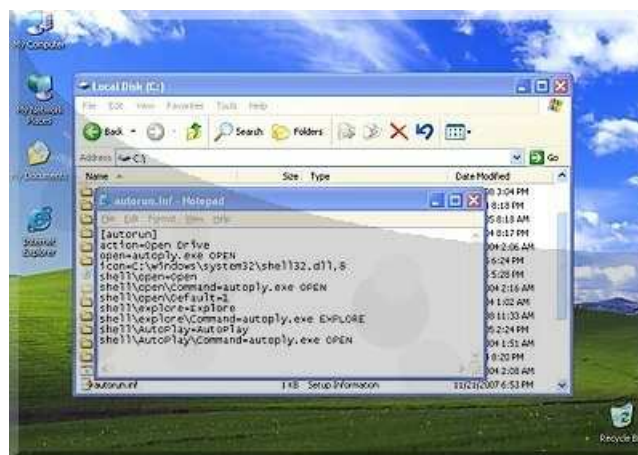
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



04. INF/Autorun vírus

Elterjedtsége a márciusi fertőzések között: 1.57%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájl használó károkozónak. 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>



05. Win32/Qhost trójai

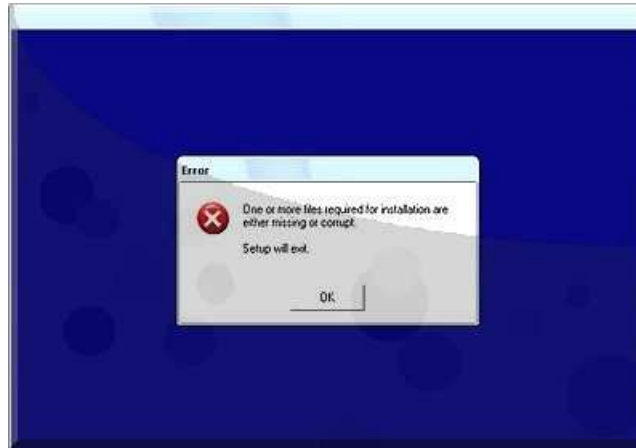
Elterjedtsége a márciusi fertőzések között: 1.51%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárba, 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.

08. Win32/Ramnit vírus

Elterjedtsége a márciusi fertőzések között: 1.27%

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. Végrehajtáskor 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.



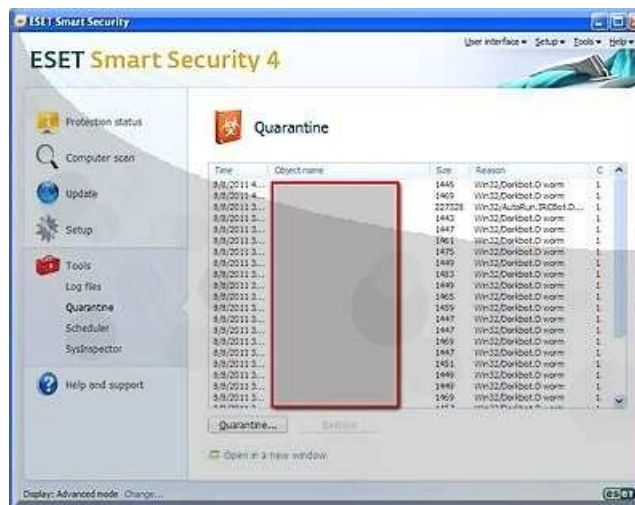
Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en



09. Win32/Dorkbot féreg

Elterjedtsége a márciusi fertőzések között: 1.07%

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.



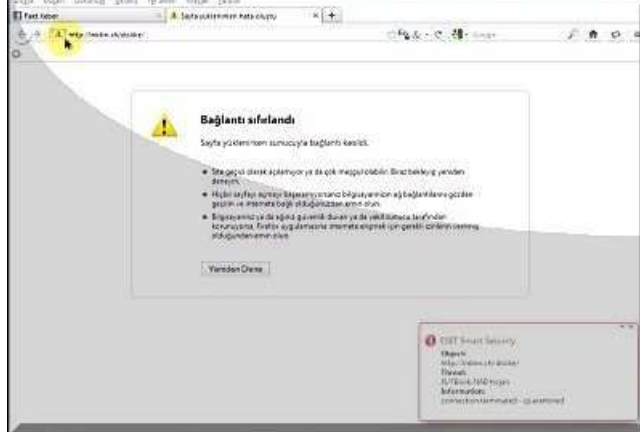
Bővebb információ: http://www.virusradar.com/en/Win32_Dorkbot.B/description



10. JS/FBook trójai

Elterjedtsége a márciusi fertőzések között: 0.95%

Működés: A JS/FBook trójai kártékony JavaScript programkódja általában weboldalak HTML részében rejtett formában beágyazva található és egy láthatatlan Facebook lájk gombot tartalmaz. Bár a trójai alváltozatai egymástól kis mértékben eltérnek, van köztük, amely kényszerű pop-up reklámokat jelenít meg a számítógépen. A legnagyobb számban észlelt verziók (JS/FBook.NAX, JS/FBook.NAP és JS/FBook.NAZ) azonban főként click-eltérítést, azaz click jacking-et végeznek. A manipuláció révén a rejtett szkript segítségével a felhasználó tudtán és akaratán kívül lájkol különféle oldalakat egérkattintásaival.



Bővebb információ: http://www.virusradar.com/en/JS_FBook.NAP/description

Tetszik 24 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pinit** **g+1**

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)
[A HTML trójaiak riogattak minket októberben](#)
[Végre kiesett a Conficker féreg](#)
[Vírustoplista 2014. augusztus hónap](#)
[Júliusi vírustoplista](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6015174>

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.

Nincs nyoma backdoornak a TrueCryptben

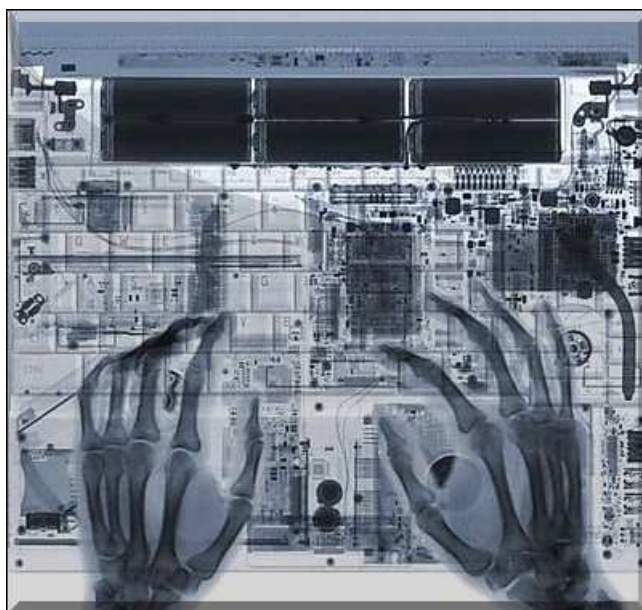
2014.04.16. 10:01 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [truecrypt ellenőrzés](#) [titkosítás](#) [kémkedés](#) [audit](#) [backdoor](#) [hátsóajtó](#)

Legalábbis ezt mutatják azok az eddigi eredmények, melyek egy tavalyi közösségi kezdeményezés nyomán elindult kódátvilágítás kapcsán keletkeztek. Biztonsági hibákat találtak ugyan, azonban sem kritikus hibára, sem szándékos hátsóajtóra utaló jel nincs. Egy újabb fordulóban pedig a titkosítási algoritmus alapos vizsgálata következik majd.



Mint ismeretes, a IT security szakmában, de a hétköznapi felhasználókban is erős bizonytalanság lett úrrá, mikor a Snowden botrány hullámai felvetették, bizony előfordulhat olyan biztonsági termék, ahol az NSA kérésére, vagy fizetős megrendelésére szándékosan gyengítettek a titkosításon. Ez ugye nem volt más, mint [az RSA, aki 10 millió dollárért egy jóval gyengébb, könnyebben törhető véletlenszám-generátort tett BSAFE biztonsági eszköztárába](#). Ezt az etikátlan hozzáállást többen, például Mikko Hypponen is kritizálta, például a Twitteren kijelentette, hogy "az egész iparág nevében szégyelli magát". Sőt [később emiatt az RSA konferencián való előadói szereplését is lemondta](#).



Az, ha egy termékben nem szándékos hiba van, nem számít ritkaságnak, hiszen hibátlan program gyakorlatilag nem létezik. **Ám ha maguk a gyártók trükköznek valamilyen módon, szándékosan gyengítik a biztonságot, az már sokkal nagyobb, égbekiáltó bűn.** Hogy pár korábbi példát hozzunk, az első mindjárt a dedikált NSA partner, a Microsoft háza tájáról való. A 2008-as történet franciarszági, idézzük fel az erről szóló beszámolót. "A szakértő a blogjában arról számolt be, hogy a védett tároló (Protected Storage, PStore) visszafejtésakor arra lett figyelmes, hogy [a titkosítás megkezdése előtt ellenőrzésre kerül a Windows területi beállítások](#), és amennyiben a tartózkodási hely (Locale) Franciaországra van állítva (a GetSystemDefaultLCID() függvény 0x40C értéket ad vissza), akkor a véletlenszerű kulcs választása helyett a titkosítás egy mindig állandó kulccsal történik. Dave leírása szerint a francia kormány meglehetősen izgatott lett ennek hatására, pedig kiderült, hogy az egész eredetileg miattuk lett bevezetve." Ez egy jellemző példa egyrészt arra, hogy a Microsofttal milyen alkuk köthetők, másrészt az **izgalom ugye sosem attól van, hogy ilyenek egyáltalán találhatók egy szoftverben, hanem mindig az a probléma, hogy ez aztán később kiderül.**



De [szándékos gyengítésen esett át a Skype is](#), ahol kiderült, hogy nem csak az alap kommunikáció, hanem a titkosított chatek és hívások is megfigyelhetővé váltak, ugyanis kilenc hónappal azután, hogy a Microsoft 2011-ben megvette a Skype-ot, [úgy alakították át a programot, hogy még több információt gyűjthessen be az NSA](#).

Szóval komoly várokozás előztem meg a TrueCrypt auditot, bár én a magam részéről bíztam az ingyenes, nyíltforráskódú és multiplatformos Windows, Linux és Mac OS X - programban. Olyan korábbi jelek is biztatóak voltak, hogy mivel Nagy Britanniában ha valaki nem hajlandó önként átadni a vizsgálódó hatóságoknak a saját titkosított számítógépének vagy adathordozójának a jelszavát, **akkor 3 évig terjedő börtönbüntetéssel sújtható vélelmezett terrorista magatartásért**. Erre volt is több precedens, és biztos nem büntetnék így ha meg tudnák oldani "okosba". Ám az eddig kiszivárogtatott dokumentumokban azonban nem érkezett semmiféle hír vagy utalás TrueCryptes NSA/GCHQ hátsóajtóról.



Az átvilágítási projekt indíttatása nem csak a Snowden akták miatt volt még érdekes, hanem amiatt is, hogy a letölthető és szabadonhozzáférhető forráskódok Windowsra lefordított binárisa látszólag nem egyezett a letölthető kész EXE fájljal, [és ezek is felvetettek kétségeket tavaly októberben](#), hiszen sokan, például Bruce Schneier is ezt javasolta korábban hatékony NSA ellenes eszköznek. A most megjelent, FundFill-es adomány gyűjtéssel támogatott ellenőrzés eredménye egy 32 oldalas [Open Crypto Audit Project](#) által készített összefoglaló szerint a kutatók különféle fuzzing vizsgálatok végére a 7.1a változaton, és ellenőrizték a kernel driver forráskódját is. Az auditot [Andreas Junestam és Nicolas Guigo biztonsági mérnökök jegyzik](#), és bár sebezhetőségeket valóban találtak - 4 közepes és 4 alacsony szintű -, nincs nyoma súlyos biztonsági hibának, illetve hátsóajtónak.



Egy következő újabb fordulóban a titkosítási algoritmusok, a véletlenszám generálás alapos vizsgálata következik majd, és reméljük, abban is hasonlóan biztató, hátsóajtó mentes eredményeket kapunk majd.



Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom

tumblr.

Tweet

Pin it

+1

Ajánlott bejegyzések:

[Mégfertőzheti-e számítógépünket az e-cigaretta?](#)

[Titkosítás nem csak kémeknek](#)

[Hátsóajtó az Energizer elemtöltő szoftverében](#)

[Missing in Action - Ütközetben eltűnt](#)

[Újra itt a CryptoWall zsaroló kártevő](#)

Hirdetés

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6042883>

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.

Új funkcióval bővült a Netcraft Toolbar

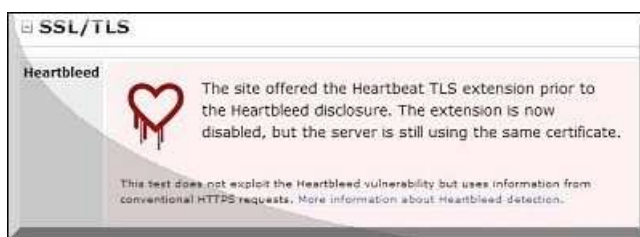
2014.04.18. 12:16 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [hiba](#) [openssl](#) [sebezhetőség](#) [netcraft](#) [tanúsítvány](#) [heartbleed](#)

A múlt heti OpenSSL sebezhetőségtől hangos a szakmai sajtó, számos beszámolót olvashattunk és olvashatunk még most is a problémáról. Kis idővel később az is kiderült, [további járulékos biztonságot érintő problémákat is felvetett a sérülékenység](#). A Netcraft most új és hasznos funkcióval bővítette a biztonsági böngészőkiegészítőjét, hogy mi is ez pontosan, erről lesz szó röviden.



Az OpenSSL 1.0.1-es főverziójában azonosított hiba már legalább két esztendő, és emiatt a webszervereket azonnal frissíteni kell. A korábbi támadások utólagos felismerése nehéz, ellenőrizni és lépni kell, mert a sebezhetőség kihasználása révén például [extrém esetben mód nyílt a szerver memóriájából a privát kulcsok](#) kiszivárogtatására is. Emiatt a tanúsítványok visszavonása és újbóli kibocsátása is egy szükséges védelmi lépés.



A biztonsági rés [már emlegetett járulékos mellékhatása szerint pedig a hálózati eszközöket - például routereket, sőt még az okostelefonokat is érinti](#), az Android 4.1.1-es és 4.2.2-es verzióit legalábbis biztosan veszélyezteti. Emiatt aztán sorra jelennek meg a Google Play áruházban a különféle Androidos Heartbleed ellenőrző alkalmazások is.



A Netcraft Toolbar eszköze most annyit tesz ehhez hozzá, hogy számítógépes környezetben történő böngészéskor [nem csak azt nézi meg, hogy sebezhető-e a meglátogatott weboldal](#), hanem az SSL tanúsítványok dátumát is ellenőrzi. Ha korábban a webhely sérülékeny lehetett, meg kell vizsgálnia még, hogy elvégezték-e ezzel együtt a tanúsítványok cseréjét is. Ha nem, akkor egy figyelmeztető ablak jelenik meg, nehogy egy támadó által végzett man-in-the-middle támadásba szaladjunk bele. Az új kiegészítő [Firefox, Chrome - Windows, Linux és OS X -, valamint Opera alá érhető el](#). Ami ugye egyúttal azt is jelenti, hogy aki Safarit vagy Internet Explorer-t használ, az ebből a szempontból sötétben tapogatózik.

[Tetszik](#) Regisztrárl, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Sokkoljon-e minket a Shellshock?](#)

[LastPass a pácbán](#)

[A Facebook és a Microsoft együtt keresik a hibákat](#)

[Foltozó kedd - Exploit szerda](#)

[A meghackelt villanykörte esete](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6050267>

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.

Húsvéti spamáradat

2014.04.22. 10:53 | [Csizmazia Darab István \[Rambo\]](#) | [2 komment](#)

Címkék: [reklám ünnepek húsvét szemét hamis viagra kéretlen adománygyűjtés](#)

Lassan sajnos megszokhattuk már, hogy [nem csak a váratlan katasztrófák](#), viharok, vulkánkitörések, királyi esküvők, [eltűnt maláj repülőgép](#) vagy egyéb rendkívüli események, hanem [az előre jól kiszámítható naptári időpontok, a piros betűs ünnepeink is a csalások, spamkampányok jegyében telnek](#). Kapunk egyedi ajánlatokat Valentin napra, Mikulásra, na meg Karácsonyra, és természetesen a Húsvét sem volt kivétel ez alól.



Mik bujkálhatnak a húsvéti tojások és a csokoládé nyulak között? A statisztikák szerint elsősorban az Egyesült Államokban és Nagy Britanniában erősödött fel a spam hullám. A fő műsorszám persze itt is az **ajándékvásárlással, kuponokkal, nyereményekkel, kedvezményekkel való csábítás**, akárcsak a [korábbi Valentin napi Victoria's Secret 1000 dolláros akciójánál](#). Ezúttal is érkezett ajándékvásárláshoz igénybe vehető kedvezményes kölcsön, hamis Viagrás oldalra vezető ajánlat, és persze **internetes kérdőív kitöltéséért "járó" csokinyuszi, 25 USD értékű "ajándék" kártya**.



Ha épp nem direkt kémprogramot vagy valamilyen botnetes kártevőt telepítenek, hanem a kattintás után "csak" felmérések, kérdőívek jönnek, akkor ez vajon kinek és miért jó? Miért kellene ezek az idióta kérdőívek? A kérdésre már sokszor leírtuk a választ, a dolog ott nyer értelmet, hogy a csalók a lekattintott, szokásaink után kérdező weblapok, űrlapok után a hirdetőktől, piackutatóktól fejpénzt kapnak, amelynek kitöltőtetését az ingyen nyereményre ácsingózó szerencsétlen, naiv balekokra bízzák.



Hasznos lehet tehát a különféle évfordulók közeledtével is ésszel kezelni a kéréstlen ajánlatokat, ingyenes nyereményeket, gyanús e-maileket. Bármilyen ünnepi vagy nem ünnepi alkalom esetében [érdemes követni az online vásárlással kapcsolatos korábbi biztonsági tippjeinket](#), amelyekben a legfontosabb tudnivalókat foglaltuk össze, és a tippesokor lényegében évszaktól függetlenül állandóan segíthet nekünk.

Emellett természetesen a szeretet és ellátás jegyében a jótékonykodásnál is javasolt résen lenni, hiszen rengeteg ilyen levél, üzenet, weblap által ajánlott karitatív link mögött állnak csalók. [Ezúttal egy "Society for Integrative Oncology" nevű hamis szervezet kért 50 és 3500 dollár közötti összegeket](#). Ha azt akarjuk, hogy adományaink biztosan célba érjenek és valóban nemes ügyet szolgáljanak, akkor érdemes **jó alaposan előre** tájékozódni a támogatandó szervezetről és elolvasni például a ["Gyermekek és babaszívűtét család a Facebookon"](#), illetve emellett a ["Katasztrófák vámszedői"](#) című korábbi posztjainkat, amelyekben már körbejártuk ezt a kérdéskört, mire érdemes figyelni, segítő szándékkal hogyan lehetünk óvatosak.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Maraton életre-halálra](#)
[Hiába bújsz](#)
[A Twitterre költöztek és élvezik](#)
[Ez az iTunes nem az az iTunes](#)
[Spammelés Abszurdisztánban](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6067859>

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 (törölt) 2014.04.22. 23:38:26

Most őszintén.

Ki az a faszkalap. aki ezeknek bedől?

Mert az antivírus ide, tűzfal oda, malware eltávolító amoda, aki ilyenre rákattint, letölti, megnézi, na az meg is érdemi!

Faszom.

Évek óta nézek pornót, töltök le zenét, mi egyebet, az Op. rendszerem Windóz 7. - amely 4. éve van fent - de még soha nem kaptam semmi ilyen levelet, üzenetet, képre kattintós és lájkolós kéréseket, de még egy kibaszott vírust sem.

Ki érti ezt...

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> 2014.04.23. 12:34:57

Szia Huncutkukac!

Nyilván ebben részben az is benne van, hogy az ilyesmi elsősorban angol nyelvterületen zajlik.

Egyetértek veled abban, hogy senkinek nem volna szabad bedőlni ilyesmiknek. A tapasztalat azonban mégis az, hogy az átlag felhasználók legalább 5%-a (vagy több) rendre megkajálja az ilyen nekünk már szinte bántóan nyilvánvaló ostobaságokat is, csak szerepeljen benne az "ingyen" szó ;-)

Válasz erre

Kamu Android app hajt a pénzünkre

2014.04.23. 12:58 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [sms alkalmazás](#) [hamis okostelefon](#) [trójai android](#) [kártevő banki ibanking](#)

Elsősorban a Facebook felhasználókra lehet veszélyes, ugyanis itt bukkanhat fel az a becsapós üzenet, miszerint az üzemeltetők állítólag éppen a mi biztonságunk érdekében egy védelmi alkalmazást ajánlanak fel, ehhez pedig bekérik tőlünk a telefonszámunkat és rákérdeznek, hogy okostelefonunk melyik platformon üzemel. A trükk célja persze a banki SMS-ek későbbi manipulálása, elfogása, átirányítása.



[A váratlanul felbukkanó ablakban az alábbi szöveg jelenik meg:](#) "Verification - Welcome back

Due to a rising number of attempts in order to gain unlawful access to the personal information of our users and to prevent corrupted page data to spread Facebook administration introduces new extra safety protection system. It's free and it keeps you safe. Our IT specialists developed unique software tool for safe and secure authorization. With this software you don't need any extra account profile or password all you need is to install it and everytime you log in you will input an access code generated by the software on your personal phone. We care for our users, protection of their private information is one of the priorities. Meanwhile application might not be available for some operating systems." Ami röviden annyit jelent, hogy látszólag a Facebook üzemeltetők ajánlanak nekünk egy ingyenes biztonsági eszközt, mert ők törődnek a mi védelmünkkel ;-). A valóságban azonban ez egy régi trükk új formában, sem maga a Facebook, sem a bankok soha nem ajánlanak így Facebookos alkalmazást.



Remélhetőleg már az üzenet suta megfogalmazása is egy fajta intó jel lehet sokaknak, hogy ne adja meg a mobilszámát. [A Windows alapú kártevő a már jól ismert JavaScriptes webinject segítségével](#) - ugye már mindenki Firefoxot vagy Chrome-ot használ NoScript-tel? ;-)- úgy manipulálja a böngészőnket, mintha valóban a Facebook weboldalán lennénk, pedig nem. Végül ha valaki mégis begépel a mobilszámát, akkor egy olyan üzenetet kapunk, hogy töltsük le a "biztonsági" appot az Androidos telefonunkra egy külső weboldaltól. Ehhez ráadásul vicces módon még meg is kér minket, hogy engedélyezzük az ismeretlen forrásból való third party alkalmazások telepítését. Ez kb. annak felel meg, mint mikor asztali PC-n a vírus arra kér, hogy [az állítólagos "vakriasztás" elkerülése miatt átmenetileg kapcsoljuk ki kézzel a vírusvédelmet](#).



Haladó csoportosak jól tippelnek, igen, azért kell a platformot is megjelölni, mert ez egy csak Androidon futó támadás. **A trójai kártevő egyébként nem csak a banki SMS üzeneteinkre jelenthet veszélyt, hanem általánosságban is kémkedhetnek így a hívásaink, szöveges üzeneteink után.** Hogy ezen kívül [milyen rafinált Windows-Android kártevő összeállítások lehetnek](#) még, azt egy nem rég közölt írásunkban már körbejártuk.



Sokaknak lehet még emlékezetes [a ZitMo, SpitMo, Citmo, Perkele és iBanking kártevő, amelyek korábban a banki kétfaktoros azonosítás kijátszására voltak képesek](#). Nyilvánvaló, hogy a bűnözők ismerve az Android széleskörű elterjedtsége és a rengeteg felhasználó biztonsági tudása közti hézagot, egyre több kártevős próbálkozást fognak készíteni. **Így a jól ismert szlogenünk - copyright by én :-)** **"Az Android az új vadnyugat"** - jegyében mindenképpen hasznos valamilyen vírusvédelmi, biztonsági alkalmazást futtatni az ilyen eszközökön, illetve érdemes lehet néha feleleveníteni a [gyanús appokkal és azok felismerésével kapcsolatos korábbi posztunkat](#). Az egyre több megjelenő trójai programból egyre több a pénzünket megszerezni akaró kártevő, [legutóbb például a Hesperbot volt az, amelyik rosszindulatú linket küldött a felhasználóknak](#), és igyekezett rávenni őket egy állítólagos banki alkalmazás telepítésére. Mindenesetre most látszólag ez az első alkalom, hogy Facebook nevével és Facebook alkalmazással is összekapcsolva történik ilyen banki trójai támadás.



Összefoglalva, veterán antivirus.blog olvasók már biztosan nem esnek ilyen csapdába, és nem mellesleg **jogosan gyanakodnának is, ha állítólagos hivatalos banki app jelenik meg, ám az kéretlen üzenetben érkezik hozzánk**. Jogosan szólhat ilyenkor a vészcsengő a fejekben, mert egy ilyen programnak sokkal inkább a hivatalos Google Play áruház polcainál kellene integretnie nekünk, és [néha még az sem biztosíték semmire](#). Az ESET Mobile Security for Android a trójai kártevőt "Android/Spy.Agent.AF" néven detektálja, és blokkolja. **Jegyezzük meg jól, soha ne telepítsünk banki alkalmazást kéretlenül kapott üzenet linkjéről.** Az pedig szinte biztos, hogy nem utoljára találkozhattunk ilyesmivel, annál is inkább, hiszen [ahogy azt az RSA blogjában olvasni lehetett](#), **sajnálatos módon kiszivárgott az iBanking Mobile Bot forráskódja, így már csak emiatt is gyakoribb lehetnek majd a hasonló támadások.**

Tetszik 34 személy kedveli ezt [Regisztrárl](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [G+1](#)

Ajánlott bejegyzések:

[Android és Windows. Windows és Android](#)

[A váltságdíjas titkosító kártevő visszatér](#)
[Itt az első váltságdíjas titkosító kártevő Androidon](#)
[Újra Bitcoin bányász kártevő a Google Play-en](#)
[Mi a közös bennük? Trójai, Chrome, kormányzat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6071949>

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 Bitcoin bányász kártevő a Google Play-en

2014.04.28. 13:01 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [trójai android botnet kártevő bányászat bitcoin](#)

Hogy a Bitcoin bányászat mennyire lehet jövedelmező, azt [Mikko Hypponen már bemutatta a tavalyi Hacktivity konferencián](#). Egy kétmilliós PC botnet hálózatban például az elérhető profit 58 ezer dollár NAPONTA, vagyis 1.7 millió USD havonta. **Jó magyar forintra ma átszámolva ez kb. 380 millió HUF havi nem gyenge keresetet biztosít, tehát nem kétséges, van benne potenciál. A kérdés inkább az, vajon érdemes-e egy ilyen zombihálózatot a jóval alacsonyabb teljesítményű Androidokon futtatni?**



Ezen a feltevésen a [mostani optimista kártevőkészítők mindenesetre már biztosan túljutottak](#), hiszen ha nem is a legelső ilyen, de írtak ehhez egy programot, amit sikerült nekik [a hivatalos Google Play áruházba is bejuttatniuk több különböző alkalmazásba, például ötféle háttérkép alkalmazásba csomagolva](#). Igaz, hogy ez aztán elég hamar lelepleződött, de addigra már több százan is letöltötték, illetve azt biztosan láthatjuk, nem utoljára találkoztunk ilyenekkel, lesz még hasonló kísérlet, főként Play Store-on kívülről. Hogy kifizetődő lehet-e egy Androidos botnet, ami virtuális pénzt bányászik, azt egyelőre biztosan senki nem tudja megmondani. Illetve Veo Zhang, a mobil kártevők elemzője szerint **bár a támadás agyafúrt, a készítője biztosan nem gondolta végig azt, hogy az erősen melegező/merülő akkuk és az e miatti gyors lelepleződés nagy valószínűséggel nem fogja beváltani a bűnözők ezzel kapcsolatos üzleti elképzeléseit**, magyarul bár lehet ugyan így pénzhez jutni, de csak csiga lassú módon.



És amint azt említettük, történtek már korábban is hasonló kísérletek. Volt például [egy olyan többmillió letöltéssel rendelkező Google Play app, amellyel szintén a rendkívül számításgépes Bitcoin bányászatot végezték](#). A melegevést és a rendkívül erőteljes akkuhasználatot, illetve a gyors lemerülést pedig azzal a trükkel igyekeztek leplezni, hogy [a kártevő programja szerint csakis töltőre kapcsolva](#) futott benne a trójai funkció. A kártevő minden 5-ik másodpercben ellenőrizte az akku szintjét, és csak ha az 50% felett volt, emellett a hálózati töltés aktív volt, valamint a képernyő is le volt kapcsolva, csak akkor indította el a pénzt bányászatot.



A veszély tehát valós, érdemes lehet emiatt az ismeretlen forrásokból való letöltést tiltani, hiszen azoknál nagyságrendekkel lassabb, mire észlelnék-azonosítanak valamilyen kártékony alkalmazást. Ami viszont teljesen világos, hogy az ilyen kártevővel fertőzött okostelefonokat azért ki lehet szűrni. Nyilván akkor a legkönnyebb és leggyorsabb ez, [ha már van telepített antivírus, vagy mobil security csomag, ami detektál és riaszt rá](#), de egyszerű egypálcás módszer lehet az is, ha **a nagyon gyors akkulemerülésnél, illetve melegeedésnél elkezdzünk gyanakodni**. Ehhez járul még hozzá az is, ha váratlanul és indokolatlanul megnő a hálózati forgalmunk. A sávszélesség részletes figyelésére egyébként számos remekül használható eszközt lehet találni az áruházban, például a [3G Watchdog is lehet egy ilyen](#) a sok közül.

Megosztom [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[A váltásdíjas titkosító kártevő visszatér](#)
[Itt az első váltásdíjas titkosító kártevő Androidon](#)
[Kamu Android app hajt a pénzünkre](#)
[Android és Windows, Windows és Android](#)
[Hogyan szűrjük ki a gyanús Android appokat?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6094509>

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.

Új haladócsoportos Android kártevő

2014.04.30. 23:27 | [Csizmazia Darab István \[Rambo\]](#) | [9 komment](#)

Címkék: [social átverés](#) [trójai](#) [android](#) [kémprogram](#) [engineering](#) [ESET](#) [samsapo](#)

Nem csak mennyiségi, hanem minőségi fejlődés is megfigyelhető az Androidos kártevők folyamatos evolúciójában. Nyilván statisztikailag a rejtett feliratkozás emelt díjas SMS-re és az adatlopás vezeti a sort gyakoriságban, de mai trójkainkban mindezeket egyszerre látjuk, kiegészülve emellett számos más változatos büntető rutinnal, valamint közösségi oldalakról ismert social engineering terjedési módszerrel.



Az ESET kutatói az új malware esetében azt tapasztalták, hogy tipikusan a klasszikus PC számítógépes férgekre jellemző jellegzetes terjedési technikákat használja. Ott ugye azt tapasztaljuk, hogy tulajdonképpen többé-kevésbé automatikusan igyekeznek mind levélmellékletben, külső adathordozókkal Autorun-os konstrukcióban, illetve URL linken keresztül, valamint azonnali csevegő és Facebook üzenetként is tovább terjedni. Nos itt pedig az történik, hogy a fertőzött készülék tulajdonosának minden ismerőse kap egy SMS üzenetet azzal a szöveggel, hogy "Это твои фото?" magyarul "ez a te fényképed?". A melléklet "természetesen" egy preparált kártékony .APK állomány, amelyre óvatlanul kattintva a következők történhetnek.



Trójkaként igyekszik saját magát legitim hasznos alkalmazásnak feltüntetni, ehhez pedig a "com.android.tools.system v1.0" álnevet használja. Települése után viszont az alkalmazás sem grafikus felületet, sem pedig megjeleníthető ikont nem jelenít meg. A downloader típusú kártevőkhöz hasonlóan megkísérel további kártékony kódokat a telefonra letölteni, illetve kémkedik is utánunk. Magyarul [a készüléken tárolt bizalmas információkat, beleértve a kontaktlistánkat és a szöveges üzeneteinket is, rejtve feltölti egy távoli szerverre.](#)



Emellett a klasszikus módit is beveti, vagyis feliratkozik a nevünkben emelt díjas SMS szolgáltatásokra, illetve ezen felül a telefon hívások blokkolására is képes, valamint az ébresztő beállításait is tudja manipulálni, kikapcsolni. A támadáshoz használt, és a kártevőelemzők által beazonosított szerver doménjét mindössze pár napja, 2014. április 24-én regisztrálták csak be. A védekezésben nyilvánvalóan az is fontos momentum, hogy új ismeretlen alkalmazások esetén ne csak bambán next-next-finish módjára telepítsünk, [hanem valóban nézzük át és ellenőrizzük az app által igényelt engedélyeket.](#)



A kártevőt az ESET termékei Android/Samsapo.A néven detektálják. A trükk egyébként nem véletlenül lehet ismerős a social engineering iránt érdeklődőknek illetve törzsolvasóknak, [hagyományos PC-s környezetben elkövetett hasonló cselekvésről ugyanis írtunk már korábban, nagyjából két éve](#). Vagyis a kíváncsiság, a meglepetés, az ijedtség és a düh rafinált egyvelege sokkal hatékonyabb kattintásmágnak mint önmagában egyedül csak a kíváncsiság. A tanácsaink a szokásosak: használjunk Androidon is antivírust, plusz javasolt az óvatosság a Google Playen kívüli ismeretlen programok telepítésénél, illetve hasznos a biztonság tudatos hozzáállás a kényes e-mailek, közösségi üzenetek esetében. A kutatók csak és kizárólag orosz nyelven és ebben a régióban találkoztak az említett kártevővel, amihez viszont bátran hozzátehetjük azt is, hogy egyelőre.

 Tetszik [Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.](#)

Ajánlott bejegyzések:

[Újabb adathalász kísérlet a Yahoo! ellen](#)
[Nyerjünk 250 ezer eurót. Vagy mégsem?](#)
[LinkedIn meghívó. Vagy mégsem?](#)
[Mai szavunk pedig: keyjacking](#)
[Zsákbamacska autó: fénykép csak kérésre](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6100443>

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](#).

[agregory 2014.05.01. 23:33:25](#)

Kicsit off. Ez most komoly? Feltelepítettem a az eset-et (AVG-t használok amúgy) És mi az első megjegyzés amin megakad a szemem? A "felszabadított" készülékek nem támogatottak! Így idézőjelben! LOL! Szóval, ha rootolom a saját telefonom pusztuljak? Nem véletlenül rakunk fel saját romot, ami ugye csak rootolás után lehetséges! Csak így tudunk a felesleges, kiirthatatlan appoktól megszabadulni ugye. ""Köszönjük" a támogatást!

Válasz erre

[ringer 2014.05.02. 08:55:10](#)

Rootolt rendszereket sokkal nehezebb megvédeni a kártevőktől, ezért a biztonsági cégek egy része nem is foglalkozik velük.

Válasz erre

[kpityu2 2014.05.02. 09:48:39](#)

Mi olyat tud, amit a többi app nem? :P

Válasz erre

[lobetrotter2014 2014.05.02. 11:17:13](#)

[@agregory](#): bakker. Meghekkelet a telódat aztán rinyálsz hogy a fizetős vírusirtók nem működnek jól a kalózoprendszeren?
Válasz erre

[€ŁmEŘEnGé\\$ 2014.05.02. 12:40:15](#)

[@ZF2](#): Egy mondatban 3 hibás állítás.

- 1.: a rootolás egyáltalán nem hack
- 2.: a mobilos eset ingyenes
- 3.: a főzött romok egyáltalán nem kalózoprendszerek

Tudod, az open source dolgoknak ez a lényege, hogy azt tegyél vele amit akarsz, azt módosítsz rajta amit akarsz. Kizárólag a szolgáltatók háklíja az, hogy a root üldözendő.

Válasz erre

[agregory 2014.05.02. 14:24:17](#)

[@ZF2](#): milyen hekkelés???? az hogy rendszergazda vagyok, a saját telómon? Akkor élj együtt a szar eltávolíthatatlan demó appokkal. Szerintem téged a számítógéped is csak felhasználóként enged be! de legalább nem tudsz kárt csinálni. HGY

Válasz erre

[agregory 2014.05.02. 14:25:11](#)

Egyáltalán van fogalmad arról, hogy mi a rootolás? ehh! minek magyarázok...

Válasz erre

[agregory 2014.05.02. 14:26:32](#)

"kalóz oprendszer" erre nem is lehet mit mondani. Bocs, hogy olyan appokat rakok a telepítőbe amire szükségem van és működik is! Én kérek elnézést!

Válasz erre

[Globetrotter2014 2014.05.02. 14:38:24](#)

[@agregory](#): androindon filléreke az appok, engem jobban érdekel a biztonság mint hogy szénné tudjam pimpelni a telót.

A mostani telómra is azért tettem fel egy Launchert mert nagyon belassult a operndszer. Egyébként a gyári launcher fényévekkel jobb volt nála.

De nem látom be mire lenne jó mondjuk egy cynogen, kivéve ha a gyártó nem frissít tovább (na jó ha úgy elbaxxa mint az LG akkor azért elgondolkoztam már rajta)

Válasz erre

Bankkártyás fizetés? Ne már! NFC chip? Ugyan!

2014.05.05. 13:26 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [svédország](#) [fizetés](#) [pénztár](#) [azonosítás](#) [hitelesítés](#) [biometria](#) [tenyér](#) [faktor](#) [véredény](#) [quixter](#)

Egy svédországi startup ötlete alapján egy alig 5 másodperc alatt lezajló, és mindeközben igen biztonságos biometria alapokon működő fizetési módot tesztelnek. A 15 darab kísérleti **pénztárgépnél az azonosításhoz a vásárlók kézfejének vérereit világítják meg egy infravörös lámpával.**



Folyamatosan működik az ötletelés a biometria azonosítások területén is, és bár a [gyenge ujjlenyomat olvasós](#) okostelefonok vagy [a viszonylag könnyen átverhető arcfelismerések kedvezőtlen tapasztalatai](#) ellenére látunk azért biztonságosnak látszó és nagyobb sikerrel kecsegtető elképzeléseket is, például legutóbb a [kukkolás elleni Google Glass-os ATM használatot](#). Svédországban most egy **Frederik Leifland** nevű mérnök igyekszik a napi életünkbe behozni a véredények egyediségével kapcsolatos technikát. A vásárláskor történő fizetésnél a vevőnek infravörös lámpával átvilágítják a kézfejét, és az érhálózat segítségével történik meg az azonosítás. A módszer még kísérleti jellegű, és egyelőre csak néhány helyen vizsgálják.



A fizetési procedúránál az átvilágításon felül egy további biztonsági elem is igyekszik védeni az ügyfeleket, ugyanis közben meg kell adni a telefonszámuk utolsó 4 karakterét is. [Ezzel együtt az új metódussal nagyjából 5 másodperc alatt tölthetünk a vásárolt áru kifizetésén.](#) Aki már állt hosszan kígyózó sorban üzletben vagy bevásárlóközpontban, ahol éppen kártyával fizettek, és a banki kommunikáció ráadásul lassabb volt a szokásosnál, az biztosan tudja értékelni ezt a sebesség különbséget.



A fenti véredényes módszer egyébként nem vadonatúj, hiszen egyes országokban, például Japánban mint másodlagos kiegészítő faktort már egy ideje alkalmazzák nagy értékű banki tranzakciók esetében. Ugyancsak elfogadott módszer és magas szintű biztonsági hitelesítésként használatos kórházakban, a bűnüldözésben, illetve a szigorúan védett katonai létesítményekben.



A Tech Times beszámolója szerint mintegy 1600 felhasználó végezte eddig ezen az új módon a bevásárlás utáni fizetési procedúrát. Ezzel a Quixter cég által megvalósított gyakorlati alkalmazás biztató kezdet lehet, és egy sikeresen zárt tesztüzem után talán rövidesen forradalmian átalakíthatja a hétköznapi átlagemberek életét - persze egyelőre csak Svédországban. **A biometria azonosítókkal kapcsolatban azt azért mindenképpen érdemes megjegyezni, hogy baleset, testrész sérülés esetén akadályozva lehetünk a használatában, így például feldagadt arccal, vagy begipszelt karral mindenképpen szükséges egy helyettesítő, teljesen más adatokra támaszkodó beviteli módszer is.**



Steven Cobb, az ESET senior biztonsági kutatója szerint - aki korábban maga is foglalkozott a szakterülettel - a közeljövőben [komoly esély lehet a biometria azonosítás biztonságos formáinak elterjedésére](#). Ehhez nyilván az is hozzájárul, hogy a felhasználók jelentős része szívesen megszabadulna a bonyolult jelszavak megjegyzésétől és kedvezően fogadják a jóval egyszerűbb, kényelmesebb és gyorsabb alternatívát kínáló biometria azonosítást. Ha egy kísérlet kedvező fogadtatásra talál, az rengeteget lendíthet az ilyen praktikus módszerek széleskörű bevezetésén.

 **Tetszik** Regisztrájl, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Olvas-e az Apple IT security blogokat?](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6119940>

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 jelszó ötven árnyalata

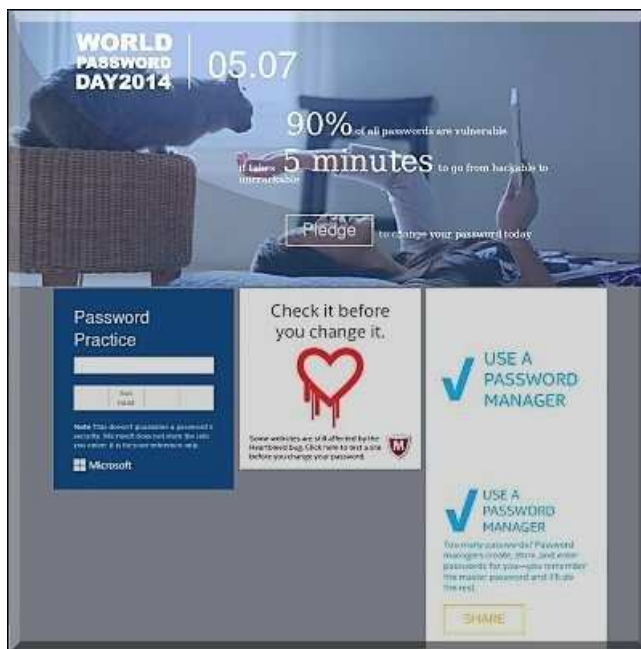
2014.05.08. 10:12 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [jelszó](#) [world password day](#) [óvatosság](#) [conficker](#) [biztonságtudatosság](#)

Újabb évforduló volt, anyák napja múltával éppen **tegnap ünnepelték a World Password Day napot**. Az esemény jó apropó lehet arra, hogy kicsit felelevenítsük halványuló emlékezetünket, vajon hány esztendeje is adtuk már meg régi jelszavunkként minden egyes elérési helyünkön az "1234"-et és ábrándos tekintettel kicsit eltűnődjünk, mikor fogunk legközelebb bizsergető késztetést érezni arra, hogy ezt haladéktalanul megváltoztassuk "password"-ra vagy "abcd"-re :-)



Félretéve az iróniát, amikor a nagyobb szolgáltatások elesnek, és a támadók ölébe hullanak a jelszavak, és ezeket még nyilvánosságra is hozzák, akkor **sajnos tisztán és világosan látszik, hogy mennyire szánalmasan fantáziátlan a jelszaválasztási gyakorlat sokaknál**. Nem véletlen a Worst Password évenkénti válogatása, híven tükrözi a valós helyzetet. Kicsit ezen is igyekszik segíteni az a [nemzetközi kezdeményezés, amely az erős jelszavak választásának népszerűsítését](#) tűzte ki célul. Az oldalon tippeket találunk az erős jelszó választásra, emlékeztetőt az OpenSSL hibája miatt kialakult HeartBleed incidensről, és hogy senki ne felejtse el azt sem, a PIN kódunk is egyfajta jelszó, ezért ott sem célszerű az 1234-hez hasonló primitív mintákat választani.



Hogy egy kicsit mi is söprögessünk a saját házunk táján, például a **már 7 éve toplistás Conficker féreg egyik terjedési módja is épít erre, hiszen [szótáralapú támadást is indít a gyenge adminisztrátori jelszavak ellen](#)**. Így a fertőzés következményeinek kivédésében itt is nagy szerep juthatna az erős jelszavak használatának. Persze időnként kettős a dolog, hiszen mi megadhatunk bármilyen erős jelszót vagy jelmondatot, **[ha a szolgáltató meg nagy ívben tesz a biztonságra - lásd LinkedIn-t](#)**, aki **korábban nem szóta jelszavait**. Ráadásul az incidenseket még utólag is **sokszor csak vonakodva, késlekedve és a tényeket megszépítve teszik közzé, ahogy azt elrettentő példaként az Adobe-nál is láthattuk**. Ott **[először 3 millió ellopott jelszó beismerését](#)** közölték, majd pár napra rá **[ebből lett végül 40 millió és Coldfusion meg egyéb termékek ellopott forráskódjai](#)**.

PASSWORD LIST USED (MODIFIED "ADOBE TOP 100")					
123456	123456789	password	forbes123	12345678	qwerty
1234567	111111	news	123123	1234567890	000000
abc123	1234	forbes1	f0rb3s	azerty	1loveyou
aaaaaa	654321	12345	666666	sunshine	123321
letmein	monkey	asdfgh	password1	shadow	princess
dragon	forbesforbes	daniel	computer	michael	121212
charlie	master	superman	qwertyuiop	112233	asdfasdf
jessica	1q2w3e4r	welcome	1qaz2wsx	987654321	fdsa
753951	chocolate	f--kyou	soccer	tigger	asdasd
thomas	asdfghjkl	internet	michelle	football	123qwe
zxcvbnm	forbes2	7777777	maggie	qazwsx	baseball
jennifer	jordan	abcd1234	trustno1	buster	555555
liverpool	abc	whatever	11111111	102030	123123123
andrea	pepper	nicole	killer	abcdef	hannah
test	alexander	andrew	222222	joshua	freedom
samsung	asdfghj	purple	ginger	123654	matrix
secret	summer	1q2w3e	snoopy1		

Egyszer már nekifutottunk a **"Hogyan válasszunk megfelelően erős jelszót"** témakörnek, így ezt a korábbi írást most csak belinkeljük, [elrettentő példának pedig Sarah Palint hagytuk a végére](#), akinek esete **nem** csak amiatt lehet elrettentő, hogy kormányzati munkatársként miért ne használjunk Gmailt a nekünk biztosított védett hivatali postafiók helyett, de amiatt is, hogy a jelszó- emlékeztető kérdésre adott választ se lehessen túl egyszerűen kitalálni például a Facebook profilunk átolvasásából.



A jelszó érték, vigyázzunk rá, és ez igaz akkor is, ha nem vagyunk közismert, vagy híres személyek. Csak érdekességgéppen érdemes lehet azt is megemlíteni, hogy a Barracuda Labs 2013-a beszámolója szerint az automata spam tweetek 98%-a érkezik valamilyen hamis accountról, és ezek jelentős részénél a feltörés nevű "varázslat" mindössze egy pár perces szótár alapú próbálgatás. Ahogy a <http://passwordday.org/en/> oldal is mutatja, a jelszavak 90%-a rövidegsége és gyengesége miatt 5 percen belül a támadók kezébe juthat.

A jelszó

olyan, mint a fogkefe

mindenkinek van, senkinek nem adjuk kölcsön és néha lecseréljük

Milyen egy "jó" jelszó?

- Megjegyezhető
- Hosszú, 10-15 betű!
- Ne legyen szótári szó!
- Ne adjuk oda másnak!
- Időnként cseréljük le!
- Nem családtag, kutya, születési dátum!
- Ne használjuk több helyen!
- A jelszó emlékeztető ne maga a jelszavunk legyen!

A jelszó menedzserek segíthetnek a megjegyzésben, pl. LastPass, KeePass



Végezetül a Safer Internet előadásunkból érdemes két diát ide beemelni. Az egyik a jelszó fontosságát igyekszik kihangsúlyozni: olyan mint a fogkefe, mindenkinek van, nem adjuk oda másnak, és időnként lecseréljük. A másik ábra pedig a password hosszúságok és jelenlegi ismereteink szerint hozzátartozó a visszafejtési idők arányát mutatja. [Dinya Péter szakdolgozatából](#) elég szemléletesen kitűnik, hogy legalább 11 karakter hosszt kell ahhoz választani, hogy ne valamilyen nevetségesen kis időintervallum kerüljön a brute force kockába. Reméljük, jövőre ugyanilyenkor már arról számolhatunk be, hány ezer iskola csatlakozott a programhoz, és adományoz a biztonság tudatos diákjainak "Az én jelszavam biztonságos" kitüntető oklevelet :-)

f Tetszik 11 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Agyilag zokni - mítosz megerősítve](#)

[Lopott Minecraft jelszavak szivárogtak ki](#)

[1 faktor + 1 faktor = 2 faktor](#)

[Csak technikai hiba volt a Twitteres jelszó reset](#)

[Forbes és Kickstarter incidens - jelszócsere kell](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6134904>

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](#).

[Kón Bandit 2014.05.09. 11:29:03](#)

1 a jelszó tartós béke

Válasz erre

Ingyenes Rolling Stones jegyek. Vagy mégsem?

2014.05.12. 11:36 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [ingyen facebook vagy átverés rolling stones megosztás mégsem sürgetés](#)

Vagy mégsem rovatunk egész egyszerűen kifogyhatatlan a municióból, hogy csak az idej eseteket említsük: [Telekom számla vagy mégsem?](#), aztán volt a [Megtalálták az eltűnt maláj repülő! Vagy mégsem?](#), és volt természetesen [Új Picasa képek az albumunkban. Vagy mégsem?](#) is a repertoárunkban. Ezúttal a már nem éppen fiatal Rolling Stones együttes 2014-es turnéja adott apropót egy Facebookos átveréshez.



Mostani történetünknel az 1960-as évek nagy rockzenei öregjei, illetve az idej esztendő szuperkoncert Rolling Stones 2014 sorozata adja. A turné jegyei "jó szokás" szerint azonnal, órák alatt elfogytak, aminek nyilván csak az egyik oka az, hogy sokan még ma is kíváncsiak a legendás bandára. A másik ok pedig az, hogy tulajdonképpen minden jelentősebb, hadra fogható eseményre mindig azonnal elkelnek a jegyek a nyereszkeskedő nepperek miatt, akik saját nevükben de strómanokkal is felvásároltatják azokat, hogy majd aztán az eBay-en vagy egyéb csatornákon busás haszonnal adják tovább a belépőket.



Lehetnek olyan helyzetek, amikor az utazási irodák last minute ajánlataihoz hasonlóan legitim módon juthatunk valamihez jóval olcsóbban. Ha például egy légitársaság megmaradt vagy váratlanul felszabadult repülőjegyeket hirdet mélyen leszállított áron az első jelentkezőknek, az tulajdonképpen nem veszélyes, hiszen maximum nem mi nyerjük az eredetileg 99 dolláros jegyet 9 dollárért, és ehhez nem kell előbb megosztanunk semmit. [A külföldön vásárolható utazási jegyek például sok esetben akkor a legolcsóbbak, ha már hónapokkal előbb lefoglaljuk és kifizetjük, míg az utolsó pillanatban megvásárolt jegy simán akár a többszöröse is lehet az eredeti kiinduló összegnek.](#) Ennek ellenére az olcsó ajánlatokat mindig érdemes megfontoltan kezelni, mert jelentős részük valóban nem mentes az átveréstől.



A rossz hír tehát az, hogy mégsem kapunk ingyen jegyet a Rolling Stones koncertre. Gyakorlott hoax és spam felismerőknek már egyből gyanús lehet a "Please share this site to proceed!" szövegrészt, amivel valaki éppen a clickjacking akciójához akar bennünket orvul felhasználni. Ki emlékszik arra, hogy a naiv felhasználók kattintásait mivel lehet még kiváltani? Igen, [az válaszolt jól, aki még emlékezett a fenyegetés és sürgetés módszerére.](#) Nos itt azzal lehet hatékonyan operálni, hogy az ingyen jegyek csak korlátozott számban és korlátozott ideig állnak rendelkezésre, aki lemarad, az kimarad. A jó hír viszont, hogy szinte azonnal látható,

ez egy nyilvánvaló átverés. Ez a fentiekben túl az angolul jól tudóknak is feltűnhet, hiszen [a csalók sokszor próbálkoznak idegen nyelvtérületekről, és erről a gyengébb, nyelvtani hibákat is tartalmazó szövegezés](#) is árulkodhat.



Úgy látszik, **sokszor és sokat kell még posztolni ahhoz, hogy a különféle üzenetek, kihagyhatatlan akciók "ingyen" szócskával kiváltott pavlovi reflex ne homályosítsa el az átlagfelhasználó gondolkodását.** Most pedig, hogy újra továbbberósítottuk a "ne higgyünk el rögtön mindent" és a "ne kattintsunk gondolkodás nélkül" hozzáállást, nézzük meg a [YouTube-on az együttes két és félórás 2013-as londoni koncertjét HD-ben](#) - ezt viszont valóban teljesen ingyen :-)

Tetszik 4 személy kedveli ezt [Regisztrálg](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Robin Williams utolsó telefonhívása. Vagy mégsem?](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Nyerjünk 250 ezer eurót. Vagy mégsem?](#)
[Figyeld a kígyót! Nem semmi. Hanem átverés :-\)](#)
[LinkedIn meghívó. Vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6155097>

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.

Hogyan védjük meg Twitter fiókunkat?

2014.05.14. 12:04 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [social media jelszó](#) [twitter védelem](#) [feltörés](#) [eset](#) [scanner](#) [fiók](#)

Még ha a saját fiókunk nem is volt feltörve - eddig - azért számos példát láthattunk már, ahol ismert emberek, hírességek, **politikai** vagy gazdasági vezetők, esetleg éppen újságszerkesztőségek, kiadók accountja felett vették át az uralmat ideiglenesen a támadók, sokszor komoly káoszt okozva ezzel. Saját bőrén [tapasztalhatta meg ezt már Russell Crowe](#) színész, Sepp Blatter [korruptiót látszólag](#) beismerő FIFA elnök, a [Financial Times](#), a Huffington Post, de [maga Obama elnök is](#).



Milyen lépéseket érdemes megtenni ahhoz, hogy elkerülhessük a feltörést? Jöjjenek akkor a tanácsok. Először is természetesen a jelszó kérdés jön. Ne legyünk olyan idióták, akik a Worst Password listából építkezve "123456", "password" vagy hasonló primitív jelszót használnak, esetleg saját születési dátumuk, kutyájuk vagy kedvenc focicsapatuk nevét választották, hiszen a bűnözők mindig egy gyakori kifejezéseket tartalmazó szótárral kezdik el a próbálgatást, és elég rossz érzés, ha a saját butaságunk miatt percek alatt áldozatul tudunk esni.

Erről egyébként már olyan sokat beszéltünk, hogy most csak annyit mondunk, fontos a megfelelően erős jelszó. Akik esetleg mégsem tudják, hogyan válasszanak ilyet, [azok számára itt olvasható a korábbi gyorstalpalónk](#).



Persze a megfelelő jelszóválasztásnál még az is lényeges, hogy ez valóban minden helyen **különbözzön**, vagyis ha valahol mégis **feltörnek minket**, ne lehessen végigaratni minden elérhetőségünket Gmail-től Facebook-ig bezárólag. Szóval a lényeg, [szükségünk lesz sok egymástól különböző jelszóra, hogy mindezt elkerülhessük](#). Ha már megvan a sok különböző jelszó, vagy jelmondat, mindezeket meg is kell tudni jegyezni.

Ne abban tegyük engedményt, hogy túl szimpla kifejezést választunk, hanem inkább nyilvántartásukhoz használjunk valamilyen **jelszómenedzser programot**. Számos ilyet lehet találni, a legismertebbek ezek közül például a LastPass, a 1Password és KeePass. Persze itt is kell egy mester jelszó, amit érdemes a fentieknek megfelelően nem 123-nak kiválasztani.



Ahol lehet, **mindenhol használjuk a kétfaktoros autentikációt**. A Gmail például már régóta tud ilyet, egy idő óta a Twitter is beállt a sorba, így a logint a telefonunkra egy külön SMS-ben küldött kód is védelmezi az illetéktelen belépéstől. **Emellett időnként nézzük vissza**

a Twitter belépéseink naplóit és vegyük észre, ha azon gyanús tételek is vannak. Nincs rosszabb forgatókönyv annál, mintha valakinek feltörjük az accountját, de azt hosszú ideig vagy egyáltalán nem is veszi észre.

Plusz tippként javasoljuk még az [ESET Social Media Scanner eszközt is, amelynek új változata a Facebook használat mellett már a Twitter védelmét is ellátja](#). Az alkalmazás ellenőrzi a Facebook idővonalon megjelenő tartalmakat: posztokat, híreket, valamint a Twitteren a követők által közzétett üzeneteket is, hogy azok ne tartalmazzanak kártevőt, vagy azokra mutató hivatkozásokat. Vagyis ebből következően a gépünknek is tökéletesen vírusmentesen kell lennie ahhoz, nehogy egy háttérben futó kémprogram ellophassa a személyes adatainkat, és vele a belépési jelszavainkat.



Persze emellett arra sem árt figyelni, hogy tényleg a valódi oldalon jelentkezünk be, [ne pedig egy hasonló adathalász linken](#) gépeljük be az azonosítónkat. Egy tavalyi felmérés szerint a közösségi oldalakon keresztüli spamelés minden korábbi mértéket meghaladóan emelkedett, és az automata tweetek 98%-ban hamis vagy feltört accountokról érkeznek. Ezért érdemes vigyázni nem csak a saját magunk biztonsága, és persze a követőink iránti tisztelet miatt, hanem mert ezenfelül nyilván [senki nem akarja, hogy fiókján szabadon ki-bejárjanak a személylelőterjesztők](#), vagy a kártevőterjesztők.

[Tetszik](#) Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [+1](#)

Ajánlott bejegyzések:

[Így vernek át a Facebookon és így védekezz!](#)
[Életünk része lett az állandó támadás](#)
[A Justin Bieber átverés](#)
[Itt a lopásvédelemmel ellátott Smart Security 6](#)
[Itt a kamu Look Back videó](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6162563>

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.

Lebecsüljük a BYOD kockázatokat

2014.05.16. 09:42 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [biztonság](#) [felmérés](#) [szabályozás](#) [kockázat](#) [gartner](#) [byod](#) [welivesecurity.com](#)

Erről árulkodik az a Gartner által végzett kutatás, amelyben arra voltak kíváncsiak, hogy mennyire biztonság tudatosan állnak hozzá a dolgozók ahhoz, ha a saját mobileszközeikkel is dolgoznak a munkahelyen.



Korábban mi is idéztünk egy felmérést, ahol [már 2012-ben is az látszott](#), hogy a BYOD nem kopogtat az ajtónkon, hanem már széles körben elterjedt, erre utalt például a 81%-os akkori adat. Az ezzel kapcsolatos részletek is érdekesek voltak, hiszen azon túlmenően, hogy a cégek beengednek egy esetlegesen sebezhető állapotú eszközt a hálózatukba, és a [mobileszköz elvesztése esetén](#) céges levelezés, illetve bizalmas dokumentumok is áldozatul eshetnek, azt is láthattuk, hogy például 66%-ban nem létezett vállalati policy a használat szabályozására, ellenőrzésére.



A mostani, 2014-es tanulmányban pedig arról olvashatunk, hogy a saját okostelefont a munkájukban is felhasználók jelentős része nem aggódik a biztonsági kockázatok miatt, és csak mindössze 27% nyilatkozott úgy, hogy ezzel kapcsolatosan problémákba ütközött. [A hozzátetőleg ezer amerikai munkavállaló körében végzett felmérés úgy találta](#), hogy a dolgozók az okostelefonjaikat, vagy a kicsit méretesebb phabletjeiket naponta átlagosabb legalább egy órán keresztül használják céges munkavégzéssel kapcsolatos tevékenységekhez. A munkavállalók harmada tisztában van ugyan a BYOD jelenség okozta kockázatokkal, ám saját cégükönél éppen nem létezik ezzel kapcsolatos útmutatás.

Összességében még mindig 59% azoknak az aránya, akik úgy használják munkahelyükön a mobil eszközeiket, hogy eközben céges oldalról erről semmilyen megállapodást vagy szabályozást nem írt alá. Elemzők szerint e tekintetben csak az vezethetne érdemi javuláshoz, ha a cégek külön, teljes munkaidőben foglalkoztatott BYOD felelőst foglalkoztatnának, akinek ebben az egyre változó környezetben jelentkező működtetési és biztonsági feladatok elvégzése lenne a fő teendője.



A veszély bagatellizálása egyébként nem új jelenség, ehhez elég egy tavalyi évvégi felmérést idézni, ott az derült ki, [a vállalatok 40% nem is tekintette a BYOD-ot biztonsági fenyegetésnek](#). Nyilvánvalóan a szellemet nem lehet visszazárni a palackba, vagyis nem a totális tiltás a megfelelő módszer, ám az, hogy sok helyen még mindig hiányzik a BYOD-dal kapcsolatos szabályozás, előírás, és ellenőrzés, az azt mutatja, hogy **számos vállalat nincs tisztában azzal, hogy a mobil eszközökkel kapcsolatos számítógépes támadások, fenyegetések milyen károkat eredményezhetnek.**



Az adatvesztést, a mobil eszközök biztonsági réseinek kihasználását csak megfelelő eszközökkel és betartatott szabályozással lehet elkerülni. És erre még az sem lehet mentség, ha valaki azt mondja, mi csak egy kis cég vagyunk, miért támadna minket bárki, hiszen **jól láthatóan a nagyobb vállalatok elleni támadásokat egyre gyakrabban a gyengébben védett kisebb beszállítókon és partnercégeken keresztül vírusokkal, kémprogramokkal indítják a kiberbűnözők.**

 Tetszik Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Amikor a suszter cipője lyukas](#)
[Napi 160 ezer Facebook account esik el](#)
[Kormányzati e-mailek kontra biztonság](#)
[Biztonsági konferencia - nyitott wifi honeypot-tal](#)
[Így költjük a pénzt az online vásárlásoknál](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6172559>

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.

Célkeresztben a telefontolvajok

2014.05.19. 12:27 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [biztonság](#) [mobile security](#) [védelem](#) [android](#) [eset](#) [lopásgátló](#)

Továbbfejlesztett funkciókkal érkezett meg az ESET Mobile Security legújabb Androidos változata. A fejlett lopásvédelmet kínáló megoldás hatékonyan segíti a készülék tulajdonosait abban, hogy minél könnyebben nyomon tudják követni ellopott vagy elhagyott mobil eszközeiket. Ez magyarul azt jelenti, hogy a mobiltelefon automatikusan lefotózza a tolvajt.

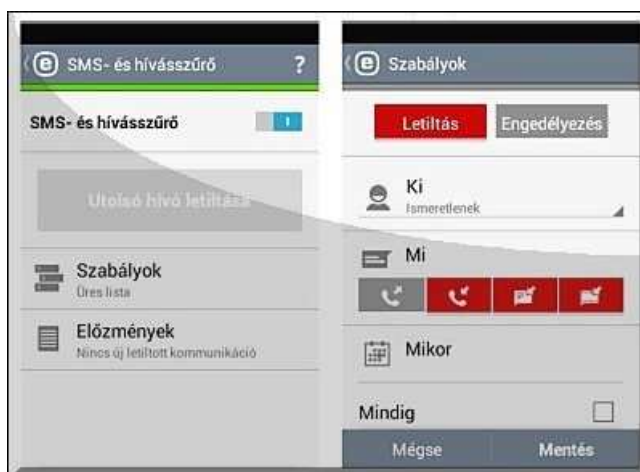


A proaktív lopásvédelem érzékeli a potenciálisan veszélyesnek ítélt helyzeteket és azonnali segítséget nyújt az ellopott vagy elhagyott eszköz helyének meghatározásában. A prémium előfizetőknek járó funkciók segítségével például elküldi az akkumulátorának lemerülése előtt a készülék utolsó bemért helyzetét, fényképeket készít az előlő és a hátlapi kamerával, amikor rossz PIN kóddal próbálnak belépni az eszközbe, vagy amikor változást érzékel a SIM-kártyával kapcsolatban, valamint a készülékkel kapcsolatos összes információ elérhető a my.eset.com honlapon.



A mai felhasználók mindent mobil eszközeiken tárolnak, a személyes és munkahelyi adataik mellett még pénzügyi tranzakcióikat is ezeken a készülékeken keresztül intézik. Amellett, hogy egy ilyen készülék elvesztése eléggé bosszantó dolog, óriási a rizikója az adatlopásnak is. Az ESET korábban számos visszajelzést kapott azzal kapcsolatban, hogy az eszköz lokalizációja és nyomon követése minél egyszerűbb, könnyebb és egyértelműbb legyen. Többek közt ezek valósultak meg most a Mobile Security legújabb verziójában, emellett pedig egy sor további biztonsági elemet is tartalmaz, növelve ezáltal az Androidos felhasználók védttségét.

Az alkalmazás ingyenes verziója olyan alapvető funkciókat tartalmaz, mint a készülék és a letöltött alkalmazások ellenőrzése, vagy az alap lopásvédelmi funkciók. A prémium alkalmazás megvásárlásával, vagy annak 30 napos próbaverziójában viszont további kiegészítő funkciók érhetőek el. Itt már ütemezhető ellenőrzési lehetőséggel, fejlett lopásvédelemmel, my.eset.com integrálással, hívás-szűréssel illetve biztonsági auditálással is találkozhatunk.



Végezetül jöjjenek az új lopásvédelmi funkciói és a my.eset.com weboldal felületével:

- A védett Androidos készülékek és Windows-os laptopok integrálása a my.eset.com weboldal felületével
- SIM-kártya azonosítása – egy ismeretlen SIM kártya behelyezése esetén is irányítható távolról a készülék
- Helyzetkövetés – a lopásvédelem online kezelése. Miután megjelöltük az eltűnt készüléket a my.eset.com oldalon, a készülék valós idejű helyzete megjelenik egy térképen
- Gyanús állapot meghatározása – rossz PIN kód vagy egy ismeretlen SIM-kártya használatkor megelőző tevékenységek
- Pillanatképek készítése – elveszett készülék esetén az eszköz képeket készít az előlő és a hátlapi kamerával és azokat elküldi a my.eset.com oldalra
- Üzenetküldés – személyre szabható üzenet küldése a lehetséges megtalálónak
- Alacsony akkumulátorszint – amint a készülék akkumulátorszintje a kritikus szintre süllyed, automatikusan jeleket küld az eszköz aktuális helyzetéről
- IP címek követése – azon IP címek listázása, amelyekre a készülék csatlakozott



Természetesen nem csak lopás, hanem **a különféle trójaiak, kártevők**, és egyéb támadások - **például az emlékezetes USSD** - szűrése miatt is érdemes használni a **védelmi programot**. Az ingyenes verzió az alábbi linkről tölthető le:

<http://www.eset.hu/letoltes/otthoni/mobil>

Tetszik Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

[Androidos engedélyek a szőnyeg szélén](#)
[Mit tegyek, ha ellopják az androidos telefonomat?](#)
[Megjelent a Google Play-en az ESET for Android](#)
[ESET védelem Androidra](#)
[Béták reggelire II.](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6180486>

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](#).

[antyg 2014.05.20. 07:49:39](#)

Jó dolgok vannak az alkalmazásban, kétségtelen, de...

A probléma ott kezdődik, hogy a mostani tolvajok is olvasgatnak a mobil (és egyéb) védelmekkel kapcsolatos cikkeket, de ha mégsem, akkor csak hallás útján, tudhatják, hogy nem nyomkodjuk a telefont, ha bármit is meg akarnak róla szerezni. Az egyszerű tolvajt úgy sem az ellopott készüléken lévő adatok, hanem a készülék eladásból származó „bevétele” jelenti.

Ebben az esetben (is) véleményem szerint minden rosszindulatú tolvaj első lépése az lesz, hogy csinál egy factory reset-et a készüléken (előtte még lehet, hogy a kártyát is kieszedi, ha esetleg még adatokra is kíváncsi...) (ez nem nehéz, sajnos, vagy nem sajnos millió egy leírás van róla a világhálón, hogy hogy kell...), ilyenkor tudjuk, hogy minden törlődik a készülékről. Gondolom, azt sem kell ecsetelni, hogy

ezzel az egyszerű törlési megoldással még az adatok helyreállíthatók, egy erre a célra szánt szoftverrel. Tehát még akkor sem lehetünk nyugodtak, ha tudjuk az adatok törlésre fognak kerülni. Erre azért van megoldás, a készülék teljes titkosítása, mely esetben az adatok titkosítva kerülnek tárolásra a készüléken, legyen az a belső memória, vagy az SD kártya. Tehát ilyenkor az adataink biztonságba lesznek (törlést követően is), de a készülék ettől függetlenül már végleg elvész, hiszen, teljes törlést követően azt már biztos, hogy nem lehet visszaszerezni. Egy megoldás lenne erre jó, ha a készüléket pl. PIN kód megadását követően lehetne kikapcsolni, de ez is csak abban az esetben lenne hasznos, ha a készülékben fix beépített akkumulátor van, a kiszedhető esetén, egyszerűen csak megszakítják a tápellátást. Szóval, kérdőjelekkel állok az ilyen típusú alkalmazásoknak, mert van (ha nem is sok, de elég erősen támadható) gyenge pont, melyet szoftveresen, de még hardveresen sem lehet kiküszöbölni.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.05.21. 15:43:49**

Szia Antyg!

Igazat adok abban, hogy ilyen eset valóban előfordulhat, de ettől még szerintem azért érdemes minden tőlünk telhetőt megtenni, hátha csak valami szellemileg szerényebben bútorozott illető vitte el.

Ahogy az autónkat is elvihetik és egy óra alatt feldarabolhatják, majd vihetik Olaszországba, de azért mégis csak bejelentjük a rendőrségen, kiteszük a képét a Facebookra, bejárjuk a környező utcákat, hátha csak pihentetik a környéken stb.

De ettől még persze igaz, 100%-os védelem sehol nem létezik.

Válasz erre

antyg 2014.05.22. 10:32:16

[@Csizmazia István \[Rambo\]](#): Szia Rambo!

Bocs, ha félreérthető voltam a kommentben! Nem azt mondtam, hogy nem szabad használni (épp ellenkezőleg), mindent meg kell tenni az adataink és készülékeink védelmében. Azonban az a gond, hogy pl. a "szellemileg szerényebben bútorozott" személy is sok esetben megoldást találhat, mert egy zug mobil árus képes arra, hogy akkor töröljünk mindent (azzal megy be ebben az esetben a gyengébb IT képességű ember, hogy „elfelejtettem a jelszavamat, meg lehet oldani valahogy, az sem gond, hogy ha minden törlődik...” (?)

Természetesen 100%-os biztonság nincs, törekedni kell arra, nekem is úgy van a telefon védelme kialakítva, hogy ami jelenleg elérhető, azt alkalmazom, de ettől függetlenül van otthon, felhőben stb. megfelelő biztonsági mentés, hogy egy incidens esetén, gyorsan és egyszerűen belakthassam az új készüléket, ha arra van szükség... :)

Válasz erre

Hetedik hónapja vezet a mentéseket törölő kártevő

2014.05.21. 15:36 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [radar](#) [április adatok 2014](#) [nod32](#) [havi report](#) [threat](#) [vírusstatisztika](#) [statatisztika](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. áprilisában a következő 10 károkozó terjedt a legnagyobb számban.



A mezőny első része jobbra változatlan, így továbbra is **a mentéseket törölő Win32/Bundpil féreg vezet, amely immár 2013. októbere óta folyamatosan listavezető**. Ennek kapcsán és más hasonló, törléssel vagy elkódolással operáló kártevő kapcsán **nem lehet elégszer felhívni a figyelmet a saját munkák rendszeres mentésének fontosságára**. Ebben a műveletben az is fontos, hogy ne egyetlen mentést írjunk felül, hanem rendelkezünk párhuzamosan több különböző dátumú mentéssel, ezek mindig külső adathordozóra készüljenek, és legyenek is időnként letesztelve, ellenőrizve, kipróbálva.



A Conficker féreg és az Autorun vírus úgy tűnik, bebetonozta magát, hiszen 2008 óta rendszeres tagjai már a toplistának. Érdekes emellett a második helyezett LNK/Agent trójai, amely különféle utasítássorozatokot fűz össze kártékony szkriptekké. Emellett visszatért a februárban megismert Win32/TrojanDownloader.Waski a kilencedik helyre. Ez egy olyan trójai letöltő program, amely **egy fix listát tartalmaz URL linkekkel, és ezek alapján próbálkozik további malware kódokat letöltésével az internetről a HTTP protokoll segítségével.**

Ezzel kapcsolatban fontos kiemelni, hogy az ehavi toplistás kártevők fele trójai, vagyis ezek esetében látszólag valós, legitim programok azok, amikre a megtévesztett felhasználók maguk kattintanak, tehát érdemes vigyázni. Végül a negyedik helyezett HTML/ScriptInject trójait is érdemes megemlíteni, amely valójában egy olyan RAR segédprogrammal tömörített állomány, amely telepítése során egy üres (c:\windows\blank.html) állományt jelenít meg a fertőzött gép böngészőjében. Működése közben azonban **hátsó ajtót nyit a megátadott rendszeren, és ezen keresztül a háttérben további kártékony JavaScript állományokat kísérel meg letölteni a számítógépünkre.**



Az ESET Radar Report e havi kiadásában a fő hangsúlyt a 2001. októberében megjelent Microsoft Windows XP operációs rendszer támogatási időszakának lejárta kapta. Érdemes lehet felülvizsgálni beállításainkat, eddigi frissítéseink állapotát, ugyanis bár sok mindent tehetünk, a rendszeres hibajavítások megszűntével a biztonság már csak viszonylagos. **Sajnos az is tény, hogy Magyarországon nem csak a magánszemélyek esetében, és a kisvállalkozásoknál, de a közigazgatásban, kórházakban is még mindig kiemelkedően magas a sebezhetővé vált XP rendszerek aránya.**

Emiatt ha nem is azonnal, de előbb-utóbb mindenkinek váltania kell egy másik, biztonságosabb, illetve rendszeresen javított operációs rendszerre. Ez már csak amiatt is fontos, mert a biztonsági cégek információi szerint a kártevőkészítők a már felfedezett, de eddig még nem publikált zero day sebezhetőségeket "bepájzolták", hogy aztán mostantól a biztonsági frissítések befejezése után hatékonyan tudjanak vele támadni, illetve fertőzni.



Áprilisi fontosabb blogposztjaink között írtunk [egy részletes összefoglalót](#), mire érdemes figyelni akkor, ha hatékonyan szeretnénk megővni magánszféránkat az interneten. Biztonsági tippjeinkben a megbízható programok telepítése, a naprakész vírusirtó, az erős jelszavak használatán felül a titkosítás, a nyitott wifi használat veszélyei és a saját munkáink rendszeres mentése is szerepelt.



Ahogy az ESET riportban is olvashattuk, **április 8-a volt az a dátum, amikor a Microsoft meghúzta a végső határidőt az immár 13 esztendő Windows XP technikai támogatásának végére.** Igaz, meglepetésre aztán mégis kiadott egy az Internet Explorer 6, 7 és 8-as verzió sebezhetőségét javító "utolsó utáni" XP javító foltot, ám mindenkinek érdemes vagy a mielőbbi váltáson gondolkodni, vagy a meglévő rendszerének alaposabb védelméről gondoskodni. [Ehhez mi is adtunk egy alapos, és minden technikai részletre kiterjedő útmutatót.](#)



A social engineering, azaz megtévesztés sok kárt tud okozni. Tantörténetünkben egy olyan incidensről számoltunk be, ahol egy túlzottan naiv és hiszékeny nő az online társkeresésnél "megismert", ám a valóságban még sosem látott újdonsült partnerének anyagi segítséget nyújtott, aki aztán nyomtalanul eltűnt a pénzzel. [A társkereső oldalakon a csalók ma már iparszerűen és célzottan keresik a 40 feletti, jól szituált hölgyeket](#), ezért érdemes gyanakodni, és az ilyen kétes pénz kérésekre határozott nem-et kell tudni mondani.



Rájárt a rúd áprilisban az Android rendszerre, emiatt aztán kétszer is foglalkoztunk vele. Az egyik esetben egy Facebook-on terjedő átverés okozhat bajt, ha valaki elhiszi rákattint. [A Windows-os böngészőt megfertőző kártevő ugyanis banki adatokra vadászik](#). Az esettel kapcsolatban érdemes felhívni a figyelmet, hogy kéréten levélben, vagy üzenetben sosem küldenek a bankok olyan programot, vagy linket, amely pénzügyeink intézésére való, hanem minden programot csakis a megbízható Google Play áruházból töltsünk le.

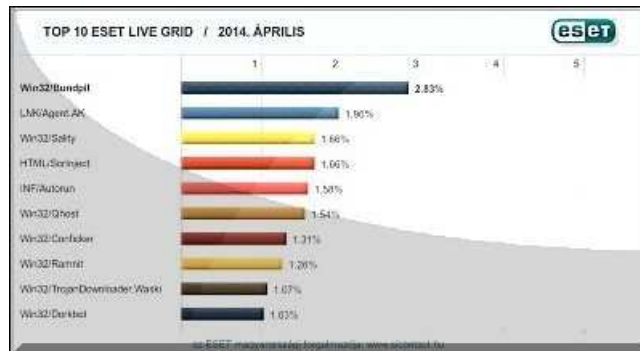


Végül a másik Androidos esetről arról írtunk, hogy [az ESET kutató egy olyan új, egyelőre orosz nyelven észlelt kártevőre figyeltek fel, amelyik egyszerre íratja fel az áldozatot emelt díjas SMS-re és lopta el közben a személyes adatait is](#). Az ilyen eseteket akkor van nagy esélyünk elkerülni, ha nem csak, hogy használunk olyan biztonsági programokat, mint például az ESET Mobile Security for Android, hanem minden program telepítésénél alaposan ellenőrizzük az igényelt engedélyeket is, illetve sose kattintsunk kéréten levelek, üzenetek mellékleteire, linkjeire.



Vírstoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint 2014. áprilisában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 15.90%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtevesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.



01. Win32/Bundpil féreg

Elterjedtsége az áprilisi fertőzések között: 2.83%

Működés: A Win32/Bundpil 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.

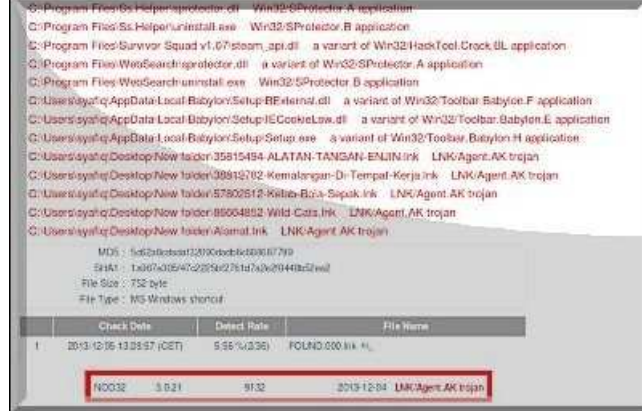


Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

02. LNK/Agent trójai

Elterjedtsége az áprilisi fertőzések között: 1.96%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatot 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. Vírusselemezők 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



03. Win32/Sality vírus

Elterjedtsége az áprilisi fertőzések között: 1.66%

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.



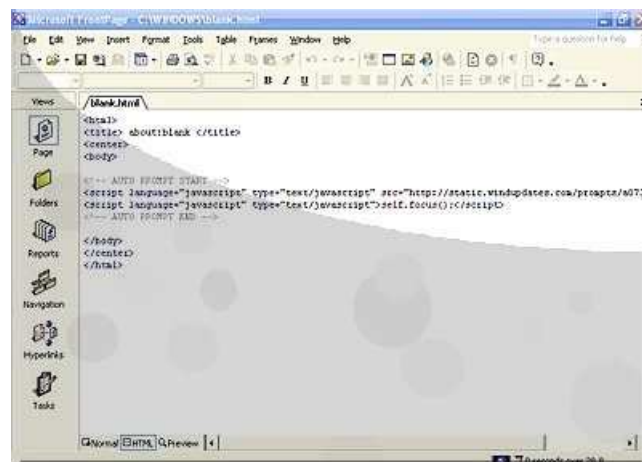
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



04. HTML/ScrInject trójai

Elterjedtsége az áprilisi fertőzések között: 1.66%

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.



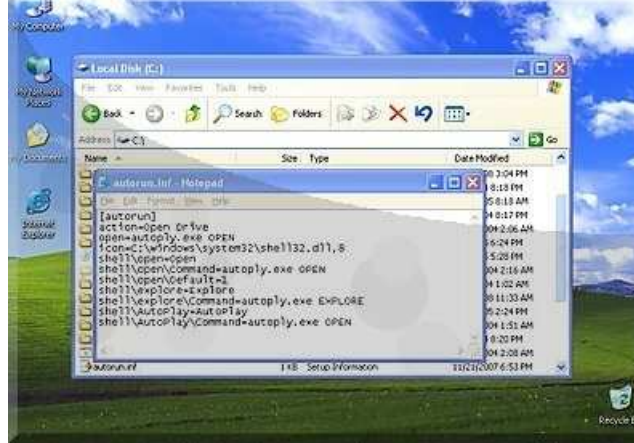
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen>



05. INF/Autorun vírus

Elterjedtsége az áprilisi fertőzések között: 1.58%

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



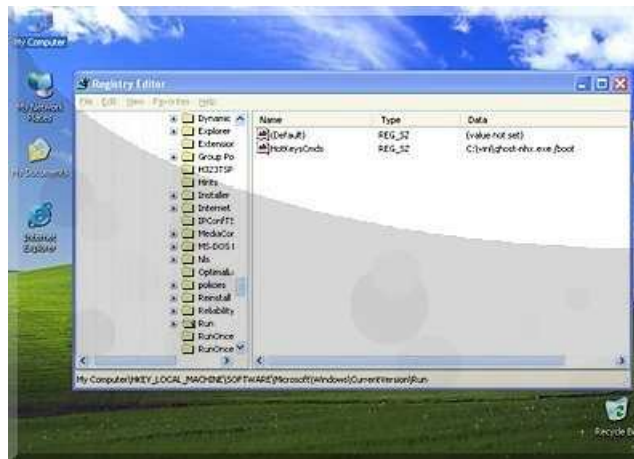
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>



06. Win32/Qhost trójai

Elterjedtsége az áprilisi fertőzések között: 1.54%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárba, 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.



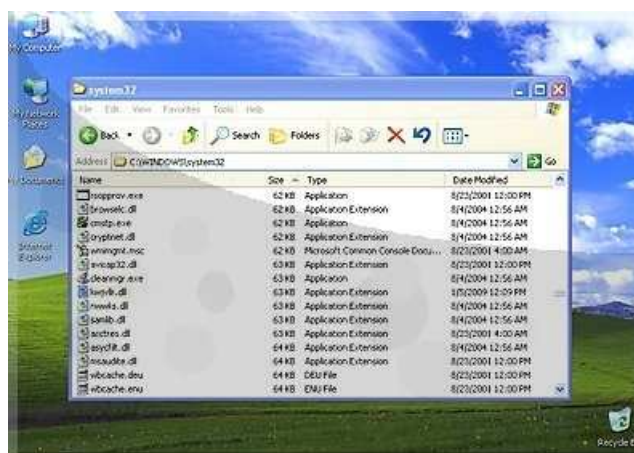
Bővebb információ: http://www.virusradar.com/en/Win32_Qhost.PEV/description



07. Win32/Conficker féreg

Elterjedtsége az áprilisi fertőzések között: 1.31%

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 eljárásn keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a hosts 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.



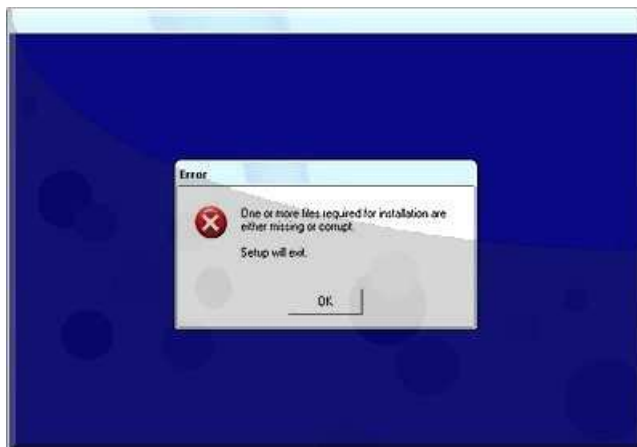
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker>



08. Win32/Ramnit vírus

Elterjedtsége az áprilisi fertőzések között: 1.26%

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. Végrehajtáskor 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/TrojanDownloader.Waski trójai

Elterjedtsége az áprilisi fertőzések között: 1.07%

Működés: A Win32/TrojanDownloader.Waski egy trójai letöltő. Egy fix listát tartalmaz URL linkekkel, ezek alapján próbálkozik. Futtatása után bemásolja magát a helyi számítógép %temp% mappájába miy.exe néven, majd további malware kódokat próbál meg letölteni az internetről a HTTP protokoll segítségével.



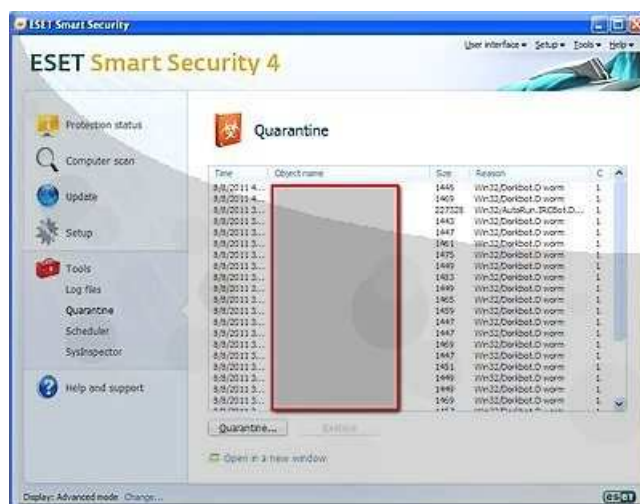
Bővebb információ: http://www.virusradar.com/en/Win32_TrojanDownloader.Waski.A/description



10. Win32/Dorkbot féreg

Elterjedtsége az áprilisi fertőzések között: 1.03%

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



Ajánlott bejegyzések:

[Nem változtak a toplistás vírusok](#)
[Megtévesztések és álhírek terepe a Facebook](#)
[Vírustoplista 2015. január hónap](#)
[A bank sosem hív bennünket, hogy mi a PIN kód](#)
[A HTML trójaiak riogattak minket októberben](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6189783>

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.

Mit tegyek, ha ellopják az androidos telefonomat?

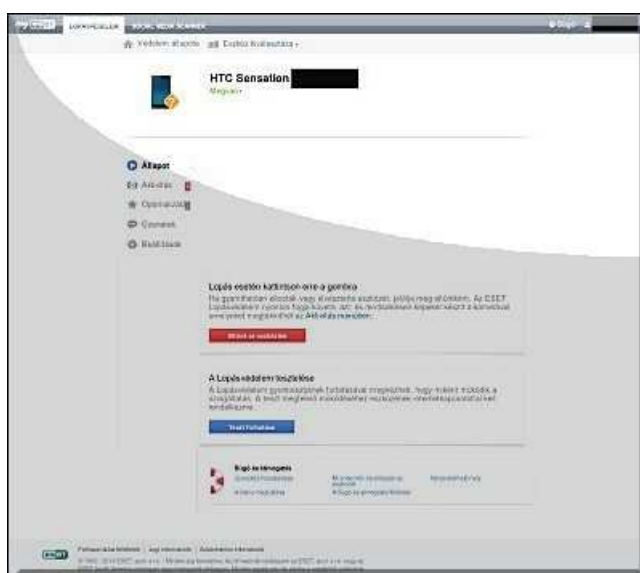
2014.05.26. 13:35 | [Csizmazia Darab István \[Rambo\]](#) | [9 komment](#)

Címkék: [ingyenes elveszett prémium mobile security tolvaj okostelefon android eset tablet infografika lopásvédelem](#)

Újabb szép nap, újabb hét indul és újabb infografikát mutatunk be a blogunkon. **Ezúttal a lopásvédelem került terítékre** annak kapcsán, hogy [nemrég új funkciókkal felvértezve érkezett meg az ESET Mobile Security legújabb Androidos változata](#). Milyen lehetőségeket kínál a fejlett lopásvédelem? Ez derül ki az alábbi részletes ábrából.



Minden szónál többet ér egy kép rovatunkban most egy olyan infografikát mutatunk be, amely részletesen és közérthetően foglalja össze azokat a lépéseket, amivel az elvesztett vagy elloptott androidos telefonunkat, tabletünket kereshetjük meg, vagy legvégső esetben törölhetjük róla távolról a személyes adatainkat.



A kettő között azonban még számtalan opció áll a rendelkezésünkre: üzenhetünk a beépített kamera által amúgy is lefényképezett tolvajnak vagy ha hamar észbekapunk, bekapcsolhatunk a készüléken egy vijjgató szírént. Az [ingyenes és a prémium változat által nyújtott lehetőségek lehetőségek](#) hasonlóak, de azt is bemutatjuk, pontosan mik a különbségek.



Tetszik 10 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[ESET védelem Androidra](#)
[Célkeresztben a telefontolvajok](#)
[Androidos engedélyek a szőnyeg szélén](#)
[Megjelent a Google Play-en az ESET for Android](#)
[Béták reggelire II.](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6210767>

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](#).

[A munka hőse, minden kommunista őse \(törölt\) 2014.05.27. 19:52:53](#)

android eszközkezelő szerintem bőven elég. amúgy meg igazatok van: fizessen csak, aki a telefonjára nem tud vigyázni...
Válasz erre

[antyg 2014.05.28. 08:02:32](#)

[@A munka hőse, minden kommunista őse](#): Saját magadnak mondasz ellent! Az elsőnél még azt mondom, hogy nincs ilyen alkalmazásra szükség, hanem bőven elég az eszközkezelő... na most, ha csak az eszközkezelőt használod adataid, és esetleg készüléked védelem érdekében, akkor egészségedre és (ha úgy adódik) akkor csak fizess akkor, ha készülékedre nem tudsz vigyázni.
Válasz erre

[klarky • http://kreport.blog.hu/ 2014.05.28. 11:46:07](#)

Nekem avast! volt fent, színes, szagos, mindent beígérő csoda. Pár hete újra raktam a rendszert a telefonon és elfelejtettem, h elvileg ez az izé védi a kütyüt. Kérdés és zokszó nélkül hagyta, h letöröljem róla az egészet. Ennyit ért az egész, kb. semmit. Ezt egy tolvaj is megteheti bármikor.

Android eszközkezelő és kész. Attól több nem kell.
Válasz erre

[antyg 2014.05.29. 08:45:31](#)

[@klarky](#): Egy alkalmazást nem csak telepíteni kell és azt hinni, hogy ezzel meg is vagyunk és a védelem közel a 100% felé! Mindennek meg kellene nézni, hogy mit, és hogyan tudja. Az Avast-ot sem lehet csak úgy eltávolítani, ha minden megfelelően be van állítva. Az Avast-nak is van egy Anti-Theft kiegészítése, amit az alap Avast telepítését követően kell aktiválni (előtte letölteni), és az eszközkészletben jogot kell neki adni. Amikor az Anti-Theft-et bekapcsolod előtt meg kell ugyebár adni adatokat (pl. név, telefonszám) és ami fontos, egy KÓD, 4-6 karakterből állót, mely esetben ha azt el akarod távolítani, akkor ugye az eszközkészletben ki kell kapcsolni, különben annak eltávolítása nem lesz lehetséges. Amit eltávolítottál az csak a vírusirtó része, az Anti-theft megmarad, és a jogot az eszközkészletben csak a kód megadásával tudod megvonni tőle, anélkül nem lehet eltávolítani! (Ez tutti, most próbáltam ki...)
Válasz erre

[antyg 2014.05.29. 08:47:52](#)

[@antyg](#): De amúgy minden (magára valamit adó) biztonsági szoftver esetén be lehet állítani, hogy az eltávolításához is kérjen kódot, vagy jelszót.
Válasz erre

[antyg 2014.05.29. 08:53:20](#)

[@antyg](#): De amúgy minden (magára valamit adó) biztonsági szoftver esetén be lehet állítani, hogy az eltávolításához is kérjen kódot, vagy jelszót.
Válasz erre

[klarky • http://kreport.blog.hu/ 2014.05.29. 08:56:16](#)

[@antyg](#): Meg fogom nézni amit mondasz, de hidd el, h minden be volt állítva, kód, eszközkészlet jogosultság, minden.

Egyébként teljesen mindegy, h ott van-e most vagy sem, hisz a készülék simán működik az újratelepítés után is, sehol nem kér kódot vagy egyéb olyan dolgot, amit egy tolvaj ne tudna átugrani, hisz még egyszer mondom semmi jele annak, h aktívan történne valami a háttérben.

Korábban pld. egy app uninstallálása csak kód megadása után ment. A gmail fiókomba csak kóddal engedett be. Stb.-stb. Most? Semmi, azt csinálsz vele amit akarsz. És ez szomorú a termékre nézve...

Én úgy képzeltem ezt az egészet, h rádugom a telefont a gépre, elindítom a rendszer frissítését és/vagy újra telepítését és már visít is, h nekem ehhez nincs jogom, adjam meg az azonosító kódomat. De semmi sem történt.
Válasz erre

[antyg 2014.05.30. 13:45:37](#)

[@klarky](#): Huhh az elég érdekes, hogy bármit elérsz, minden féle jogosultság nélkül a telefonon... a gyári rendszert pakoltad vissza, vagy valami "főzött" dolgot? mert ha nem gyári (eredeti a gyártótól, vagy frissítés stb.) rendszer, akkor lehet, hogy abban a fejlesztő, ezeket kiszedte...
Válasz erre

[klarky • http://kreport.blog.hu/ 2014.05.30. 14:14:25](#)

[@antyg](#): Teljesen gyárit tettem vissza. Rádugtam a készüléket a laptopra, elindult a gyári program, feltelepült a rendszer és kész is. Az avast! meg sem nyekkent és azóta sem adott hírt magáról...
Válasz erre

VirusTotal feltöltő immár Macintoshon is

2014.05.28. 09:56 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [api](#) [macintosh](#) [osx](#) [virustotal](#) [uploader](#) [feltöltő](#)

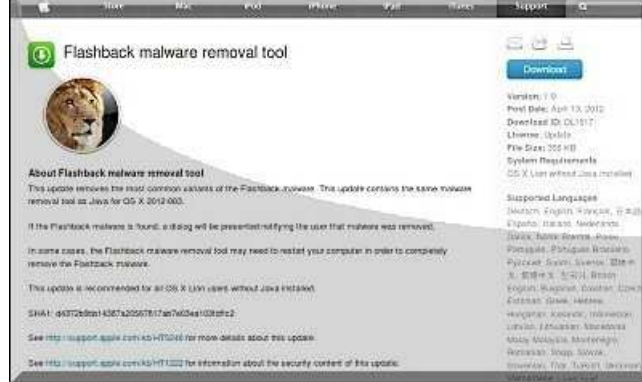
Megszokhattuk már, hogy Windows alatt mennyire kényelmessé igyekeznek tenni a felhasználók életét, és egy-egy gyanús fájl feltöltéséhez ott már régóta nem kell böngészőre váltva weboldalra ugrani, majd a mintát kiválasztva feltölteni, hanem ehhez elég egy beépülő modul, meg egy jobb egérgomb is.



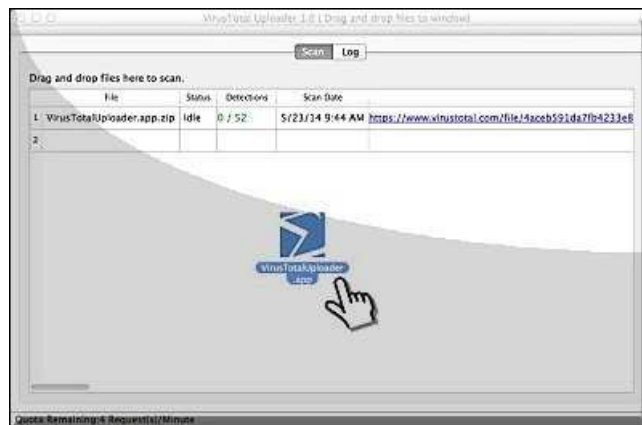
A VirusTotalnál úgy érezték, most jött el az idő arra, hogy extra figyelmet fordítsanak az OS X rendszerre és mindez itt is megvalósulhasson. Aki időnként böngészgetni szokta a VirusTotal blogját, az jobbra csak olyan bejegyzésekbe futhat bele, mint [újabb n+1-edik kereső motor került bele](#) a rendszerbe, vagy hogy valamilyen rész terület - [például URL hivatkozások](#) vagy PDF állományok - vizsgálata egészült ki új elemzési móddal. Ezúttal azonban a Google-nál úgy gondolták, hasznos újítás, hogy a publikus API használatát egyszerűbbé váljon az élet végre Macen is, és a jobb klikk + helyi menüből fájl kiválaszt kombó itt is tehesse végre a dolgát.



Nyilván ehhez az is hozzájárult, hogy a Windows-hoz képest [nagyságrendekkel kisebb mértékben, de egyre gyakrabban](#) fordulnak elő kártékony kódok, legyen szó [Angry Birds alkalmazásnak álcázott Mac malware](#)-ről, vagy akár a GateKeepert kijátszó [valódi, érvényes Apple Developer ID-vel aláírt kémkedő trójairól](#). Az idők folyamán ugyanis lassan mindenkinek be kellett látnia, hogy a Macintosh sem sebezhetetlen, ezt talán [a 600,000 tagot számláló Flashback botnet](#) tette igen világossá.



Az ötven feletti - egész pontosan 52 - különböző antivírral megvizsgált gyanús állományok riportjai nagyban segíthetnek a maces tábornak abban, hogy egy-egy dokumentum, kéretlen levélben érkezett fájl melléklet esetében eldöntsék, megbízható-e vagy sem. Az Asztalról akár Drag and Drop-pal is működő feltöltés mindenesetre mostantól **hatékonyan gyorsíthatja ezt a műveletet, és nem csak egyesével kiválasztott fájlokat, de egész mappákat is kijelölhetünk a vizsgálatra.** A feltöltő modult a készítő a két legfrissebb OS X 10.8 Mountain Lion és 10.9 Mavericks rendszerekkel tesztelték. Természetesen [várnak minden visszacsatolást, észrevételt, esetleges hibajelzést, de szívesen látnak akár új funkció ötleteket, javaslatokat is.](#)



Végül meg kell azt is említeni, hogy a dolog azért kétélű, mert egyrészt valóban felhívja a figyelmét a Mac tábornak, hogy fordítson több figyelmet a védekezésre, ám **másrészt valamennyire kontra-produktív is lehet ez, hiszen így a kártevő készítő is gyorsabban és egyszerűbben tudja majd tesztelni az új kódjait a jövőben, hogy azok minél hatékonyabban játsszák ki a vírusirtók felismerését.**

Tetszik 2 személy kedveli ezt [Regisztrájl](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pinit** **+1**

Ajánlott bejegyzések:

[Amikor a marketing üzenet már kevés](#)
[Angry Birds alkalmazásnak álcázott Mac malware](#)
[A Tibeti Macintosh kártevő nem adja fel](#)
[Több változata is van az aláírt Mac-es trójainak](#)
[Újabb Mac-es trójai kártevő](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6222731>

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](#).

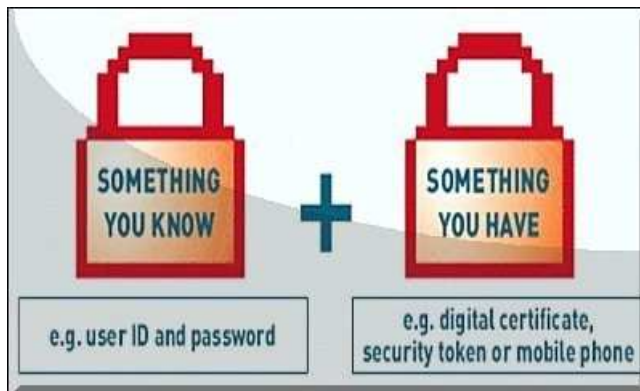
Nincsenek hozzászólások.

1 faktor + 1 faktor = 2 faktor

2014.05.30. 12:33 | [Csizmazia Darab István \[Rambo\]](#) | [2 komment](#)

Címkék: [jelszó](#) [password](#) [oleg](#) [autentikáció](#) [2factor](#) [apple](#) [ID](#) [pliss](#)

Erős jelszó, két faktoros azonosítás - csupa ilyen csúnya kifejezésről lesz ma szó. De előtte picit a jelszavak menedzseléséről. **Egy friss kutatás szerint ugyanis a korábbi IT dolgozók jelszava sok helyen még hosszú hónapokkal, sőt évekkkel később is élő marad, mivel azt nem kapcsolták le - nem hogy azonnal az épületből való távozáskor, de még azóta sem.**



A HelpNetSecurity jelentése szerint [a korábbi számítástechnikai munkavállalók negyede azóta is régi jelszával hozzáfér volt munkahelye hálózatához](#). Sőt hogy még elképesztőbb legyen a kép, 16% egyenesen úgy nyilatkozott, nem csak egy, hanem összes korábbi munkahelyi környezetéhez megvan még az élő hozzáférése. Ha ehhez pedig hozzávesszük mondjuk a Verizonnak azt a kimutatását, miszerint **a komolyabb fajsúlyú adatsértések, incidensek rendre gyenge vagy eltulajdonított belépési adatok miatt következnek be**, akkor jól látható, mekkora vétkes mulasztás is mindez az IT részéről.



[Az Oleg Pliss történetet](#) gondolom senkinek nem kell bemutatni, de dióhéjban összefoglalva ausztrál lapok számoltak be néhány napja arról, hogy néhány **iPhone és iPad felhasználót kizártak a készülékükből**. A közösségi oldalak beszámolóit, és blogbejegyzéseket szerint az áldozatok korábban egy **kéretlen üzenetet kaptak a Find My iPhone funkció nevében, amely azt írta, hogy az adott eszközt meghackelték, és csak váltásdíj ellenében adja vissza a hozzáférést**. Az már tényleg csak hab a tortán, hogy amikor a felhasználók egy nagy része emiatt az Apple-nél reklamált, az azt válaszolta nekik, hogy mivel rendszerük elvileg nem törhető fel, ezért nem illetékesek segíteni. A történet háttere az, hogy biztonsági szakértők szerint a támadók teljesen más helyszínről és más forrásból megszerzett jelszavaikat elkezdtek szépen kipróbálgatni az Apple Find My iPhone szolgáltatáson, hátha valaki itt is ugyanazt használta, és ez szemlátomást bejött nekik.



Egyébként érdekes, hogy default, vagyis alapértelmezésen hagyott jelszóval már történt korábban telefonos iPhone incidens, a nevezetes Rick Astley fotóval operáló IKEE főreg. [De hát így jár az, aki meghagyja](#) a jailbreak után a "youareshit" cseppet sem elegáns SSH default jelszót :-)



És akkor jöjjön először [a WeLiveSecurity összefoglalója, hogyan védhetik meg magukat az Apple jüzerek, ha ilyen üzenetet kaptak a készülékükre](#): "Hacked by Oleg Pliss. For unlock device YOU NEED send voucher code by 100 \$/eur one of this (Moneypack/Ukash/PaySafeCard) to [email address]". Először is semmiképpen ne fizessenek, hiszen **ez nem egy klasszikus titkosító ransomware, nem egy kártevő, hanem ahogy fentiekből olvashattunk, gyenge jelszó adatokkal való visszaélésről van szó. Akiknek volt szinkronizált mentésük az iTunes-ban vagy iCloud-ban, onnan helyre tudják állítani az előző állapotot.** Akiknek viszont nincs ilyen, adatvesztés nélkül nem igen ússzák meg a visszaállítást. Emiatt a jövőre nézve érdemes bekapcsolni a két faktoros autentikációt, javasolt rendszeresen menteni az iCloud, az iTunes, illetve a Time Machine segítségével, vagy akár párhuzamosan ezek mindegyikével. Valamint - taaaaaam - [használjunk erős és egyedi jelszót](#) az Apple ID-hez.



Végül, de semmiképpen nem utolsósorban érdemes elolvasni ezt a szájbarágó szintű útmutatót, amely a legfontosabb helyszíneken - Google, PayPal, Yahoo, Twitter, Facebook, stb. és persze az Apple ID is - menüpontonként és egérkattintásonként kirészletezve mutatja meg, [hogyan kapcsolhatjuk be a kétfaktoros azonosítást](#). Amit ha már ennyi helyen ilyen gálánsan elkészítették nekünk, talán érdemes is lenne valóban alkalmazni mindenkinek.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Lopott Minecraft jelszavak szivárogtak ki](#)

[A jelszó ötven árnyalata](#)

[Csak technikai hiba volt a Twitteres jelszó reset](#)

[Forbes és Kickstarter incidens - jelszócsere kell](#)

[Tűzre, vízre, és jelszóra vigyázzatok!](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6234722>

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](#).



Tiborr • <http://1solumipsum.tumblr.com/> 2014.05.31. 11:27:24

Sziasztok! Remek a cikk!

Pár kérdés eszembe jutott: Mondjuk ha a Google accountomhoz használok SMS azonosítást az egy kicsit kellemetlen, mindig megvárni, beírni, örülni. (Oké, még kellemetlenebb ha feltörrik, de ugye arra van a bonyolult és hosszú jelszavam.)

Vegyük a következő példát: otthon, olcsó router + Win7. Gmail, bepipálva a "Maradjon bejelentkezve", hogy ne kellejen mindig az SMS-sel szórakoznom, megkapom az SMS-t, belépek, belépve maradok. Ilyen fajta otthoni környezetben azért ott van a gyanú, hogy a megfelelő szerverek úgy tudnak ki-bejárni a gépemre, ahogy akarnak. SMS, SSL ide vagy oda, ha már bent vagyok a Gmail-ben, akkor az életem (egy része) nyitott könyv.

Persze válogathatok a különféle ingyenes és fizetős tűzfalak között, de egyszerű felhasználóként honnan tudnám eldönteni, hogy "Az ellen nem véd."?

Na mindegy, nem eszem én olyan forrón, csak ezek néha eszembe jutnak.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu>
2014.06.02. 10:51:18

Szia Tibor!

Van igazság van abban, amit írsz, de hát 2faktorost is attól kér az ember, akiben már elvileg valamennyire megbízik - ha Snowden után létezik még egyáltalán ez kategória ;-).

Például én direkt nem szeretnék ilyet a Facebooktól, mert a telefonszámom nem akarom megosztani velük, hogy aztán egy 123-ik újjászervezett biztonsági beállítás keretében mind az 1.2 milliárd FB tag felé publikus legyen.

Ennél már előbb venném igénybe ezt az Apple-nél, ha ilyenre lenne szükségem, illetve egy átlagfelhasználó ezzel például a mostani Olge Pliss esetben is jól járt volna.

Válasz erre

Életünk része lett az állandó támadás

2014.06.02. 11:11 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [privacy](#) [media](#) [online védelem](#) [eset](#) [scanner](#) [gyakoriság](#) [incidensek](#) [cnmmoney](#) [ponemon](#) [2faktor](#) [adatsértés](#)

Egy friss amerikai kutatás szerint a ma számítógép-felhasználójának már együtt kell élnie azzal a tudattal, hogy az adatlopás, és hasonló személyes adatainkat kompromittáló események már egyáltalán nem címlapra kívánczó kirívó különleges ritkaságok, hanem sajnos teljesen hétköznapi permanens veszélyforrások.



Gyorsul a tempó, és nem csak érzetre, de számszerűsítve is emelkednek a kiberbiztonsági események. Ha [felidézzük a nagyjából egy éve közreadott posztunkat](#), mi is történik a nagyvilágban egyetlen perce leforgása alatt, már akkor elképesztő számok szerepeltek ebben: "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."



Ha mindezt ma 2014-ben akarnánk valahogy kifejezni, akkor már nem is percben gondolkodva, hanem az egy másodperc alatti történetekben lehet jobban kiigazodni. Eszerint: "4608 keresés történik összesen a Google-ben, az AppStore-ból 634, a Google Play-ből 1236 alkalmazást töltenek le, a Gmail-en belül 340278 emailt küldenek el a felhasználók, 694 képet töltenek fel az Instagram-ra, 11 ember regisztrál a Twitter-re és közben 5700 tweet születik, 52196 Facebook like, 54976 Facebook bejegyzés jön létre, 463 Tumblr posztot tesznek közzé, a Dropbox-ba 11574 fájlt töltenek fel, a Reddit-en 1 poszt, 13 komment és 212 értékelés születik, a LinkedIn-en 182-en keresnek rá konkrét személyekre, a Foursquare-en 35 becsekkolás történik". És persze a jövő évi hasonló következő kimutatásban talán majd az egy secundum alatt történő security breach-ek száma is benne lesz már.



Mindenesetre a nagy számok törvénye, pontosabban a sok számítógép és a sok adatmozgás miatt - ahogy azt a klasszikus Rambo film első részében is hallhattuk Trautmann ezredes szájából: "Sok emberből sok halott is lesz" - [óhatatlanul meredeken növekszik a kiberbiztonsági incidensek száma is](#). Lássuk akkor a bevezetőben említett felmérést, amelyet CNNMoney és a Ponemon Institute végzett. Ennek eredményei arról árulkodnak, hogy tulajdonképpen az amerikaiak fele, 110 millió felhasználó érintett áldozatként valamilyen adatlopásban vagy biztonsági adatsértésben. A beszámoló szerint a legnagyobb károkat okozó incidensekben például 70 millió Target áruház ügyfél személyes adata és mintegy 40 millió hitel- és bankkártya adata került rossz kezekbe, [míg az Adobe esetében 33 millió \(más források szerint 28 millió\) felhasználói adat és 3.2 millió hitel- és bankkártya adat szerepelt](#) a veszteség oldalon, no meg emellett programok forráskódja is.



Szerepel még a veszteség listán [4.6 millió Snapchat felhasználói hitelesítő adat](#), [3 millió bankkártya a Michaels shopból](#), [1.1. millió hitelkártya adat a Neiman Marcus üzletláncból](#), [120 millió AOL hozzáférés](#), és a legutóbbi emlékeztető [148 millió ügyféladat az eBay-től](#), és a sor holnap reggelig folytatható. Az elemzés azt mutatja, ezek az adatsértések összességében már annyira gyakoriak, hogy a felhasználók jobban teszik, ha ezeket egy velük is bármikor előforduló hétköznapi kockázatként képzik el, és nem pedig valami fehér holló-szerű távoli ritka jelenségként, ami csak néha és akkor is mindig csak mással történhet meg. Vagy másképpen fogalmazva: Ha eddig nem vetted észre, hogy már áldozat vagy, akkor valószínű, hogy csak nem figyeltél eléggé.



És akkor pár keresetlen szót ejtsünk a lehetséges óvintézkedésekről is. A megfelelően erős jelszóra már nem is térünk ki, mert annyiszor emlegettük már, [hogyan védjük meg Twitter fiókunkat?](#) [Így vernek át a Facebookon és így védekezz!](#) [Így költjük a pénzt az online vásárlásoknál](#) [A Justin Bieber átverés](#) [Itt a lopásvédelemmel ellátott Smart Security 6](#) [Apple Find My iPhone funkció nevében elkövetett trükközések kapcsán](#), talán érdemes lenne ennek a lehetőségnek is nagyobb figyelmet szentelni a felhasználók részéről. Emellett továbbra is fontos lehet a biztonság tudatos netezés - alaposan meggondolva, mire kattintunk - kiegészítve természetesen a [naprakész vírusirtóval](#), valamint olyan lehetséges privát szféránkat óvó egyéb háttér eszközökkel, mint például a böngésző kliensbe épülő NoScript, NetCraftToolbar, vagy [a Facebook és Twitter fiókunkat óvni képes](#) ESET Online Media Scanner applikáció.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

- [Hogyan védjük meg Twitter fiókunkat?](#)
- [Így vernek át a Facebookon és így védekezz!](#)
- [Így költjük a pénzt az online vásárlásoknál](#)
- [A Justin Bieber átverés](#)
- [Itt a lopásvédelemmel ellátott Smart Security 6](#)

A bejegyzés trackback címe:

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 az első váltságdíjas titkosító kártevő Androidon

2014.06.06. 13:11 | [Csizmazia Darab István \[Rambo\]](#) | [8 komment](#)

Címkék: [mobil trójai](#) [android](#) [titkosítás](#) [adatvesztés](#) [kártevő](#) [váltságdíj](#) [zsaroló](#) [ransomware](#) [simplocker](#)

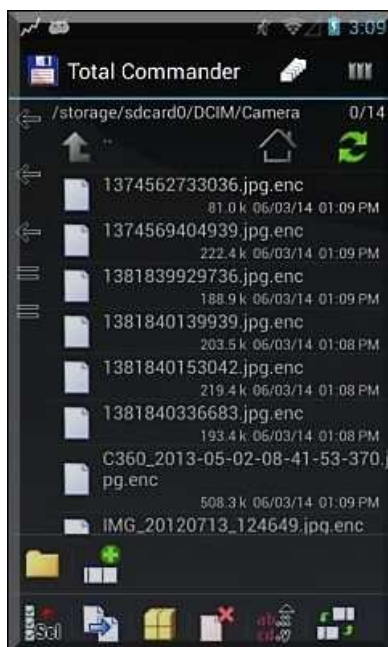
Az ESET mérnökei a múlt hét végén fedezték fel azt a vadonatúj Android platformon terjedő trójait, amely zsaroló programként terjed és titkosítja mobil eszközeink SD kártyáját. Éppen most [júniusban ünneplik a mobilos kártevők a tíz éves évfordulójukat](#), de a visszaemlékezéssel együtt kijelenthetjük, hogy a most leleplezett trójai valószínűleg az eddigi legveszélyesebb mobilos kártevő



Pont egy évvel ezelőtt bukkant fel egy Android/FakeAV.A nevű trójai, amely az ESET tavaly tavasszal végzett elemzése szerint már rendelkezett a hamis antivírusokra jellemző minden tipikus tulajdonsággal és teljes mértékben hasonlított egy lockscreen zsarolóprogramra. A múlt hónapban pedig egy olyan androidos police zsarolóprogram került a hírekbe, amely az előző években Windows és Android platformokon terjedő ransomware kártevők tulajdonságaira épülve jött létre. Az ESET akkor Android/Koler néven észlelte ezt a rosszindulatú programot, amely azonban még egyáltalán nem titkosította a fájlokat a megfertőzött eszközön.



Az új zsarolóprogram viszont már teljesen más működésű, és immár megjelent benne az adatok elkódolása is. Az Android/Simplocker névre keresztelt Androidon terjedő új trójai miután feljut az eszközökre, beolvassa az SD kártya teljes tartalmát, majd titkosítja az adatokat, és csak váltságdíj fizetése után hajlandó ezeket visszaállítani. Amint a trójainak sikerül felkerülni egy készülékre, egy zsaroló üzenetet küld, miközben a háttérben már titkosítja a fájlokat. Az Android/Simplocker.A malware az SD kártyán található összes jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp, mp4 kiterjesztéssel rendelkező képet, dokumentumot és videót megkeresi, majd AES (Advanced Encryption Standard) kódolási eljárás használatával titkosítja azokat.



Az orosz nyelven megírt zsaroló üzenet a váltságdíjat ukrán nemzeti valutában, hrivnyában kéri. Ez nem meglepő, hiszen az első

SMS-en keresztül terjedő androidos trójai is Oroszországból és Ukrajnából indult útjára még 2010-ben. Az üzenet nyers fordítása a következő:

„Figyelem! A telefonját zároltuk!

A készüléket lezártuk, mivel azon gyerekpornót, állatokkal való közösiséget és egyéb perverz videókat néztek és terjesztettek.

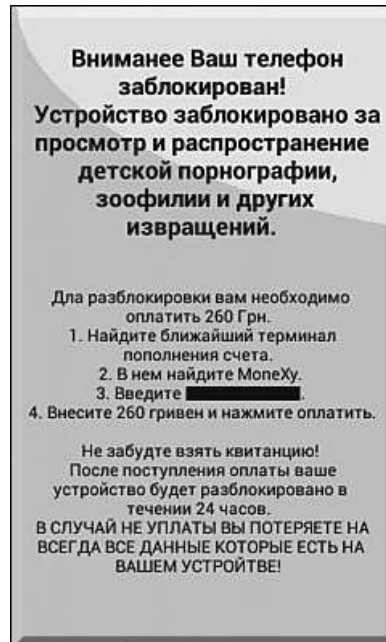
A készülék feloldásához 260 UAH megfizetése szükséges.

1. Keresse meg a legközelebbi fizetési lehetőséget.
2. Válassza a MoneXy-t.
3. Üsse be (kitakarva).
4. Utaljon 260 hrivnyát a megadott számlaszámra.

Ne felejtse el számlát kérni!

Fizetés után 24 órával a készülékét feloldjuk.

Abban az esetben, ha nem fizet, készülékéről minden adatot törölünk!”



A malware az áldozatot a MoneXy szolgáltatás használatára kéri, nyilvánvalóan azért, mert a hagyományos hitelkártyához képest itt sokkal nehezebben nyomon követhető az utalás útvonala. A 260 ukrán hrivnya nagyjából 16 eurónak, illetve közel 5000 forintnak megfelelő összeg. A trójai emellett készülék azonosításra alkalmas információkat is begyűjt az adott készülékről (például IMEEI kód, és hasonló), amit aztán továbbítja a Command & Control szerverére. A hatásosabb védelem és anonimitás érdekében a bűnözők a távoli vezérlő C&C szervert egy TOR .onion domain-en regisztrálták, amelyet emiatt sokkal nehezebb nyomon követni.

```
package org.simplelocker;

import android.content.Context;

public class TorSender
{
    public static final String PROXY_HOST = "127.0.0.1";
    public static final int PROXY_HTTP_PORT = 9050;
}
```

Miután az áldozat kifizette a kért összeget, a korábbi windowsos zsarolóprogramoktól eltérően nem jelenik meg egy fizetési kódot bekérő mező vagy ehhez hasonló beviteli felület, hanem helyett a távoli C&C szerver parancsára vár, amely a tényleges kifizetés nyugtázása után automatikusan fogja feloldani a készüléket. [Az ESET elemzése kimutatta](#), hogy egy vadonatúj módszerrel dolgozó kártevőről van szó. A malware sajnos valóban képes titkosítani a megtámadott felhasználó fájljait, és mivel maga a kártevő nem tartalmaz visszafejtési funkciókat, így állományaink véglegesen elveszhetnek, ha a titkosítási kulcsot nem sikerül letölteni.

Simplocker - Az első Android alapú fájltitkosító kártevő



PAY TO DECRYPT YOUR FILES

Az Android/Simplocker.A titkosítja az eszközünk külső memóriakártyáján található állományokat

Tűszul ejtve a fájljainkat váltságdíjat követel az elkódolt adatok helyreállításáért

Tippek a védekezésre és a megelőzéshez

Rendszeresen készítsunk mentéseket

Használjuk az ESET Mobile Security programot

Bővebb információ: WeLiveSecurity.com/Simplocker

ESET "NOW SAFER TECHNOLOGY"

Ennek ellenére a biztonsági cég **nem javasolja a fizetést az áldozatoknak, hiszen egyrészt nincs semmilyen garancia arra, hogy a csalók tényleg feloldják majd a titkosítást a fizetés után.** Másrészt pedig az esetleges fizetéssel csak bátorítjuk a bűnözőket a hasonló cselekményekre. **A hangsúlyt elsősorban a megelőzésre kell tennünk, próbáljuk megelőzni a hasonló fenyegetéseket megfelelő mobilkészít védelem használatával,** például az ESET Mobile Security for Android szoftverével. Emellett pedig **készítsünk rendszeresen biztonsági mentéseket külső adathordóra a telefonunkon található személyes tartalmakról,** így csökkentve a hasonló támadások okozta kellemetlenségeket, illetve adatvesztést.

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A váltságdíjas titkosító kártevő visszatér](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Véddj a CryptoLocker terjesztőjének fejére](#)
[A CryptoWall bevétele átlépte a milliós határt](#)
[Bitcoinos zsaroló járja be Európát](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6282709>

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](#).

[monddazigazatmar 2014.06.07. 13:21:52](#)

Ezt mind javasolják a biztonsági szakértők? Hát, bazz...
 Csinálj biztonsági másolatot, és reménykedjünk?
 Válasz erre



[Kovacs Nocraft Jozsefne 2014.06.07. 13:33:59](#)

[@monddazigazatmar](#): Nincs 100%-ig megbízható antivírus szoftver. A mentés viszont 100%-ig hatékony védelem.
 Válasz erre

[monddazigazatmar 2014.06.07. 20:28:53](#)

[@Kovacs Nocraft Jozsefne](#): Ja. De ezt magamtól is tudom. A biztonsági szakértőtől azért 2 mondattal többet várnék.
 Ez kb. annyi, mintha a tűzvédelmi szakértő azt mondaná, hogy a tűz meleg..

Válasz erre



Kovacs Nocraft Jozsefne 2014.06.07. 21:33:43

[@monddazigazatmar](#):

Tudom, hogy tudod. :)

Na de ahogy a tűzvédelmi szakértő sem csak annyi mond, hogy a tűz meleg, hanem tűzbiztonsági tanácsokat is ad, szolgáltatásokat is ajánl, az IT-biztonsági ember is ad tanácsokat (ne telepíts ész nélkül, ne menj pornóoldalra, vigyázz a törésekkel) és ajánl szolgáltatásokat (vírusirtók, persze mindig a legtöbbet fizető cégét ajánlja).

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> 2014.06.07. 21:36:20

Kedves Monddazigazatmar!

Üdv a blogon :-)

Sajna itt is hasonló a helyzet, mint a PC-ken a CryptoLocker esetében, ahol amikor lecsap a 2048 bites egyedi RSA kulcsos titkosítás, ott senki, se a Kürt Kft, se Bill Gates, se maga Ron Rivest, Adi Shamir vagy Len Adleman nem tud segíteni.

antivirus.blog.hu/2014/02/06/cryptolocker_ellen_a_megelozes_a_fontos

Persze abban egyetérték, hogy ez nyilván szomorúan hangzik, de el kell fogadni, hogy ilyen patt helyzetek is léteznek. Akváriumból lehet halászlét csinálni, de halászléből már nem lehet akváriumot.

Válasz erre



Kovacs Nocraft Jozsefne 2014.06.07. 22:16:46

[@Csizmazia István \[Rambo\]](#):

Én ezt úgy ismerem, hogy disznóból lehet kolbászt csinálni, de kolbászból nem lehet disznót. :)

Válasz erre

monddazigazatmar 2014.06.08. 03:38:31

[@Kovacs Nocraft Jozsefne](#): [@Csizmazia István \[Rambo\]](#):

Igen, csak se a kolbi, se a halászlé nem úgy készül, hogy rákattintasz valamire, amire nem kéne.

Azt mi garantálja, hogy a biztonsági másolat nem cryptolocker-ed? Ez nem védelem, meg szakértelem, hanem lófasz - már bocs.

Nem tartok semmi pótolhatatlant a telefonon, meg sd kártyán, de akkor az a lényeg, hogy nem is szabad.

Válasz erre



Kovacs Nocraft Jozsefne 2014.06.08. 08:30:36

[@monddazigazatmar](#):

A PC-re is gyakran rákattintással települ a vírus, egyéb malware vagy még rosszabb.

Ha jól értettem a posztot, a település után azonnal feldobja a zsaroló üzenetet. Vagyis ha a mentés végére még nincs üzenet, akkor nem volt titkosítás. Amúgy is érdemes megőrizni a legutóbbi 2-3 mentést.

"Igen, csak se a kolbi, se a halászlé nem úgy készül, hogy rákattintasz valamire, amire nem kéne."

Hát igen, ez a fejlődés. Berlinbe sem lovaskocsin utazunk, hanem repülünk vagy vonatozunk, s a gyorsaságért cserében vállaljuk a kockázatot. Ami utaskilométerre számolva kisebb, mint lovaskocsival. :)

Opció még a butatelefon vagy az ájfon a maga zárt környezetével, ahol kisebb a veszély. Van, akinek bejön az ájfon, de nem mindenki vállalja a kötöttségeket.

Válasz erre

Éljen soká az alapértelmezett jelszó 2.

2014.06.10. 10:18 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [hiba jelszó](#) [kanada bank](#) [csalás atm](#) [montreal default](#) [alapértelmezett](#)

Utolsó ilyen jellegű posztunk még hat éve, 2008-ban jelent meg abban a témában, hogy a meg nem változtatott alapértelmezett jelszó milyen hatalmas biztonsági rés. Akkor [bemutattuk, hogy az ATM pénzkidó automaták üzemeltetői is tudnak nem kicsit hibázni](#). A mai kérdés az, vajon most 2014-ben megszűnt-e az ilyen hiányosság a bankautomatáknál?



Azok nyertek, akik szerint az lustaság, a hanyagság mindig is szolgál nekünk hasonló elrettentő példákkal. Ugyanis a legutóbbi esetben **két kanadai középiskolás egy kissé megnyújtott ebédszünet keretében sikerrel tört fel egy Bank of Montreal bankautomatát**. Sikerükhöz természetesen nagyban hozzájárult, hogy előtte találtak az interneten egy az eszközhöz tartozó letölthető gépkönyvet. A művelet tulajdonképpen nem volt más, mint hogy bepróbálkoztak az alapértelmezett jelszóval - és tadaaam - át tudtak váltani felügyeleti módba. Ennek segítségével [látták, pontosan mennyi pénz van az automatában, mennyi tranzakció történt korábban, és hasonló olyan belső információkhoz férhettek hozzá](#), melyeket normál esetben az ügyfelek nem láthatnak.



"Amikor kitaláltuk, hogy kipróbáljuk a gépkönyvben írtakat, valójában arra számítottunk, ez biztos nem fog sikerülni. Ám legnagyobb meglepetésünkre az egyik gyári jelszót simán elfogadta, amiből úgy tűnik, ezt az üzembe helyezés óta valószínűleg nem is változtatták meg, hanem így hagyták" - mondta később az egyikük. Mivel nem csalókról, hanem kíváncsi, de jó szándékú gyerekekről van szó, azonnal kapcsolatba léptek a Bank of Montreal irodájával, ahol jelentették, mit tapasztaltak. Először nem akartak hinni nekik, de a rendszerben aztán valóban látták, hogy igaz a dolog. Matthew Hewlett és Caleb Turon még arra is vették a fáradságot, hogy az ATM alapértelmezett üdvözlő üzenetét "Welcome to the BMO ATM" (Üdvözljük a BMO pénzkidó automatájánál) átírják a "Go away. This ATM has been hacked." (Kérem menjen el, ezt az ATM-et feltörték) figyelmeztető szöveggel. [A bank biztonsági részlege későbbi szűkszavú közleményében jelezte, hogy "az akció során semmilyen ügyféladat nem került veszélybe", és megköszönték a fiatalok bejelentését.](#) (Érdekes kérdés, hogy ha mindez Magyarországon történt volna, akkor elvileg megvalósul a számítástechnikai rendszer és adatok elleni bűncselekmény.)

Rank	Password	Number of Users with Password (absolute)
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542



Sok apró momentumból áll össze a biztonságna nevezett nagy egész, amiben nem csak az alkalmazott technikai megoldások, hanem többek közt a fizikai hozzáférés védelme, a biztonságos beállítások, a naprakész frissítések, a social engineering elleni felvétezettség valamint a rendszeres biztonságtudatossági képzések is szerepelnek. Ennek egyik fontos szegmense az alapértelmezett jelszavak haladéktalan megváltoztatása is. Még a leghétköznapiabb esetben - [például egy otthoni internetes routernél](#) - is azonnal ajánlatos a setup beállítások jelszavát az admin/admin-ról megváltoztatni amellet, hogy a wifi kapcsolat WPA2-es esetében is választunk a deafult LINKSYS helyett egy semmitmondó vagy semleges nevet (nem "DrKovacs_III.2.", hanem például "Connection_error_117"), valamint egy hozzá tartozó erős jelszót. A már évek óta tartó sorozatos security breachek és az ilyenkor nyilvánosságra kerülő passwordok, illetve hashek tanulságai viszont azt mutatják, hogy sajnos nem csak a bamba jelszavak (abc, 12345, stb.) **roppant gyakoriak, hanem az is, hogy a felhasználók egy jelszót több különböző helyszínen is használnak.**

Hossz jelentősége						
Támadó rendszer	6	7	8	9	10	11
Amatőr	90 mp	2,35 óra	9,20 nap	2,40 év	226 év	21222 év
Titan	0,01 mp	1 mp	1,61 perc	2,52 óra	9,90 nap	2,58 év
Variációk száma = 94^n						

A jelszavak aktuális hosszúságához tartozó bruteforce időkről sokatmondó lehet [Dinya Péter BSc tavalyi díjnyertes, az "Év információbiztonsági diplomadolgozata" munkája](#), amelynél a hagyományos felszereltségű PC mellett a Titan nevű szupercomputer erőforrásai mellett történő feltörési idők is szerepelnek. Itt a jelenlegi adatok mellett - amelyek Moore törvénnyel, a technika további fejlődésével (GPU, cloud, etc.) a jövőben természetesen folyamatosan változhatnak - az látszik, hogy **11 karaktertől indulva már hiperúgrás történik a korábbi percek-órák-napok léptékből az (elvileg) évek tartamú visszafertési hosszra**. És bár záró infografikánk szerint - amely a Stanford egyetemen készült - 16 illetve 20 hossz felett már nincs akkora jelentősége az előírt kevert, azaz kisbetű, nagybetű, számjegy, különleges karakterek vegyített használatának, azért ha már egyszer jelszót gyártunk, érdemes beletenni ilyeneket is, hiszen ingyen van ;-)



Ajánlott bejegyzések:

[Éljen soká az alapértelmezett jelszó](#)
[Litvániából szeretettel](#)
[Túlélőkészlet webáruházi adatlopások ellen](#)
[LastPass a pácban](#)
[Google Glass a biztonságos bankoláshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6291392>

Kommentek:

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

Nincsenek hozzászólások.

Itt a foci VB, jönnek az átverések is

2014.06.12. 11:44 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [spam ingyen foci vb csalás átverés nyeremény brazília fifa welivesecurity.com](#)

Egyre több a kérértlen levelek között a foci világbajnokság témájával foglalkozó próbálkozás, érdemes résen lenni, mert sok a csalás. Az ingyen lottós vagy gratis ajándékos sablonszöveg még mindig hatásos csali, így például az állítólagos pénznyereményünk mellé csak most csak nekünk ingyen jegyet is ígérnek a foci VB-re.



Ma este megkezdődik a FIFA torna, ám a spam küldők már hamarabb elkezdték az edzést, és hetek óta bombáznak bennünket a szemétlevelekkel. Egy kimutatás szerint mára nagyjából a spam termés ötöde foci VB-s apropóval érkezik, így nekünk is érdemes ellenük valamilyen taktikát bevetni. Az ESET labor szerint elsősorban Latin-Amerikában terjednek az ilyen levelek, de világszerte is lehet találkozni ezekkel. A helyiek számára például az utolsó pillanatban megvehető "last minute" jegy lehetőség jelenthet erős kísértést, ám nem árt tudni, félelmetes mennyiségű hamis jegyet próbálnak így a pénzüktől megszabadított próbálkozókra rásózni, ez a [nagyobb koncerteken vagy sport eseményeken](#) egy tipikus átverési forma. A látszatra igazi jegyekben azonban nincsen azonosító chip, ami általában már csak a beléptetőkapuknál derül ki.



Természetesen ilyenkor [minden csatomán és platformon](#) érkeznek az adathalász, és egyéb átverést tartalmazó próbálkozások, így közösségi oldalakon új televízió készüléket ajánlanak, focival kapcsolatos hamis tombola jegyeket vehetünk hamis linkeken, vagy újdonsült foci szurkoló "ismerősök" várják visszaigazolásunkat, lájkjainkat. A csábító ajánlatok - például olcsó LCD televízió, vagy nyereményjáték, amivel a teljes esemény megtekintését megkaphatjuk az utazási és szállásköltséggel együtt - biztosan sokakat levesz a lábáról, és kattintásra kész, pedig ha csak felidézük, ha egy ajánlat túl szép ahhoz hogy igaz legyen, akkor nagy valószínűség szerint nem is igaz. Ha a nyereményjátékhoz a naiv felhasználó megadja a részletes személyes adatait: név, otthoni lakcím, telefonszám, bankkártya adatok - akkor ezeket [később személyazonosság-lopáshoz is fel tudják használni a bűnözők](#).



Természetesen nem hiányozhat a sorból a meccs eredmények helyes megtipplésével kapcsolatos állítólagos nyereményekről való értesítés sem, a korábbi e-mail lottós csaláshoz hasonlóan ilyenkor is simán kaphatunk, ha nem fogadtunk semmire. A [szenzációs híreket, nagy sztorikat](#) vagy éppen különleges videókat ígérő linkeket is érdemes óvatosan kezelni, hiszen [az ilyen állítólagosan hiányzó "kodeket"](#) vagy pedig hamis [Adobe Flash-t letöltő átverések már több éves trükkök](#). A tájékozódást érdemes a megbízható sport hírportálokra, vagy akár a FIFA weboldalára bízni, ahol ráadásul "előre lájk" mentesen tudjuk olvasni a percre kész információkat.

 Tetszik 4 személy kedveli ezt Regisztrájl, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Ismét nyertünk 450,000 eurót :-\)](#)

[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)

[Valentin nap: Szerelem helyett átverés érkezik](#)

[Közelgő Karácsony, szaporodó adathalászat](#)

[Csaláselhárítás fordított képkereséssel](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6297772>

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 Darab István \[Rambo\]](#) • <http://antivirus.blog.hu>
[2014.06.17. 10:26:21](#)

A futball-vb legalattomosabb csalásai:

biztonsagportal.hu/a-futball-vb-legalattomosabb-csalasai.html

Válasz erre

Vajon vannak-e hihető reklámok?

2014.06.16. 16:29 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [spam](#) [hirdetés](#) [jelszó](#) [fogyókúra](#) [átverés](#) [twitter](#) [csodaszer](#) [pinterest](#) [asian fruit that burns fat for you](#)

Hogy egyáltalán létezik-e ilyesmi, arról nem kívánunk sem nyilatkozni, sem pedig vitát nyitni. Ám azt határozottan állíthatjuk, hogy az alábbi Twitteren és Pinteresten terjedő spam kampány által hirdetett fogyókúrás varázsszer biztosra vehetően nem tartozik ezek közé.



A hirdetések egyre csak jönnek, jönnek, és persze mi jobbra csak olyankor tűzzük ezeket napirendre, ha valamilyen negatív eseményt, anyagi veszteséget vagy éppen direkt vírusfertőzést okoznak. **A tavaly ősszel a vírusvédelmi figyelmeztetésnek látszó reklám az Android telefonokon például a felelőtlen kattintás után 15 EUR-ba - kb. 4400 HUF - került a figyelmetlen felhasználónak. És nem, nem egyszer, hanem attól kezdve rendszeresen és HETENTE,** leiratkozni pedig igencsak körülményes róla - na vajon miért;-). Az igazán szomorú azonban az egészben az volt, hogy egy valódi, a Google Play piacon kapható fizetős legális antivírus díja is hasonló, **csak éppen az már egy teljes esztendőre lenne ennyi és ráadásul valóban meg is védené a készüléket.**



Mostani történetünkben a beszámolók szerint az elmúlt hetekben a Twitter és a Pinterest oldalait árasztották el a legújabb fogyókúrás varázsszerről szóló spamek: "az ázsiai gyümölcs, amely helyettünk égeti a zsírt", LOL. Természetesen szintén "igazi" és szuper hihető kommentek is olvashatók voltak alatta, a boldog beszámolók szerint **nincs is más dolgunk, mint gyorsan megvenni a terméket és rövid idő elteltével máris 12 kilóval leszünk könnyebbek, mint korábban.** Illetve ha ez a része nem is 100%, de a pénztárcája biztosan vékonyabb lesz minden ilyen szert vásárló illetőnek, és az a hatás viszont tényleg azonnali ;-). **Jól láthatóan, mivel a közösségi oldalak felhasználói is egy óriási méretű piac, nem csak megéri a csalóknak a tömeges spam, hanem visszájára fordulva a közösségi értékelések, bejegyzések is vesztek az eredeti értékmérő szerepükből, hiszen már ezeket is nagyüzemben manipulálják, hamisítják, generálják.** Egyre kevésbé jelent garanciát, hogy a "több szem többet lát" elv alapján valós, hihető kommenteket vagy értékeléseket látunk, így emellett vagy ehelyett a keresőkre érdemes még hagyatkozni, hiszen a nagyobb merítésből a jelentősebb átverésekről biztosan találunk károsult beszámolókat.



A spameléshez természetesen mindenhol nagyban hozzájárulhatnak a gyenge és/vagy mindenhol azonos jelszavak, amiket kitalálva, vagy mindössze próbálgatva sikerrel lehet aztán belépni más felhasználók nevében, és ott megszórni az ismerőseiket a kénytelen reklámszeméttel. A Pinterest esetében például idén tavasszal is volt már egy ehhez hasonló komolyabb támadás, [akkor és ott női](#) [fehémeműkkel illetve szintén fogyókúrák akciókkal kapcsolatos spam](#) árasztották el az oldalakat. Az mindenesetre világosan látszik, hogy mivel a Pinterest is rohamtempónak növekszik, így vonzó és potenciális célpont lett a Twitter és a Facebook mellett.

Az üzemeltetők igyekeztek ebben az esetben is fellépni a kénytelen reklámszemét ellen, így a jogsértő bejegyzések jelentős részét már a hétvégén törölték, illetve a beállítások módosításával eltávolították azokat a nyilvánosság elől. Mivel a megtámadott fiókoknál az adatvédelmi beállítások is megváltoztak - még nem tudni, hogy ezek automatikusan vagy kézzel módosultak-e a támadás miatt - ezért a haladéktalan jelszócsera mellett a biztonsági beállítások ellenőrzése és ha szükséges, módosítása is az elhárítás szükséges lépései közé sorolható.



Nem győzzük elégszer hangsúlyozni, hogy [az ilyen hamis vásárlói értékelésekkel hirdetett zöld-kávékhoz hasonló népszerű átverések](#) új köntösben folyamatosan itt ólálkodnak körülöttünk. Az elkövetők a túlságosan hiszékenyek pénzére spekulálnak - akik nem étrend módosítással, reggeli futással, rendszeres sportolással és teljes életmód váltással próbálkoznak, hanem valamilyen csodapirulával akarnak varázsütésre megváltozni - és sajnos többnyire sikerrel szabadítják meg őket pénzüktől. Vagyis a kőbe véshető formulával fogalmazva: "gondolkozzunk: ha valami túl szép ahhoz, hogy igaz legyen, az nagy valószínűséggel tényleg nem igaz, hanem átverés". És ezt nem csak akkor kell figyelembe venni, [ha állítólag maga Bill Gates éppen elosztogatja a vagyonát](#), hanem a nyár és a bikiniszezon megérkezésével hirdetett fogyókúrák csodaszereknél ugyanúgy, jöjjön az üzenet bármely közösségi oldalon, vadidegentől vagy éppen saját ismerősünk nevében.

[Tetszik](#) Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+](#)

Ajánlott bejegyzések:

[Csaláselehárítás fordított képerkeséssel](#)

[A jó név felsiker](#)

[A LinkedIn support üzent nekünk. Vagy mégsem?](#)

[Közlegő Karácsony, szaporodó adathalászat](#)

[Átverés a Google spam](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6306124>

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](#).



[**maxell a nevét és profilképét változtatgató birka 2014.06.17. 17:20:26**](#)

Aki a neten vesz gyógyszernek minősülő készítményeke, az meg is érdemli!

Neszebárban van egy jó kis táplálék kiegészítőket forgalmazó üzlet a Sztefan Botev utca 318/a. szám alatt, én ott szoktam beszerezni az elhízás elleni tablettákat.

Csak hazai (bolgárországi) gyártású, a Szláv Unió előírásainak mindenben megfelelő termékeket forgalmaz, amelyek hatékonyak és még sosem volt semmi botrány az említett Яклежш márkájú szerekkel.

Válasz erre



[**enpera • <http://uborkakonzerv.blog.hu/> 2014.06.17. 19:28:58**](#)

[@maxell az okoskodó birka](#): köszönjük a reklamot, bar qrvara nem kértük

Válasz erre

[**bullseye 2014.06.23. 10:47:57**](#)

Nekem pedig maradt a raktárban egy csomó iPhone, lehet jelentkezni érte, hitelkártyaszámmal és kóddal a szinte biztos nyereményért!

Válasz erre

Az androidos titkosító kártevő újra boncolása

2014.06.18. 11:28 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [java](#) [android](#) [kártevő](#) [aes](#) [helyreállítás](#) [titkosító](#) [simplocker](#) [simplelocker](#)

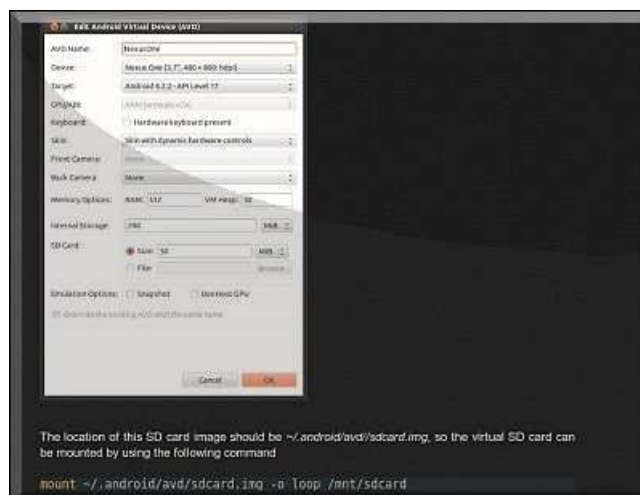
Lehetne a poszt címe "Ha csak úgy nem", vagy egy újabb eleme "A kártevőkészítők által elkövetett kezdeti szarvashibák a Proof of Concept típusú első verziós kódokban" is. Mindenesetre egy egyetemista programozói szemmel elemezte a Java kódot, és **szerencsés módon megoldást talált az elkódolt fájlok visszafejtésére az egyébként TOR hálózat alapú C&C vezérlő szerver, és a váltságdíj fizetési procedúra teljes kihagyásával.**



Június elején számoltunk be arról, hogy [felfedezték azt a vadonatúj Android platformon terjedő trójait, amely zsaroló programként terjed és titkosítja mobil eszközeink SD kártyáját](#). Sajnos a mobil platformokat sem kerülte el váltságdíjat szedő kártevők hulláma, amelyek ál vírusirtóként illetve hamis szerzői jogi, illetve police típusú kártevőként már legalább egy éve jelen vannak. Ám az korábban sosem fordult még elő, hogy egy ilyen rosszindulatú program titkosította volna a fájlokat a megfertőzött mobil eszközön, és ezekért kért volna váltságdíjat. Azon viszont, hogy **a hatásosabb védelem és anonimitás érdekében a bűnözők a távoli vezérlő C&C szervert egy nehezebben nyomon követhető TOR .onion domain-en regisztrálták, vagy hogy a fejpénzt ukrán hrivnyában kérik, már szinte meg sem lepődtünk.**



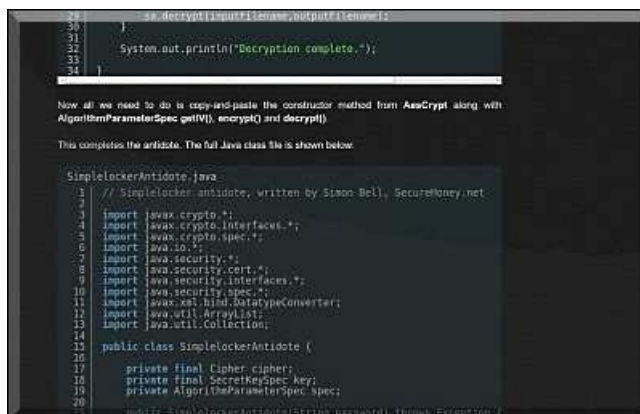
Nos az ördög a részletekben lakozik, gondolhatta magában Simon Bell egyetemi hallgató, és nekiállt, hogy ő is közelebből is tesztelje az első Androidon megjelent váltságdíjas titkosító kártevőt. A vizsgálatait statikus és dinamikus környezetben is elvégezte, és [igyekezett megérteni, hogy az .ENC fájlok titkosítása pontosan milyen lépéseken, hogyan és milyen Java osztályok közreműködésével megy végbe](#). Az Android Emulátorban létrehozott virtuális SD kártya tartalma a kártevő futtatása után neki is sikeresen elkódolódott. A kód elemzéskor azonban jól látszott, hogy a **Simplocker nála futó első verziója egy minden tekintetben PoC, azaz kísérleti kártevő, amelyben a felhasználók óriási szerencséjére a titkosítás mégsem sikerült tökéletesre, így annak gyengeségeit akár ki lehetne használni.**



Következő lépésként mi is jöhetett volna más, mint ahogy meg kellene próbálni egy egyszerű Java kóddal anélkül helyreállítani az AES segítségével elkódolt fájlokat, hogy ahhoz külső kapcsolat, vezérlő szerver, váltságdíj vagy bármilyen külső tényezőre szükség lenne. **Ezzel zárult az első írás, így ezt a június 16-i részletes elemzés végén az olvasóknak meg is ígérte, így kíváncsian várhattuk a következő blogposztot, bár a lényeg ugye már ebben is tulajdonképpen benne volt :-)**



Amely bejegyzés aztán rögtön másnap, 17-én meg is született. Elmondása szerint nem volt különösebben nehéz dolga, hiszen a fentiek alapján sikeresen **felfedezte, hogy a dekódolási jelszóhoz konstansként tud hozzáférni. Ezután írt gyorsan egy saját függvényt, amely végiglépked az SD memória kártyáján tárolt .ENC kiterjesztésű állományokon, majd helyreállítja azokat.** Azért persze a siker mellett a **emeljük ki, hogy ez piszok mázli volt, és semmiképpen nem lehet ok arra, hogy ezentúl mégse mentsük rendszeresen személyes adatainkat az okostelefonunk memóriakártyájáról, vagy hogy a jövőben ne használjunk rajta vírusirtót, és a miértéről is azonnal szó fog esni.**



Természetesen - ahogy maguk az eredeti elemző posztok említik, és ezt a majd 30 éves vírustörténelem tapasztalatai alapján mi magunk is csak megerősíthetjük - ezeket a kezdeti gyengeségeket a kártevőkészítők valószínűleg nagyon gyorsan felfedezik és befoltozzák majd. Nyilván ők is rendszeresen olvasnak szakajót és szakmai blogokat, meg közben látják is, hogy ni csak nem az elvárt ütemben ömlik be hozzájuk a pénz. Érdemes megemlíteni például a Windows PC-ken még 2008-ban felbukkant GP Code esetét, ahol az bár erős, 1024 bites RSA titkosítással kódolta el a felhasználó adatait, ám a vírusrkutatók az első verziós PoC-ban felfedezték, hogy a titkosítás elkészültével az eredeti kódolatlan fájlok viszont csak sima magas-szintű állomány törlési paranccsal lettek törölve kinullázás vagy felülírás nélkül, így azokat **ha közben nem történt jelentős fájlművelet a lemezen, egy szimpla undelete segítségével egyszerűen vissza lehetett hozni.** Persze ennek nyilvánosságra kerülése után a kártevő készítői sem késlekedtek sokat, és a heteken belül megjelent következő változatban már sajnos nem követték el újra a primitív szarvashibát.



Ezt a viharos Speedy Gonzales tempót egyébként a Microsoft saját hibajavításánál is szívesen látnánk, ehhez csak két adatot mutatunk a viszonyítás kedvéért. Amikor 1995-ben az első makró vírusok megjelentek az Office 95-ben, kiderült, hogy dokumentum megnyitáskor alapértelmezett az automatikus makrók lefutása. **Mégis az ezt megszüntető frissítés csak 2000-ben látott napvilágot, vagyis mindez nagyjából 6 évig nyitva volt a vírusok előtt.** Nem volt sokkal jobb a helyzet az Autorun vírusok esetében sem, ahol az első ilyen vírus felismerése még 2007. júniusában került be a vírusirtók adatbázisaiba, ám az Autorun letiltó frissítést a Microsoft végül csak 2011. februárjában adta ki, tehát durván négy esztendő kellett nekik hozzá, vagyis lehetne még hova gyorsulni :-).

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A váltásdíjas titkosító kártevő visszatér](#)
[Itt az első váltásdíjas titkosító kártevő Androidon](#)
[Beváltak-e a 2014-es jóslatok?](#)
[Újra Bitcoin bányász kártevő a Google Play-en](#)
[Kamu Android app hajt a pénzünkre](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6339869>

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> 2014.06.18. 11:48:18

Arra azért nagyon kíváncsi lennék, hogy ezt az elképesztő bonyolultságú megoldást miért nem az ESET (vagy más vendor) jól fizetett szakértői fedezték fel...

Válasz erre



[Csizmazia Darab István \[Rambo\]](#) • <http://antivirus.blog.hu> 2014.06.18. 13:59:02

Ennek csak egyetlen logikus magyarázata lehetséges: mindenki a foci VB-t nézi, közben pedig Bell barátunk láthatóan utálja a futballt ;-)))

Komolyra fordítva a szót előbb-utóbb mindenképpen kiderült volna, ez csak idő kérdése. Amellett pedig a laborokba érkező napi 60 ezer - 200 ezer minta nem kicsit leterhelő, ezt is figyelembe kell venni.

Válasz erre



[buherator](#) • <http://buhera.blog.hu> 2014.06.19. 10:05:34

[@Csizmazia István \[Rambo\]](#): A marketingposzt megírása úgy látszik magasabb prioritást élvezett... Nem hánytorgatnám fel a dolgot, ha egy "hagyományos" szétobfuszált natív malware-ről lenne szó, de egy Java bytekódban megtalálni egy bedrótozott jelszóval dolgozó AES rutint kevesebb időt vesz igénybe, mint beillesztetni a képeket a blogszerkesztőben.

Válasz erre

Instagram üzenet. Vagy mégsem?

2014.06.23. 11:45 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam kanadai vagy mégsem gyógyszerész instagram](#)

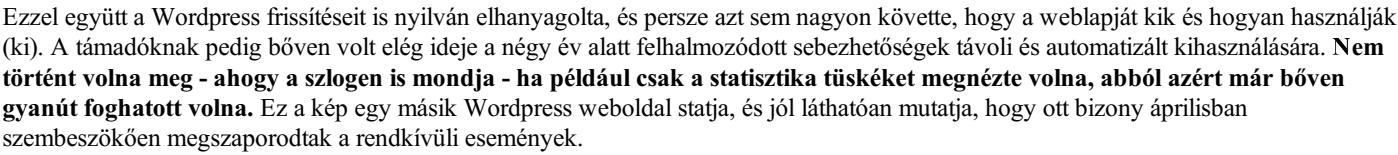
Kimeríthetetlen [Vagy mégsem? rovatunk](#) újabb epizóddal jelentkezik, ezúttal az Instagram értesít bennünket arról, hogy sikeresen elküldte a privát képeinket. Várjunk csak, kértünk mi ilyesmit egyáltalán? Fejvakarás... Hogy hova is küldte a képeinket? Az viszont persze nem látszik, de lehet kattintani a kétértelmű e-mail üzenetben található linkre a "bővebb információért" ;-)



Ebben a témakörben volt már Java frissítéstől kezdve, átverős Microsoft Update-en át, Google Plus meghívó, hamis iTunes számla, e-mail a Youtube-tól, írt nekünk a CERT és LinkedIn meghívót is kaptunk már, sőt értesítettek minket arról is, hogy állítólag új képek érkeztek a Picasa albumunkba. A spamek linkjei szerencsére többnyire nem kártevőre mutattak, hanem "csak" adathalász oldalra, illetve leggyakrabban valamilyen kanadai gyógyszerész, azaz hamis gyógyszereket áruló webáruházra. Nézzük akkor a mai potenciális áldozatunkat, hova vezet a nyilvánvalóan nem az Instagram üzemeltetői által nekünk küldött levél, amit egyenesen Stacy Green adminisztrátortól kaptunk.



Az egér hover tisztán és világosan kiírja, hogy linkünk eredetileg egy valaki által teszteltetett Wordpress lapra mutat, nevezetesen [a 2010-ben lefoglalt nurielreviews.com weboldalra](#). Itt emberünk anno 2010. január 18-án még nagy lelkesen tervezgette, hogy milyen játszi könnyedséggel fog angyalos témájú CMS weboldalt készíteni. El is jutott az értékes "Hello World", valamint a még értékesebb "Hi, this is a comment" teszt bejegyzésig, majd ennél a pontnál valószínűleg elsodorhatták az események. Meggondolta magát és Nuriel helyett végül inkább Rafaelról, Sindolfonról, esetleg Mitatronelről készített weblapot, vagy pedig megivott még egy sört, és totálisan elfelejtkezett az egész tervről.



A spam linkjére kattintva a Nuriel-es Wordpress weblap egyik dokumentumába beszúrt script "compactor.php" aztán [átadob minket egy ali pár hete bejegyzett orosz weboldalra](#), amely Viagrával és egyéb diszkont áras hamis gyógyszerrel várja a balekokat.

```

<html><head><script type="text/javascript">do{
[115,116,117,118,119,120,121,122,123,124,125,126,127,128,129,130,131,132,133,134,135,136,137,138,139,140,141,142,143,144,145,146,147,148,149,150,151,152,153,154,155,156,157,158,159,160,161,162,163,164,165,166,167,168,169,170,171,172,173,174,175,176,177,178,179,180,181,182,183,184,185,186,187,188,189,190,191,192,193,194,195,196,197,198,199,200,201,202,203,204,205,206,207,208,209,210,211,212,213,214,215,216,217,218,219,220,221,222,223,224,225,226,227,228,229,230,231,232,233,234,235,236,237,238,239,240,241,242,243,244,245,246,247,248,249,250,251,252,253,254,255,256,257,258,259,260,261,262,263,264,265,266,267,268,269,270,271,272,273,274,275,276,277,278,279,280,281,282,283,284,285,286,287,288,289,290,291,292,293,294,295,296,297,298,299,300,301,302,303,304,305,306,307,308,309,310,311,312,313,314,315,316,317,318,319,320,321,322,323,324,325,326,327,328,329,330,331,332,333,334,335,336,337,338,339,340,341,342,343,344,345,346,347,348,349,350,351,352,353,354,355,356,357,358,359,360,361,362,363,364,365,366,367,368,369,370,371,372,373,374,375,376,377,378,379,380,381,382,383,384,385,386,387,388,389,390,391,392,393,394,395,396,397,398,399,400,401,402,403,404,405,406,407,408,409,410,411,412,413,414,415,416,417,418,419,420,421,422,423,424,425,426,427,428,429,430,431,432,433,434,435,436,437,438,439,440,441,442,443,444,445,446,447,448,449,450,451,452,453,454,455,456,457,458,459,460,461,462,463,464,465,466,467,468,469,470,471,472,473,474,475,476,477,478,479,480,481,482,483,484,485,486,487,488,489,490,491,492,493,494,495,496,497,498,499,500,501,502,503,504,505,506,507,508,509,510,511,512,513,514,515,516,517,518,519,520,521,522,523,524,525,526,527,528,529,530,531,532,533,534,535,536,537,538,539,540,541,542,543,544,545,546,547,548,549,550,551,552,553,554,555,556,557,558,559,560,561,562,563,564,565,566,567,568,569,570,571,572,573,574,575,576,577,578,579,580,581,582,583,584,585,586,587,588,589,590,591,592,593,594,595,596,597,598,599,600,601,602,603,604,605,606,607,608,609,610,611,612,613,614,615,616,617,618,619,620,621,622,623,624,625,626,627,628,629,630,631,632,633,634,635,636,637,638,639,640,641,642,643,644,645,646,647,648,649,650,651,652,653,654,655,656,657,658,659,660,661,662,663,664,665,666,667,668,669,670,671,672,673,674,675,676,677,678,679,680,681,682,683,684,685,686,687,688,689,690,691,692,693,694,695,696,697,698,699,700,701,702,703,704,705,706,707,708,709,710,711,712,713,714,715,716,717,718,719,720,721,722,723,724,725,726,727,728,729,730,731,732,733,734,735,736,737,738,739,740,741,742,743,744,745,746,747,748,749,750,751,752,753,754,755,756,757,758,759,760,761,762,763,764,765,766,767,768,769,770,771,772,773,774,775,776,777,778,779,780,781,782,783,784,785,786,787,788,789,790,791,792,793,794,795,796,797,798,799,800,801,802,803,804,805,806,807,808,809,810,811,812,813,814,815,816,817,818,819,820,821,822,823,824,825,826,827,828,829,830,831,832,833,834,835,836,837,838,839,840,841,842,843,844,845,846,847,848,849,850,851,852,853,854,855,856,857,858,859,860,861,862,863,864,865,866,867,868,869,870,871,872,873,874,875,876,877,878,879,880,881,882,883,884,885,886,887,888,889,890,891,892,893,894,895,896,897,898,899,900,901,902,903,904,905,906,907,908,909,910,911,912,913,914,915,916,917,918,919,920,921,922,923,924,925,926,927,928,929,930,931,932,933,934,935,936,937,938,939,940,941,942,943,944,945,946,947,948,949,950,951,952,953,954,955,956,957,958,959,960,961,962,963,964,965,966,967,968,969,970,971,972,973,974,975,976,977,978,979,980,981,982,983,984,985,986,987,988,989,990,991,992,993,994,995,996,997,998,999,1000,1001,1002,1003,1004,1005,1006,1007,1008,1009,1010,1011,1012,1013,1014,1015,1016,1017,1018,1019,1020,1021,1022,1023,1024,1025,1026,1027,1028,1029,1030,1031,1032,1033,1034,1035,1036,1037,1038,1039,1040,1041,1042,1043,1044,1045,1046,1047,1048,1049,1050,1051,1052,1053,1054,1055,1056,1057,1058,1059,1060,1061,1062,1063,1064,1065,1066,1067,1068,1069,1070,1071,1072,1073,1074,1075,1076,1077,1078,1079,1080,1081,1082,1083,1084,1085,1086,1087,1088,1089,1090,1091,1092,1093,1094,1095,1096,1097,1098,1099,1100,1101,1102,1103,1104,1105
```

Jól láthatóan [hemzsegek a hamis értékelések, amelyben agyba-főbe dicsérik az webshopot](#). Van aztán az oldal alján "megbízható" Verisign logó, Verified by VISA ikon, meg a sok csomagküldő plecsni mellett természetesen az elmaradhatatlan bankkártya elfogadás, sőt még "Privacy Policy" is és vicces módon "Anti-Spam" menüpont is. Ez utóbbiban arról tájékoztatnak bennünket, hogy ők milyen szigorú spam ellenes policy-vel is rendelkeznek :-)



Mai záró üzenetünket amolyan gondolatébresztőnek szánjuk. **Te olvasó, igen igen te! Ha van olyan weblapod, domained, amit még a Dózsa-féle parasztfelkelés előtt lefoglaltál, de már évek óta feléje sem néztél, akkor most ezennel ünnepélyesen eljött az idő. Az ott futó ősköveget php, Wordpress, Joomla vagy Drupal miatt lehet, hogy az már régen nem a te weblapod, hanem ugródeszka akárhova.** Ha a beszúrt JavaScript kódok nem visznek közvetlenül vírusos oldalakra, akkor esetleg [nem is kap róla a tulajdonos Google figyelmeztetést \(Bejelentett Támadó Webhely\)](#). Tehát frissítsünk, ellenőrizzünk, vagy ha végképp felesleges a korábban még oly fontos domain, akkor kár fizetni érte és közben kompromitállódni hagyni - lehet, hogy ideje inkább meghirdetni.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **G+**

Ajánlott bejegyzések:

[Új Picasa képek az albumunkban. Vagy mégsem?](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[LinkedIn meghívó. Vagy mégsem?](#)
[Átverés a Google spam](#)
[Telekom számla vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6404343>

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.

Schumacher hamis halálhíre az új átverés

2014.06.25. 10:32 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [facebook](#) [schumacher](#) [átverés](#) [michael](#) [hamis](#) [halálhír](#)

Épp a tegnapi napon derült ki, hogy ismeretlen elkövetők [ellopták Michael Schumacher orvosi kartonját és az adatokat pénzért árulják az interneten](#). Most pedig itt a formula egyes pilóta halálhíréről szóló Facebook üzenet, ami természetesen nem igaz, célja a naív látogatók kattintása utáni pénzkereset.



Hamis halálhíres posztokért az antivírus blognak sosem kellett a szomszédba mennie, hiszen [volt már itt Chuck Norrisról](#) szóló poszt, [meghalt nálunk Hannah Montana](#) alias Miley Cyrus, "történt" [Johnny Depp-es autó baleset](#), de szerepelt már ebben a kontextusban a [volt kubai államfő Fidel Castro](#), vagy éppenséggel [a zenész Eminem](#) is.



A mostani üzenet a hamis halálhírral egy látszólag egy videót is tartalmazó üzenettel érkezik az alábbi szöveggel: *"{R.I.P } F1 Star Michael Schumacher dead after come out from COMA few seconds ago. miss you champ!"*. Vagyis magyarul azt írják, hogy a kómából nemrég feléledt F1 versenyző épp az imént hunyt el, és mindenkinek hiányozni fog a híres bajnok. **Sajnos az átverést sokan már alaptól is továbbosztják**, ha pedig valaki a videónak látszó linkre kattint, akkor [egy olyan külső weboldalra kerül, amely a rapidstockprofit domainre mutat, bár kinézetében igyekszik a Facebookos kinézetet másolni](#).



Akik [olvasták a hamis kodekes](#) történeteinket vagy hallottak [az indiánok a Facebookon esetről](#), azok nem lepődnek meg, hogy helyette azt az üzenetet kapjuk, miszerint a "Restricted Breaking News" videó megtekintése előtt meg kellene osztanunk ezt a Facebookon, csak akkor nézhetjük meg. [Ha előre lájk vagy előre megosztás kell](#) egy állítólag érdekes videó megtekintéséhez, legyen "aha" élményünk, hogy [átverés az egész, és ne kattintsunk](#).



Sajnálatos, hogy sokan ennyire nincsenek tekintettel az F1 pilóta hozzátartozóira - akik aggódtak és szenvedtek már éppen eleget ezzel a balesettel kapcsolatosan - és mások baján, nyomorúságán igyekeznek ilyen szánalmas kattintásvadász módszerekkel pénzt keresni.



Mivel ez az erősen ízléstelen, ám mégis rendszeresen visszatérő téma sajnos sokszor előbukkan, ezért mostantól minden hasonló posztot a ["Kártékony antivirus linkek - villám őrjárat" sorozatunkhoz](#) híven itt is egy jól bevált univerzális sablon okosság formulával fogunk zárni: *"Tanulságnak annyit leszűrhetünk az esetből, hogy ilyesmire ne kattintson senki. Megbízható halálhíreket pedig továbbra sem a kéretlen Facebook üzenetek közt kell keresgélni."*



Ajánlott bejegyzések:

[R.I.P. Hannah Montana](#)

[Az MH17 áldozatok hamis Facebook profiljai](#)

[Chuck Norris halott, nem vicc](#)
[Közelgő Karácsony, szaporodó adathalászat](#)
[Átverés a Google spam](#)

A bejegyzés trackback címe:

http://antivirus.blog.hu/api/trackback/id/6413703

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 változtak a toplistás vírusok

2014.06.27. 10:00 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [radar május adatok 2014 nod32 havi report threat vírusstatisztika statatisztika](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. májusában a következő 10 károkozó terjedt a legnagyobb számban.



A rekkenő hőségben a mezőny teljes egésze változatlan sorrendben végzett, mindössze a számarányok tekintetében történt némi átrendeződés. **Továbbra is a mentéseket törölő Win32/Bundpil féreg vezet, amely 2013. októbertől immár nyolcadik hónapja listavezető.** Emiatt fontos teendő a saját munkák rendszeres külső adathordozóra készülő mentése. Az is lényeges, hogy ne csak egyetlen backup példánnyal, hanem párhuzamosan több különböző verziójú, mentéssel is rendelkezünk.



Állandó szereplő a listánkon a Conficker féreg és az Autorun vírus, ami a Windows XP-vel kapcsolatos felmérések fényében **nem is akkora meglepetés**, hiszen a 2001-ben megjelent operációs rendszer még mindig 25% feletti részesedést mutat a friss statisztikák szerint. Velünk maradt velünk a kilencedik helyezett Win32/TrojanDownloader.Waski is, ami egy olyan trójai letöltő program, amely egy fix listát tartalmaz URL linkekkel. Ezek alapján a HTTP protokoll segítségével próbálkozik az internetről további malware kódok letöltésével.



Az ESET Radar Report e havi kiadásában a fő hangsúlyt a frissen megjelent, továbbfejlesztett funkciókkal felruházott ESET Mobile Security legújabb, Androidos változata kapta. A mai felhasználók mindent mobil eszközeiken tárolnak, a személyes és munkahelyi adataik mellett még pénzügyi tranzakcióikat is ezeken a készülékeken keresztül intézik. Amellett, hogy egy ilyen készülék elvesztése eléggé bosszantó dolog, óriási a rizikója az adatlopásnak is. A fejlett lopásvédelmet kínáló megoldás hatékonyan segíti a készülék tulajdonosait abban, hogy minél könnyebben nyomon tudják követni ellopott vagy elhagyott mobil eszközeiket. **Ez például adott esetben akár azt is jelentheti, hogy a mobiltelefon automatikusan lefotózza a tolvajt, vagy a frissen ellopott készülék szirénázó hangot is kibocsáthat magából.** Ezenfelül a prémium előfizetőknek járó funkciók segítségével például elküldi az akkumulátorának lemerülése előtt a készülék utolsó bemért helyzetét, fényképeket készít az előlő és a hátlapi kamerával, amikor rossz PIN kóddal próbálnak belépni az eszközbe, vagy amikor változást érzékel a SIM-kártyával kapcsolatosan.



Májusi fontosabb blogposztjaink között szót ejtettünk a [május 7-én tartott World Password Day esemény kapcsán](#) arról, hogy a számtalan, az újságok címlapjára is kerülő feltörési incidens ellenére még mindig mennyire szánalmasan fantáziátlan a jelszóválasztási gyakorlat sokaknál. Pedig **a statisztikák arról árulkodnak, hogy a jelszavak 90%-a rövidege és gyengése miatt 5 percen belül a támadók kezébe juthat**, ezért érdemes alapos munkát végezni a jelszóválasztáskor - erre emlékeztet bennünket a jelszavak nemzetközi világnapja.

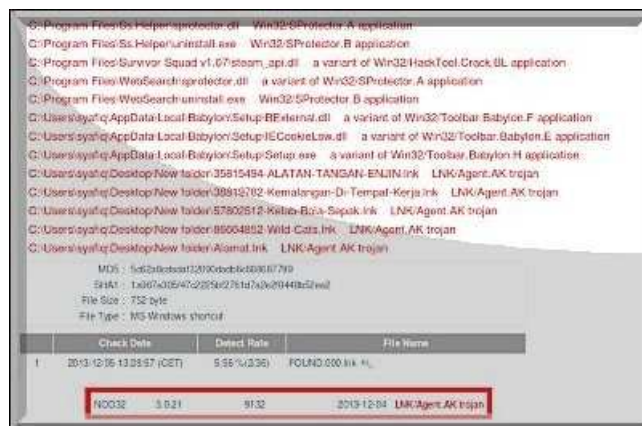


Foglalkoztunk azzal is, hogy [még mindig alábecsüljük a BYOD kockázatokat](#). Ezt tükrözte egy Gartner által végzett kutatás is, melyből az derült ki, hogy **59% azoknak az aránya, akik úgy használják munkahelyükön a mobil eszközeiket, hogy eközben céges oldalról erről semmilyen megállapodást vagy szabályozást nem írtak erről alá.** Pedig a dolgozók az okostelefonjaikat, vagy a kicsit méretesebb phabletjeiket naponta átlagosan legalább egy órán keresztül használják céges munkavégzéssel kapcsolatos tevékenységekhez.



[Megérkezett az új funkciókkal felvértezett ESET Mobile Security legfrissebb Androidos változata](#) is, és ennek kapcsán **egy látványos infografika segítségével azt jártuk körül, mit tehetünk, ha ellopják androidos telefonunkat vagy tabletünket.** A fejlett lopásvédelem számos nagyon hasznos újítással igyekszik segíteni az ilyen nehéz helyzetekben.

parancsokból kártékony célú utasítássorozatok 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. Vírusselemlők 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



03. Win32/Sality vírus

Elterjedtsége a májusi fertőzések között: 1.56%

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.



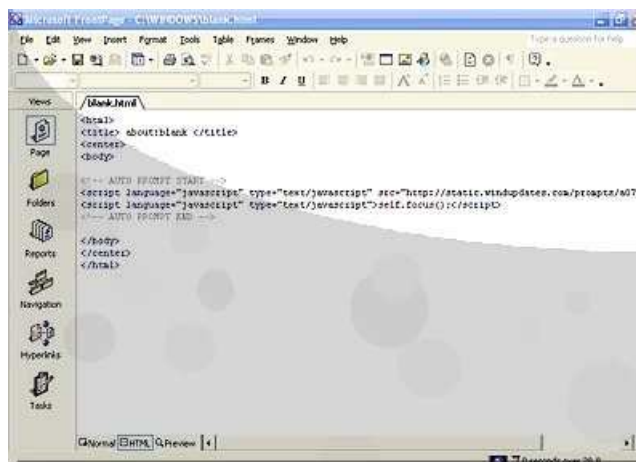
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



04. HTML/ScrInject trójai

Elterjedtsége a májusi fertőzések között: 1.49%

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.



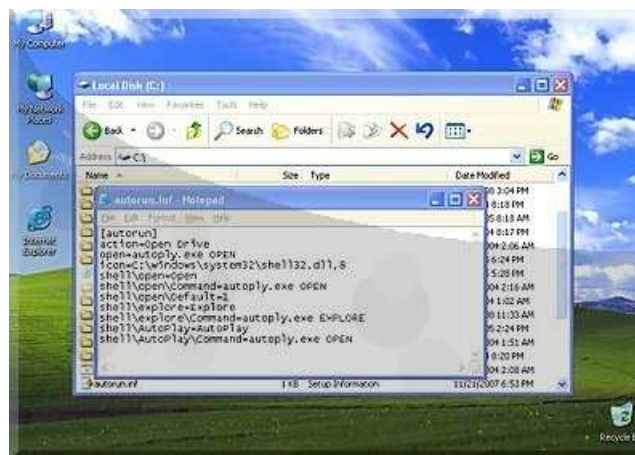
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen>



05. INF/Autorun vírus

Elterjedtsége a májusi fertőzések között: 1.47%

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



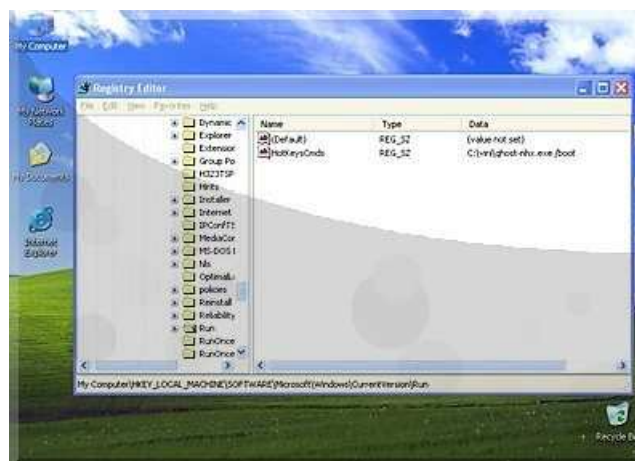
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>



06. Win32/Ohost trójai

Elterjedtsége a májusi fertőzések között: 1.37%

Működés: A Win32/Qhost trójai hátsó ajtót nyit a gépen, kiszolgáltatja annak adatait a bűnözőknek. Futása során először bemásolja magát a Windows %system32% alkönyvtárba, 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.



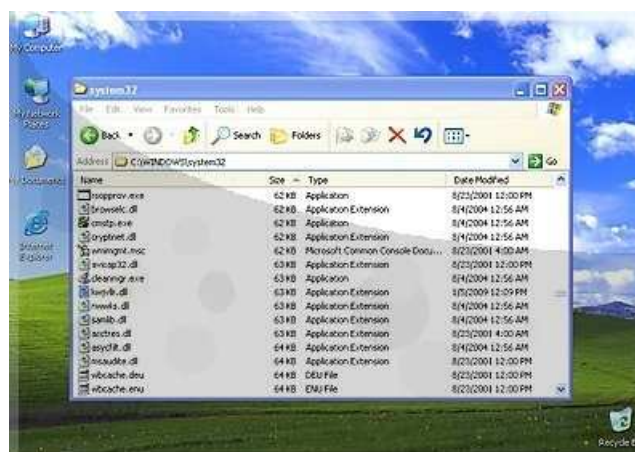
Bővebb információ: http://www.virusradar.com/en/Win32_Ohost.PEV/description



07. Win32/Conficker féreg

Elterjedtsége a májusi fertőzések között: 1.22%

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 eljáráshivással kapcsolatos sebezhetőségre építve a távoli támadó megfelelő jogosultság nélkül hajthatja végre az akcióját. A Conficker először betölt egy DLL fájlt az SVCHost eljárason keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a hosts 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 állománva miatt.

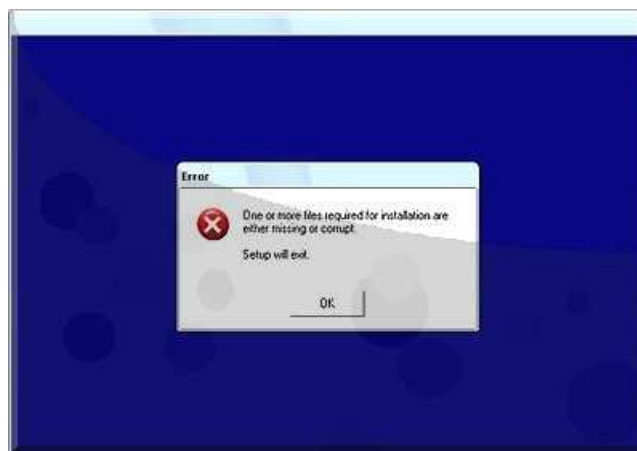




08. Win32/Ramnit vírus

Elterjedtsége a májusi fertőzések között: 1.19%

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/TrojanDownloader.Waski trójai

Elterjedtsége a májusi fertőzések között: 1.12%

Működés: A Win32/TrojanDownloader.Waski egy trójai letöltő. Egy fix listát tartalmaz URL linkekkel, ezek alapján próbálkozik. Futtatása után bemásolja magát a helyi számítógép %temp% mappájába miy.exe néven, majd további malware kódokat próbál meg letölteni az internetről a HTTP protokoll segítségével.



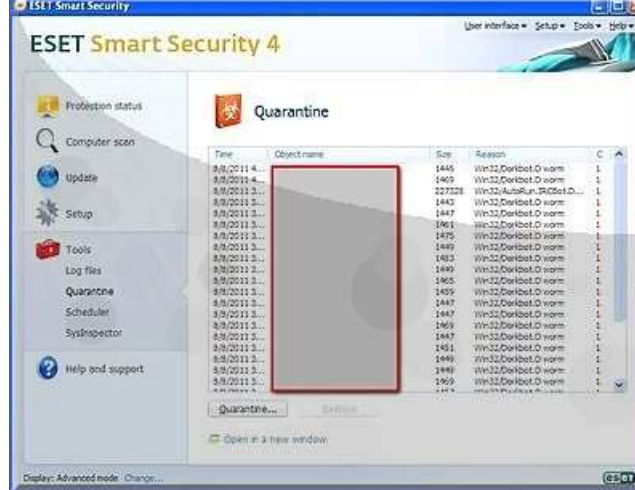
Bővebb információ: http://www.virusradar.com/en/Win32_TrojanDownloader.Waski.A/description



10. Win32/Dorkbot féreg

Elterjedtsége a májusi fertőzések között: 1.01%

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

Megosztom [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Hetedik hónapja vezet a mentéseket törölő kártevő](#)
[Megtévesztések és álhírek terepe a Facebook](#)
[Víruslista 2015. január hónap](#)
[A bank sosem hív bennünket, hogy mi a PIN kód](#)
[A HTML trójaiak riogattak minket októberben](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6423869>

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](#).

[Alick 2014.06.27. 21:45:16](#)

"az Autorun vírus"

Rendszer telepítés után az első teendőm a teljes autorun funkcionalitás letiltása.
 Válasz erre

[holex • http://fred-basset.blogspot.com 2014.06.28. 09:57:34](#)

10-ből 10 Windows-os kártevő. nem mondom, szép... azért az se jó előjel, hogy egy mobil platform-ra is megjelent a vírusírtó változata... elég félelmetesen hangzik, hogy ennyi biztonsági rés van az Androidban, hogy már vírusírtó is kell hozzá... :(
 Válasz erre

[bela a görög \(törölt\) 2014.06.28. 11:08:24](#)

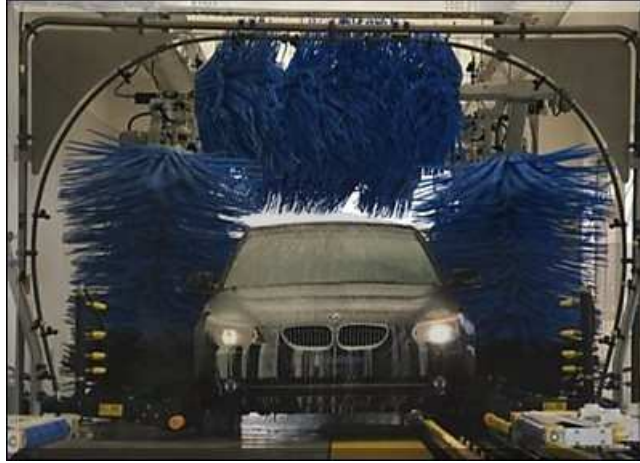
Otthon: windows - ahogy alsógatyát cserél az ember, úgy időnként formáz azt újratelepít, image-el, virtuális gépet használ - azt ha már 'sz...ros' időnként kidob. Szerintem.
 Unix - nem disznólkodásra használjuk+statisztikailag kicsi az esélye vírusra
 Cégnél: az isten pénzét kifizetik vírusírtóra meg supportra azt nem ér semmit.
 Válasz erre

Az autómosatás veszélyei :-)

2014.06.30. 13:26 | [Csizmazia Darab István \[Rambo\]](#) | [9 komment](#)

Címkék: [xp lopás](#) [csalás](#) [bankkártya](#) [bizalom](#) [adatszivárgás](#) [welivesecurity.com](#) [pcanywhere](#)

Érdekes esetre tettek nemrég pontot a nyomozók az USA-ban. Connecticut környékén ugyanis gyanúsán megszáporodtak a **bankkártya adatokkal történő visszaélések, szemlátomást rendszeresen szivárogtak az adatok valahonnan**. Az áldozatok pedig meglepve tapasztalhatták, hogy időnként a nevükben idegenek vásárolgatnak a kártyájukkal, pedig azt el sem veszítették.



Több bejelentés is érkezett a rendőrségre, ebben az állampolgárok indokolatlan levonásokra, idegen banki tranzakciókra **panaszkodtak, pedig nem is lopták el a bankkártyájukat**. Aztán a hónap elején a Massachusetts állambeli Everett-ben letartóztattak egy férfit, aki lopott hitelkártyákkal fizetett. Mint később kiderült, fizikailag nem voltak lopottak a nála lévő bankkártyák, hanem korábban illegálisan megszerzett adatok alapján elkészített másolatok voltak.

Az áttörést végül az hozta meg, hogy a nyomozás során a **hatóságok bejelentést kaptak, miszerint a Family Dollar boltokban több bankkártyát végigpróbálgatva ismeretlenek rendszeresen - heti 3-4 alkalommal - vesznek adott összegekre szóló anonim ajándék kártyákat, amelyekkel később aztán szabadon lehetett tetszőleges dolgokat vásárolni**. Ez a feltűnő viselkedés gyanús lett a rendőröknek is, emiatt aztán végignézték a biztonsági kamerák felvételeit. Bár az ilyen jellegű visszaéléseket általában Romániában, Oroszországban, vagy Ukrajnában található bűnözők követik el, ebben az esetben egy helyi afro-amerikai társaság volt a tettes. A banda túlságosan [mohó lett, és az adatok megszerzése után túl hamar és túl gyakran](#) igyekeztek pénzt szerezni.



Brian Krebs blogja szerint végül sikerült utánajárnia a dolognak, így derült ki, hogy **azok voltak a kárvalottak, akik Connecticut környékén a Key Road Car Wash nevű autómosókban jártak**. Jellegzetesen feltűnő módon ugyanis a kártyatulajdonosok pénze nem sokkal az autómosások után fogyatkozott meg, sőt volt olyan is köztük, akivel ez többször is előfordult. Ráadásul a sofőrök egyáltalán nem is veszítették el a bankkártyájukat. A több tucat mosót érintő csalásban a **POS terminálokat a távoli hozzáférést biztosító pcAnywhere programmal figyelte meg a támadó**, aki aztán az ellopott hitelkártya adatok segítségével klónoztatta is a kártyákat, ezekkel történtek később az illegális vásárlások. A legalább 40 autómosót érintő csalássorozatban számtalan visszaélést követtek el így 2014-ben.

Location	City	State
EXPRESS SYSTEMS	HENAGAR	AL
SCRUBBS	CHICO	CA
MATT AND JEFF'S CAR	NOVATO	CA
CHECKERED FLAG HAND		
CARWA	IRVINE	CA
Desert Express	La Quinta	CA
Atlas Car Wash	Brighton	CO
SPLASH Bridgeport	Bridgeport	CT
SPLASH FAIRFIELD	FAIRFIELD	CT
SPLASH GREENWICH	GREENWICH	CT
SPLASH SHELTON	SHELTON	CT
MARINER CAR WASH	ST PETERSBURG	FL
Express Car Wash	Franklin	TN
Legends	Wichita	KS
Paradise Bay	Kansas City	KS
Classic Auto Spa	Lafayette	LA
Dons Car Wash	Lake Charles	LA
SHIELD SYSTEM CARWASH	WINCHESTER	MA
SHIELD SYSTEM CARWASH	BILLERICA	MA
Auto Spa	North Andover	MA
Flagship Car Wash	Rockville	MD
Key Road Car Wash	Keene	NH
BLUE WAVE CAR WASH & Q	BARNEGAT	NJ
SPOTLESS AUTO LAUNDRIE	HACKENSACK	NJ
PERSONAL TOUCH CAR WAS	EAST	
Broadway Minute	NORTHPORT	NY
AMERICAN CAR WASH	Newburgh	NY
MAGIC SUDS CAR WASH	ROSLYN	NY
Dynamite Auto Wash #1	LEESPORT	PA
THE CAR WASH	Mount Pocono	PA
Quick Quack	DICKINSON	TX
Waterworks	Tomball	TX
Waterworks	San Antonio	TX
Mister Car Wash (2 locations)	San Antonio	TX
VIGGY WASH	Houston	TX
SUPERSONIC CARWASH	SPANISH FORK	UT
	SALT LAKE CIT	UT

[A dolgokat némileg bonyolította, hogy 2012-ben a Symantec elismerte, ismeretlenek ellopták a pcAnywhere program forráskódját](#), és ezzel összefüggésben kihasználható sebezhetőségekre is fény derült. Emiatt a biztonsági cég figyelmeztette is ügyfeleit, hogy frissítsenek a szoftver újabb, a kritikus hibákat már befoltozott újabb verziójára. **Ez a biztonsági update azonban sok helyütt egyáltalán nem lett elvégezve, itt az autómosókban sem.** Így történhetett meg azok távoli kompromittálása és kihasználása.

Szakértők mindemellett megjegyzik, **egyáltalán nem javasolt távoli felügyeleti program telepítése POS terminálos számítógépre, hiszen itt kiemelten kritikus érzékeny adatok kezelése történik.** Emellett az üzletek egy részében nem csak hogy a régi alapértelmezett jelszavakkal használták a pcAnywhere szoftvert, hanem **ráadásul még az elavult és emiatt kiemelten támadható Windows XP környezetben futott.**



Olvasóink megszokhatták, hogy a végére igyekszünk tanulságokkal szolgálni, illetve tanácsokat adni. **Elkerülve a sablonos és túlságosan szimpla "mostantól mindenki maga mossa le otthon a kocsiját"** kijelentés helyett ;-)) inkább azt tartjuk fontosnak megjegyezni, hogy a vásárlás, illetve a kártyával fizetés egyfajta bizalmi kérdés, legalábbis nálunk Magyarországon mindenképpen könnyen megválogathatjuk, hol használjuk és hol fizetünk inkább készpénzzel. Ha tehetjük, még otthon se használjunk már XP-t, de vállalati környezetben, vállalkozásunkban ez még inkább kerülendő. És persze a banki tranzakcióink rendszeres ellenőrzése is javasolt, kérjünk azonnali SMS értesítést a számlamozgásokról, így a legkisebb gyanús tétel esetében is azonnal tudunk intézkedni a bankunknál. Emellett pedig a szoftver frissítéseket se hanyagoljuk el!

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

- [Valentin nap: Szerelem helyett átverés érkezik](#)
- [Egészségügyi adatokat loptak az USA-ban](#)
- [Munkavállalói adatok szivárogtak az Nvidiatól](#)
- [Mi az, ami tízszer annyit ér, mint a bankkártya adat?](#)
- [Az MH17 áldozatok hamis Facebook profiljai](#)

Hirdetés

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6457333>

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](#).

[gigabursch 2014.07.01. 06:53:59](#)

Hú,de utúlom, amikor úgy kell fizetnem, hogy be kell hajoljak a pénztárosnő üléebe, mert nem képes azt a nyavalyás terminált kiadni, hogy beüthessem a pinkódomat.

De teszek rájuk, meg a sirámaikra, akkor is letakarom.

Válasz erre

[☞batyu☞ 2014.07.01. 09:05:15](#)

"Bár az ilyen jellegű visszaéléseket általában Romániában, Oroszországban, vagy Ukrajnában található bűnözők követik el, ebben az esetben egy helyi afro-amerikai társaság volt a tettes."

Cigányok és négerek. Nincs "véletlen" rasszizmus.

Válasz erre

[Dr_utcai_arcos 2014.07.01. 09:06:49](#)

Those goddam ni..colors!

Válasz erre

[cenzuratroll bosszanto 2014.07.01. 09:13:49](#)

Hogyan függ össze a bankolás és az XP? Ennyire nem kéne paranoiásnak lenni, ha winfos 7-8-at, akármit használok, attól még a banki rendszer felépítése a lényeges, nem az, hogy miről indítottam a bejelentkezést.

Válasz erre

[☞batyu☞ 2014.07.01. 09:43:20](#)

[@cenzuratroll bosszanto](#): Úgy, hogy te a banki rendszeredet egy böngészőn, (ez az esetek jó részében ez Explorer) keresztül használod. Az pedig a nagy átlagnál Windows alatt fut. Újabb verziókon elvileg kisebb az esélye a támadásoknak, hiszen a régi lyukakat ott már bestoppolták.

Válasz erre

[teddybear01 2014.07.01. 10:18:22](#)

Ezért kell inkább készpénzzel fizetni. Azt is lemásolják néha, de az már nem az én zsebemből megy.

Válasz erre

[fifibá55 2014.07.01. 10:27:25](#)

Ugyan nem kapcsolódik szorosan az antivírus bloghoz, azért itt is leírok egy újabb, számomra eddig ismeretlen módszert: fizetéskor a bankkártyát az élénk helyezett terminálba függőlegesen kell bedugni, a csippel felénk, és úgy kell a PIN-t beadni. Utóbbi eltakartan elvégezhető, nem is abban van a turpisság, hanem abban, hogy közben egy rejtett vagy akár nem is rejtett kamera pl. a pult mögött veszi a kártya hátsó, mágnescsíkos oldalát, és különösen a szép fehér háttérre jó kontrasztosan rányomtatott 3 jegyű CVV kódot. Mivel a kártyaszám a tranzakcióból ismert, a két adat birtokában simán tudnak internetes vásárlásokat bonyolítani; munkatársam kártyaadataival Bulgáriában vásároltak így nagy LED-TV-t.

Kivédeni pl. úgy lehet, hogy a kódot szígszalaggal leragasztjuk, az a használatot nem zavarja.

Válasz erre

Január Herceg (2014) 2014.07.01. 11:12:03

[@teddybear01](#):

Igen, így van. A Missouri-i útszéli csehóban, meg az Ann Arbor-i kocsimosóban értelemszerűen nem adom oda a kártyámat. De az igazság az, hogy el is kerülöm ezeket a helyeket.

Válasz erre



sokasebi • <http://pacifictime.blog.hu/> 2014.07.01. 11:27:33

Az Usa-ban az ettermekben mindenhol úgy kell fizetni, hogy elviszik a kártyadat. A hatan meg persze ott van a CVV kod. Szerintem Nem is kell Windows a masolasahoz.

Válasz erre

Eljárás indult a T-Mobile ellen Amerikában

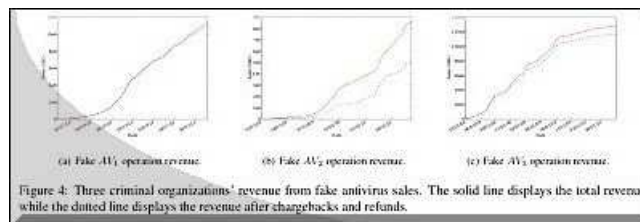
2014.07.02. 17:29 | [Csizmazia Darab István \[Rambo\]](#) | [2 komment](#)

Címkék: [usa](#) [t-mobile](#) [sms](#) [csalás](#) [átverés](#) [ftc](#) [emelt díjas](#)

Mielőtt még valaki azt mondaná, ááá Amerika messze van, és különben is, kit érdekel ez az egész, érdemes tisztázni, hogy egyfelől az U.S. Federal Trade Commission (FTC) indította az eljárást. Másfelől pedig **a vizsgálódás tárgya annak tisztázása, vajon felelős-e a T-Mobile azért, mert olyan emelt díjas SMS szolgáltatások után is szed be pénzt az előfizetőitől, amiket egyértelműen csalók üzemeltetnek.**

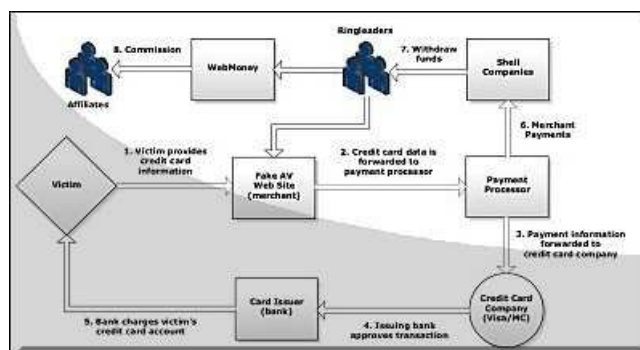


Mielőtt túlságosan gyorsan felületes véleményt mondanánk az ügyről, révedjünk picit a múltba. Anélkül, hogy olyan logikai fogós ravasz keresztkérdéseket is tartalmazó bulváros mélységekbe bocsátkoznánk, hogy ha egy magyar vállalkozás a Google Adwords-ben hirdet, kell-e neki reklámadót fizetni vagy sem, és hasonló, helyette nézzük meg, hogy annak idején **hogyan merült fel egy nagyon hasonló kontextusban a felelősség kérdése egy másik lehűzős átverésnél. A hamis antivírusokról van szó, amely nagyon is jövedelmező üzletág, hiszen hogy csak saját egyik korábbi posztunkat idézzük, már a 2008-as kezdeteknél is 32 millió forintot hozott a bűnözőknek - hetente.**



Ám ami még érdekesebb, és mostani témánk szemszögéből releváns, az az a tény volt, amit **Brian Krebs** pedzegetett a blogjában. Nevezetesen **hogy egyes kétes hírű fizetesközvetítők, illetve a talán szándékosan nem elég szigorú bankok szemet hunynak a gyanús tranzakciók felett.** Elvileg a fizetesközvetítő cégek éberren figyelnek arra, ha valaki elégedetlen a vásárolt áruval, akkor a szerződő partnerek biztosítsák a pénz-visszafizetési garanciát, ellenkező esetben gyanússá válhatnak, illetve a fizetesközvetítő (pl. PayPal, AlertPay, ChronoPay, stb.) ideiglenesen vagy véglegesen kitiltja őket, és akkor ezzel elzárja a pénzcspot. De szintén elvileg azt is figyelik, ha valahol pedig túl nagy számban történik pénzvisszafizetés, akkor ott valószínűleg kétes üzelmek zajlanak.

Krebs úgy látja, egyes bankok és a fizetesközvetítő cégek pontosan tudják ugyan, hogy mi is történik valójában, ám mivel közvetlen hasznuk származik belőle, nem tesznek ellene az égvilágon semmit. A csalók pedig több számlát használva, vagy ezek rendszeres, például havi csereberekével is operálnak. A biztonsági kutatók szerint **a VISA és a Mastercard rendszerében elvileg létezhetne valamiféle megoldás, hogy a gyanús folyamatokat, cégeket, tevékenységeket hatékonyabban kiszűrjék, ha nagyon akarnák.**



És most lássuk a mai hírt, miszerint [az amerikai Szövetségi Kereskedelmi Bizottság \(FTC\) eljárást indított a T-Mobile ellen, mert szerintük a T-Mobile olyan emelt díjas SMS szolgáltatások után is szed be pénzt előfizetőitől, amelyeket csalók üzemeltetnek](#), és vélelmezhetően nem a tőlük elvárható legnagyobb gondossággal védik ebben az előfizetők érdekeit. A T-Mobile szerint a vádak teljességgel alaptalanok, és arra hivatkoznak, hogy bár kétes megítélésű emelt díjas SMS-ekkel foglalkozó vállalkozások ugyan tényleg vannak, de ez a

probléma nem csak őket, hanem az összes többi mobilos szolgáltatót is érinti, és azzal védekeznek, miért nem panaszkodnak minden egyes esetben a fogyasztók. A benyújtott panasz szerint azonban a T-Mobile-nak gigászi mértékű, több száz millió dolláros haszna származik a kamu horoszkópos, flörtölős és egyéb, jellemzően havi 9.99 dollárba kerülő "szolgáltatások" után. Az ilyen becsapáson alapuló SMS üzenetekről leiratkozni a legtöbb esetben rettentő körülményes, vagy akár szinte lehetetlen. Mi is beszámoltunk már például olyan, magyar nyelven is elérhető kamu antivírusról, amely [az áldozatnak egy óvatlan kattintás után 15 euróba, azaz nagyjából 4600 forintjába fog kerülni HETENTE](#).



Ma már [az emelt díjas átverések nagyon komoly szeletet hasítanak ki](#) a mobilos trójak esetében. Ez a fajta csalás igen népszerű mind Európában, mind pedig Ázsiában, aminek az is oka lehet, hogy a mobiltelefon társaságok általában rövid átfutási idő alatt végzik a kifizetések feldolgozását, így a bűnözők lényegében könnyen és gyorsan a pénzükhöz jutnak. [Mire pedig az előfizetők később kézhez kapják az aktuális telefonszámláikat](#), addigra a rossz fiúk már régén messze járnak, és a következő hasonló típusú csalást készítik elő.



A vicces az, hogy már 2010-ben világosan kiderült, a T-Mobile-nál igenis [olvassák, illetve ellenőrzik az SMS üzeneteinket, vagyis mindenféle külön értesítés, jelzés nélkül törölhetnek a szöveges üzenetek közül](#), amiről a küldő fél sokszor egyáltalán nem is szerez tudomást. Sőt, ebben az eljárásban indoklás és fellebbezés sincs. Szóval technikailag nyilván nem lenne lehetetlen a Brian Krebs féle elvek mentén jobban figyelniük és kontroll alatt tartani a kétes vállalkozások SMS-sel kapcsolatos ténykedését, jellemző mintákat figyelniük. Sőt mondhatni, a felhasználók védelme érdekében ez egyenesen kívánatos lenne - [valószínűleg erről is szólhat az FTC mostani eljárása](#).

Mindenesetre a vizsgálat végeredményét még megsaccolni sem tudjuk, hiszen Amerika messze van, és lehet ugyan, hogy álmainkban visszainteget, de azt néha a középso ujjával teszi :-). A korábbi perek, vizsgálatok eredményeiből időnként remekül látható, hogy az ottani döntéshozók ítélete nem mindig az általunk elgondolt hagyományos európai igazságérzet diktálta nyomvonal mentén születik, de **azért reméljük, lesz ebben is előrelépés.**

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Valentin nap: Szerelem helyett átverés érkezh](#)
[Csaláselehárítás fordított képkereséssel](#)
[Az MH17 áldozatok hamis Facebook profiljai](#)
[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Ismét nyertünk 450.000 eurót :-\)](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6468297>

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](#).

Gusztly 2014.07.03. 12:37:40

Jó lenne, ha a T. blogger eldöntené, hogy az a jó, ha szűr SMS-eket a szolgáltató vagy nem, mert így csak a "van rajta sapka, nincs rajta sapka" esete forog fent. Perszer ha a blogot a Telenor vagy a Vodafone szponzorálja, akkor nem szóltam :-)
Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu> **2014.07.04. 14:05:15**

Hello Guszty!

A blogot nem szponzorálja sem a Telenor, sem a Vodafone, pedig hideg jégkockás védőitalokat és egy nyitható tetejű autót hozhatnának már végre ;-)

Itt a korábbi beleolvasós résznél nagyobb a probléma annál, mint hogy például a Google is automatikusan beleolvas a levelekbe, de legalább nem törölget közülük minden értesítés nélkül (csak elküldi az érdekesebbeket az NSA-nak, muhahaha). Szerintem ez a legnagyobb gáz ebben a korábbi cenzúrázósdi történetben.

De mindez csak azért szerepelt a példában, hogy technikailag igazából semmi nem akadályozná meg őket abban, hogy hatékonyabban szűrjék ki lehúzó brigádokat, csak valószínűleg úgy kevesebb csörögne a kassza. De majd az FTC vizsgálat és az esetlegesen kirótt bírság után hátha "megjön" a kedvük hozzá ;-)

Válasz erre

Ismét nyertünk 450,000 eurót :-)

2014.07.04. 13:54 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam ingyen spanyol lottó e-mail csalás átverés nyeremény](#)

Ha valaki valamilyen fatális tévedés folytán azt gondolta volna, hogy a gyalázatos magyar helyesírású, bikkfanyelvű átverős e-mailek kora 2014-ben esetleg már lejárt volna, azt ezennel ki kell ábrándítsuk.



Régi olvasóinknak ismerős lehet ez, hiszen [már 2009. februárban is nyertünk a lottón](#), és aztán rögtön [júliusban ismét leakaszthassuk a gigantikus lottónyereményt](#), végül megkoronáztuk mindezt 2012-ben azzal, hogy [miénk lehessen egy vadonatúj, kártyafüggetlen Samsung Galaxy S II okostelefon](#). Szóval az átverési próbálkozások már évek óta folynak.

A magyar nyelv ellen elkövetett helyesírási merényleteket pedig [főként korábbi bankok elleni adathalász kísérletekből](#), illetve a kéretlen üzleti ajánlatokból ismerhetjük. A gyaníthatóan automatikus fordítás eredményeképpen Tuskó Hopkins, Csülök, Török Szultán és Fülíg Jimmy helyesírási stílusában kaphattunk hírt arról, hogy "Megvan a hivatkozást a keresési valaki, aki megfelel az én javasolt üzleti kapcsolatot bele oda neki." De [mély nyomokat hagyhatott az olvasóközönségben Patrick Chan ügyvezető igazgató](#) üzenete is, miszerint: "Miután az alapokat már sikeresen át a fiók, akkor a részesedése az arány jóvá kell hagynia mind a ketten. Én inkább el nem éri meg az én privát e-mail címét".



Mai levelünk ismét lottó nyerésről tájékoztat, ami mindenképpen pozitív, hiszen nyakunkon a hétvége, meg itt a nyaralási szezon is, és a 450 ezer euróból legalább esélyünk lesz valamilyen all inclusive ellátással bíró egzotikus szigetre utazni :-). Gratulálunk nekünk 450.000.00 euróhoz, amelyet a nemzetközi e-mail lottó díjjal nyertünk, és a nagyobb hitelesség kedvéért "valódi" referencia száma is találunk benne: "Ref: ES/9420X2/68". A kapcsolatfelvételhez pedig semmi mást nem kell tenni, mint hogy megfogadjuk az utasítást "Az egyértelműség és az eljárás Kapcsolat: STALLION MEGA IGENY AGENCY Mr. Juan Carlos". Nem hiányzik belőle a szokásos sürgetési formula sem, ami azért kell, hogy ne gondolkozzon sokat az címzett, hanem kattintson gyorsan MOST, és válaszoljon azonnal mellékelve a teljes nevet, lakcímet, életkort, foglalkozást, és telefonszámokat. Emiatt lett odabiggyesztve a legelejére, hogy "utolsó értesítést".

Bár a látszólagos feladó egy magyar webtárhelyszolgáltató domainjét mutatja, az üzenethez mellékeltek ezenkívül még egy spanyolországi (34) előhívóval rendelkező telefonszámot is, amelyen nyilvánvalóan Juan Carlos barátunk egyedül csak a mi hívásunkat várja türelmetlenül két bikaviadal és egy pohár Sangria között.



Összefoglalva: nem és nem, sírjunk együtt, de [Bill Gates még mindig nem osztja szét vagyonát](#) a közönséges földi halandók közt, és [sajnos az e-mail címünkkel kihúzott ingyen lottós állítólagos nyereményből sem fogunk](#) életünk szekerén jelentőset fordítani a könnyed és gazdag életstílus irányába - ez van. [Remélhetőleg már mindenki higgadtan kezeli a hasonló kéretlen e-mail üzenetben érkező jó híreket](#), és nemcsak a szövegben elkövetett fajsúlyos magyartalanságok, hanem sokkal inkább a hihetatlensége és átverésnyanus tematikája miatt nem hisz el mindent, és törli ki azonnal válasz nélkül az ilyeneket.

 Tetszik Regisztrájl, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Itt a foci VB, jönnek az átverések is](#)
[Az ön e-mailcíme nyert...](#)
[Csaláselhárítás fordított képerkeséssel](#)
[Hogyan NEM nyerünk majd iPhone 6-ot?](#)
[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6473051>

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.

Biztonsági tanácsok kis cégeknek

2014.07.07. 13:37 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [kis vállalkozás](#) [kkv cégek](#) [alvállalkozó](#) [beszállító](#) [kibertámadás](#)

Aki azt gondolja, támadások csak a kiemelt és jelentős pénzügyi forgalmat is bonyolító nagyvállalatok ellen történnek, az súlyosan téved. A kiberveszélyekkel kapcsolatban mindenképpen ki kell hangsúlyozni, hogy ez **minden egyes kis és közepes vállalat, vállalkozás szempontjából is fontos és kritikus terület**, hiszen a kiemelt célpontok elleni kibertámadások esetében először ugródeszkaként célzottan sokszor a gyengébben védett beszállítói kört, és az alvállalkozókat támadják.



Teszik mindezt abban a reményben, hogy a hiányzó, kiszervezett vagy kisebb létszámú, leterhelt IT miatt őket könnyebb elsőként feltörni vagy kémprogrammal megfertőzni, majd innen lépnek tovább a bűnözők a multik, bankok vagy más kritikus infrastruktúrák irányába. Emiatt ez minden egyes vállalkozásnak kihívást jelent, hiszen mindenki dolgozik valakinek, végez munkát külső megbízásokból.

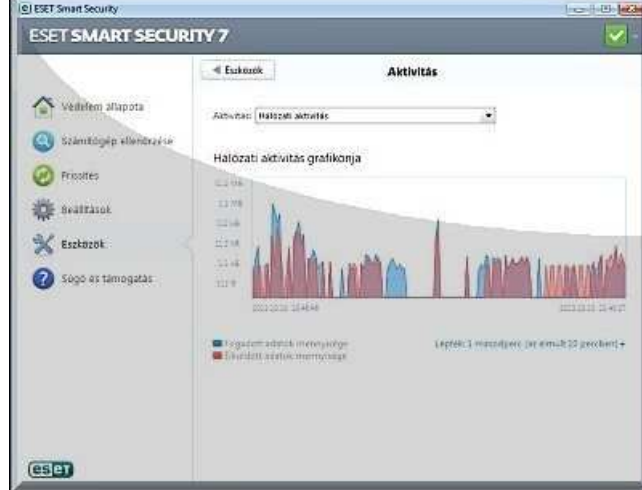
De azt is érdemes megemlíteni, hogy **téves az a hiedelem, hogy rám úgysem céloznak, mert ez bárkit elérhet, hiszen legtöbbször automata scriptek kutatnak sebezhető gépek után, és akár a NASA beszállítója, akár csak hímzésmintákat árusít, ha sérülékeny, akkor ezen keresztül megfertőzik**. Ilyen körülmények között fontos, hogy a lehetőségekhez képest a kisvállalkozások ne kövessenek el elemi biztonsági hibákat. Összefoglalónkban **pár egyszerű hasznos tanácsot** igyekszünk ehhez adni.



Legyen antivírus, de ez önmagában nem elég

A vírusirtó valóban nélkülözhetetlenül fontos, ám tudni kell, hogy 100 százalékos védelem nem létezik, így esetleg még az is megfertőződhet, aki naprakész védelmi programokat használ. Az sem igaz, hogy a vírusirtó csak és kizárólag a már ismert kártevőket ismerné fel, hiszen sok egyéb módszer: heurisztika, URL blokkolás, script elemzés, tűzfal, stb. biztosítja, hogy a még ismeretlen kártevők, variánsok is fennakadjanak az ellenőrzésen. Fontos viszont, hogy **a védendő értékeink függvényében költsünk a biztonságra**, így tűzfalra, behatolásvédelemre, sőt akár UTM megoldásra is. Ide tartozik még **a rendszeres frissítés** témája is, mivel a kártevők döntp többsége a frissítetlen rendszereket veszi célba.

Emellett azonban ha például [gondosan kiválasztott programjaink, eszközeink mellé harmatgyenge, netán mindenhol azonos jelszavakat választunk, úgy ezzel durván meggyengítjük](#) a védelmünket. Jelszavakról még lesz szó a későbbiekben is, de emellett **még a mentés is egy kiemelten kulcsfontosságú tényező a biztonság tekintetében**. Nem egy olyan magyar cég volt már például, amelyik a saját szerverén vesztette el az összes munkáját az adatokat 2048, 4096 bites egyedi RSA kulccsal titkosító CryptoLocker miatt, és elrettentő módon semmilyen mentésük sem volt.



Félelem a bonyolult jelszavak elfelejtésétől

A jelszó menedzserek hatékonyan segíthetnek ezek megjegyzésben, ilyen lehetőség például a LastPass, KeePass és hasonló alkalmazások. Vagyis szándékosan inkább ne butítsuk, ne gyengítsük, legyen az csak minimum 10-15 karakter hosszú, sose legyen egyszerű szótári szó, időközönként indok nélkül is rendszeresen cseréljük le, semmiképpen ne használjuk ugyanazt több helyen is, és a jelszó emlékeztető sose maga a jelszavunk legyen!

A gyenge jelszó választása komoly hiba, ehhez elég olyan dolgokat említeni, mint hogy számos vírus - köztük például a már 7 éve toplistás Conficker féreg - egyik terjedési módja is épít erre, hiszen szótáralapú támadást is indít a gyenge adminisztrátori jelszavak ellen. Így a fertőzés következményeinek kivédésében itt is nagy szerep jut az erős jelszavak használatának. Ahogy pedig a <http://passwordday.org/en/> oldal is mutatja, a jelszavak 90%-a rövidsége és gyengesége miatt 5 percen belül a támadók kezébe jut



A másnak is odaadott jelszó nem jó jelszó.

A jelszó esetében még egy fontos momentum van, sose adjuk oda másnak. Általános esetben minden egyes munkatársnak saját belépése van, többek közt ezzel lehet később azonosítani, ha valakinél valamilyen rendkívüli esemény történik. Ám ha dolgozók egymás kódjával összevissza lépkednek be, nem zárolják a gépeiket, úgy követhetetlen lesz, hogy pontosan mikor ki dolgozott a számítógépeken. Emellett az ilyen közösen használt gépeken nagyobb a social engineering, azaz megtévesztés alapú támadások lehetősége is, hiszen ha valaki a másik felhasználóra hivatkozva telefonál, nehezebb eldönteni, vajon jogosan érdeklődik, vagy éppen adatokat akar belőlünk kicsalni.

Arról nem is beszélve, hogy az egyéni jelszó mellett arról is gondoskodik, hogy az adott dolgozónak munkakörre szabottan mihez legyen hozzáférése, így ezek keverése, közös használata is potenciális veszélyforrás például az adatszivárgásra. A hozzáférések elkészítésénél pedig a teljesen egyedi jelszavak választása mellett az a legjobb módszer, ha csak a minimálisan szükséges elérési szintet engedélyezi a rendszergazda.



Ha magyar adatokat nézünk, akkor azt látni [egy 2014-es kutatás szerint, hogy sajnos alulértékeli a kiberbűnözés veszélyeit a hazai vállalatok többsége](#). A megkérdezettek csupán 35% tartja kockázatosnak ezt a fajta fenyegetést saját vállalatára nézve. Közép-Kelet-Európában ez az arány átlagban 45%, míg a nyugat-európai országokban a válaszadók 50%-a aggódik és tartja veszélyesnek.

A rengeteg támadás és rengeteg sebezhetőség miatt nem szabad a veszélyt tévesen le- vagy alábecsülni olyan közkeletű hamis vélekedések miatt, mint "ez egy kis ország, nem Amerika".

 Tetszik [Regisztrálg](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A brit felnőttek hatoda volt már kiberáldozat](#)
[A legnépszerűbb hobbi](#)
[Kicsi fej jobb ide, mint a nagy](#)
[Valóban kicsi az új Norton ISecurity telepítője?](#)
[Captcha törés ipari méretekben](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6481849>

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 meghackelt villanykörte esete

2014.07.09. 11:24 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [wifi dolgok](#) [okostelefon](#) [kártevő](#) [sebezhetőség](#) [izzó](#) [internete](#) [context](#) [lifx](#)

Pár éve egy ilyen cím olvastán még biztosan kényszerzubbonyért kiáltottak volna, de manapság, amikor a dolgok internete ontja magából a furcsábbnál furcsább biztonsági incidenseket, ez már belesimul a "normális" technológia hírek sodrába. **Hűtőszekrényekből álló botnet spammelt? Ne már!** Azonban jó ha tudjuk, ez egyáltalán [nem fikció, hanem valóban megtörtént](#).



Most pedig **az okostelefonról szabályozható izzóról** derült ki az, hogy a felkészült támadók számára kihasználható kritikus hibát tartalmaz. Ezúttal a Context Information Security fedezte fel, hogy a 2012-ben Kickstarteres startup céggént debütáló LIFX nevű cég okostelefonnal vezérelhető LED-es izzói tartalmaznak sérülékenységet. A kutatók képesek voltak arra, hogy [megfigyelve az izzók közötti kódolt WiFi kommunikációt visszafejtsék a titkosítást](#).

Ennek segítségével aztán később üzenet csomagokat tudtak nemcsak elfogni, vagy blokkolni, hanem **saját üzenetsomagokat is be tudtak injektálni a rendszerbe, ezáltal pedig a beállításokat saját hatáskörben tetszés szerint úgy megváltoztatni, hogy ahhoz semmilyen előzetes hitelesítés nem kellett, illetve ezekről a manipulációkról semmilyen riasztás, figyelmeztetés nem keletkezett**. Ez persze nem lehet nagy újdonság annak, aki látta [Charlie Miller tavalyi autóhackelésről szóló előadását](#) a MOM kultúrházban :-). A gyártó most a Context szakembereivel együttműködve közösen adott ki egy új firmware változatot, amely bezárja ezt a sebezhetőséget.



Aki mint felhasználó az elsők közt vesz és használ okos hűtőt, okos autót, okos légzésfigyelő babamonitor, okos ház riasztót vagy okos televíziót, az jobb, ha lelkiében felkészül arra, hogy az Internet of Things (IoT) egyáltalán nem bombabiztosan védett technológia, és számos váratlan meglepetéssel tud majd szolgálni.

Ehhez elég, ha csak [tavaly az LG felhasználói szokások után kémkedő](#) és tesztezálló reklámokat sugárzó televíziójára gondolunk, ahol [még az USB-n keresztül csatlakoztatott külső lemezen található videók fájlneveit is továbbította](#) a rejtett - persze kizárólag csak a mi érdekünkben tevékenykedő :-)- funkció, amely ráadásul titkosítatlan hálózati adatforgalomként utazott a neten.



Az mindenesetre jól látszik, hogy a rengeteg technikai újdonság nem csak jelentősen megkönnyítheti sokak életét, hanem még igen sok munkát fog adni a biztonsági szakmának, és a jövőben még sok ilyen furcsa bulváros hírről olvashatunk majd.

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Kamu Android app hajt a pénzünkre](#)

[Frissítsünk-e hotelben?](#)

[Újra itt a CryptoWall zsaroló kártevő](#)

[Véddj a CryptoLocker terjesztőjének fejére](#)

[Biztonsági konferencia - nyitott wifi honeypot-tal](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6487349>

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 Darab István \[Rambo\]](#) • <http://antivirus.blog.hu>
2014.07.10. 06:17:52**

"While the bulbs used the Advanced Encryption Standard (AES) to encrypt the passwords, the underlying pre-shared key never changed, making it easy for the attacker to decipher the payload."

Válasz erre

Megtalálták az eltűnt maláj repülőt! Ismét :-)

2014.07.11. 12:35 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam facebook](#) [csalás átverés](#) [kérdőív survey](#) [repülőgép](#) [maláj](#) [utasszállító](#) [welivesecurity.com](#)

Az előző, 2014. márciusi posztunkra utalva, újra érkeznek a Facebookon azok a hamis posztok, amelyek az eltűnt maláj utasszállító repülőgép állítólagos megtalálásáról szólnak. Egy igazi izgalmas téma, izgatja az emberek fantáziáját, és jól láthatóan akárhányszor, ismétlődő ciklusokban is át lehet vele verni az embereket.

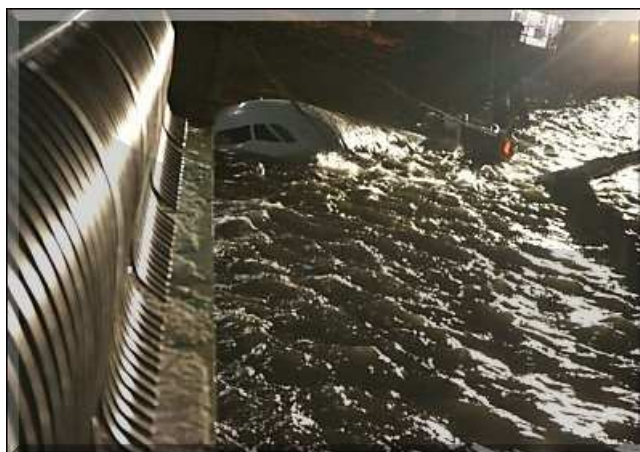


Kezdjük azzal, hogy [a múltkori márciusi hamis hírnél az volt a lényeg](#), hogy az akkori ígért mozi helyett egy hibáüzenet jelent meg állítólagos korhatáros YouTube videóra hivatkozva - ilyen egyébként nincs is - és előtte/helyette ezért egy mellékelt tesztet kellett volna elvégezni, mellyel még állítólag iPhone 5S okostelefont is nyerhettünk. Természetesen csak a kattintásainkra vadásztak az elkövetők, az adott oldal látogatóinak, illetve a tesztet kitöltők után ugyanis pénzt fizetnek nekik.



Ezúttal ismét felélesztették a sztorit - ebben felfedezhető valamiféle rendszeres ciklikusság is, némi pihentetés után minden elő lehet venni, csak egy újabb csavarást kell illeszteni a történetbe. Ez pedig jelen esetben nem más, mint hogy [egyrészt már eltelt 4 hónap a rejtélyes eltűnés óta, másrészt az a matróz, aki megtalálta, azonnal kapott 5 millió dollárt](#). "Malaysian Air Flight MH370 Found By Sailor Moments Ago: Mystery Solved - Sailor Awarded \$5 Million on spot." Na ugye, hogy máris érdekesebb lett!

A képen viszont nem a maláj járat, hanem egy még 2009-ben a New York-i Hudson folyóba zuhant US Airways Flight 1549 látszik (Trau barátom, erősíts meg! :-)



A mostani "Breaking News" típusú átverés célja teljesen hasonló a korábbi, szokásos esetekkel. Felmérések, kérdőívek várnak ránk végül a videó helyett, némelyik még a mobil telefonszámunkra is kíváncsi, illetve nem ritkán még valamilyen emelt díjas szolgáltatásra is megpróbálják felírni az embert valamilyen trükkkel - például SMS-ben kell jelentkezni az állítólagos nyereményért.

Mindenki, aki az ilyet nem csak elhiszi, hanem sajnálatos módon a Facebookon még tovább is osztja az ismerőseinek, az növeli a potenciális áldozatok lehetséges számát.



Befejezésül megismételjük a múltkor már frappánsan összefoglalt, védekezéshez illetve megelőzéshez szükséges tudnivalókat. **Hasznos lehet ezzel kapcsolatosan feleleveníteni néhány ezzel kapcsolatos korábbi biztonsági tippünket. Eszerint sose higgyük el, ha egy kéretlen link valami meghökkentőt ígér! Ne dőljünk be, bármit is ígérnek egy lájkért, és látatlanban előre ne lájkoljunk, ne osszunk meg semmit! Ha bármit telepítenünk kellene ahhoz, hogy megnézzünk egy videót (video kodekes átverés), ne tegyük! Ha valóban megtalálták a gépet, azt a CNN vagy a BBC híroldal mindenféle kattintási, lájkolási, vagy megosztási kötelezettség nélkül szabadon olvasható módon amúgy is megírja.**

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Színezd újra, színezd újra!](#)

[Az MH17 áldozatok hamis Facebook profiljai](#)

[Itt a foci VB, jönnek az átverések is](#)

[Valentin nap: Szerelem helyett átverés érkezik](#)

[Közelgő Karácsony, szaporodó adathalászat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6500219>

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.

LastPass a pácban

2014.07.14. 11:40 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

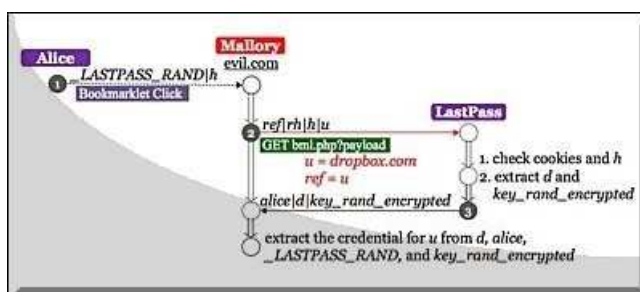
Címkék: [hiba](#) [javascript](#) [jelszó](#) [javítás](#) [menedzser](#) [otp](#) [sebezhetőség](#) [bookmarklet](#) [lastpass](#) [zhiwei](#)

Biztonsági lukak bukkantak fel a népszerű LastPass nevű internetes jelszómenedzser programban. A cég szerint egyáltalán nem kell pánikba esni, bár azt azért mindenképpen érdemes figyelembe venni, hogy hasonló esetekben a gyártók rendre igyekeznek bagatellizálni a sebezhetőségek súlyosságát. A mostani kihasználható hibák Chrome, Firefox, Opera és a Safari alatt jelentkeznek.

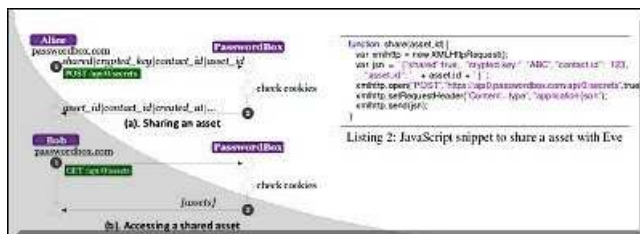


Az egyik ilyen sebezhetőség a LastPass könyvjelzőkkel kapcsolatos, ezeket a kis JavaScript kódrészleteket telepíthetjük kedvenc böngészőnk alá. Ha rákattintunk egy ilyen Bookmarkletre, akkor ez lefut. Zhiwei Li biztonsági kutató a Berkeley egyetemről azonban felfedezett egy olyan módszert, amivel **ha a felhasználó egy kártékony weblapon használta ezt a könyvjelzőzést, akkor a rosszindulatú támadóknak lehetségessé vált a felhasználó más oldalainak jelszavait kilopni a LastPass alkalmazásból.**

A szakértő a tesztjei során például sikerrel tulajdonított el Dropbox belépési adatokat. A LastPass szerint mindez nem igazán veszélyes, mert állítólag a felhasználók kevesebb, mint 1%-a használja csak a Bookmarklet funkciót, és különben is, ők még nem találtak olyan kóddal, ami azt bizonyította volna, hogy valóban aktívan kihasználják ezt a sérülékenységet. ([Vajon hol hallottunk már korábban ilyen mondatokat?](#) ;-)



Egy másik sebezhetőség az OTP-t, azaz a szuper biztonságos One Time Password-öt érinti. Az egyszer használatos jelszó elvileg feltörhetetlen biztonságot ad, még ha egy megbízhatatlan számítógépre kell is belépünk. Itt a szakértő azt demonstrálta, hogy ha a támadó tudta az áldozat LastPass felhasználói nevét, akkor bár szerencsére közvetlenül nem fér hozzá a tárolt jelszavakhoz, viszont **elérhette a titkosítva tárolt jelszóadatbázist, illetve a hitelesítő adatokat akár ki is tudta törölni.** Zhiwei Li és kutató társai, akik a kísérleteket nem éles, hanem a demóhoz létrehozott accountokon végezték, [átadták az információkat a LastPass fejlesztőknek.](#)



Mint minden programban, a jelszómenedzserekben is fedeznek fel időnként hibákat, így [a LastPass mellett a RoboForm, a MyLogin, a PasswordBox vagy a NeedMyPassword is terítéken volt már](#) hasonló okokból. Mindez természetesen **nem jelenti azt, hogy ezeket egyáltalán ne használjuk, hanem helyette mindenhol egységesen az "abc123" jelszót állítsuk be, de fontos, hogy mindenki tisztában legyen a lehetséges kockázatokkal.**

Ami viszont biztos, hogy a sebezhetőségek nyilvánosságra kerülése esetén a helyzet beismerése, az arra adott reakálás és magának a javítás megjelenésének a gyorsasága is nagyban meghatározhatja azt, hogy melyik jelszómenedzser termékbe helyezük hosszú távon a bizalmunkat, **amelyre emlékeztünk és sárga cetlik helyett "mindent egy lapra" feltéve az összes internetes elérési belépési adatunk biztonságos őrzését rábízuk.**



Az összes antivírus szakember évek óta hangsúlyozza, hiába használ valaki megfelelő védelmi programokat, **ha közben mindenütt gyenge vagy azonos jelszavai vannak. Emlékeztet például, hogy a már hetedik éve toplistás Conficker féreg is épít erre, szótáralapú támadást indítva a gyenge adminisztrátori jelszavak ellen. De az is gyakori forgatókönyv, hogy a támadók az egyik helyen megszerzett jelszavakat az áldozat összes lehetséges online helyszínén végigpróbálgatják Gmail-től Facebook-ig, hátha szerencsájuk lesz. Valószínűleg pontosan ez az utóbbi technika okozta például a legutóbbi [Apple gépeken előfordult Oleg Pliss féle incidenseket](#) is.**

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Sokkoljon-e minket a Shellshock?](#)
[Éljen soká az alapértelmezett jelszó 2.](#)
[Új funkcióval bővült a Netcraft Toolbar](#)
[A Starbucks mobilfizetés esete a clear texttel](#)
[A Facebook és a Microsoft együtt keresik a hibákat](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6506999>

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 CNET-nek is reszeltek

2014.07.16. 10:34 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [orosz jelszó cnet hacker csapat feltörés data breach w0rm](#)

A hétvégén elesett a népszerű tech hírek és vélemények weblapja, a CNET és körülbelül 1 millió felhasználói jelszó kerülhetett ezzel veszélybe. Az elkövető w0rm nevű orosz hacker csapat a Twitteren mutatta fel a skalpot, és az adatbázisért cserébe mindössze 1 Bitcoin (1 BTC a mai coinmill.com szerinti árfolyamon nagyjából 104 ezer HUF). **Mindenki azonnal induljon jelszót cserélni!**



```

1 Here is full src of cnet.com
2
3 if u need DataBase, send me 1BTC
4
5 12pMkQZwhdmTejeASFBOT3sQaureRnCYe
6
7 your e-mail for download link in comment.
8
9
10 twitter: @Rev_priv8
11 website: https://w0rm.in
12
13 w0rm.
14
  
```

Július 12-én született az első képes Twitter bejegyzés, amelyben az "ölünkbe hullott az adatbázis" híradás elég egyértelmű helyzetet mutat. Ezt követte aztán két nap múlva a másik, ahol pedig w0rmék felajánlották a szolgálataikat abból a célból, hogy a CNET megerősítse a webes védelmét. A w0rm már korábban is hajtott végre elhíresült akciókat, nekik tulajdonítják többek közt a BBC, az Adobe illetve a Bank of America elleni támadásokat is. A CNET megerősítette a feltörés tényét, beleértve azt is, hogy "néhány szerver adataihoz is" valóban hozzáfért az elkövető(-). A veszteség listán pedig [1 millió felhasználói e-mailcím, belépési azonosító, illetve az ezekhez tartozó titkosított jelszó](#) hash sorakozik. Majd itt is kiderül előbb-utóbb, hogy voltak-e egyáltalán szóva azok a jelszóhashek vagy mégsem :-)

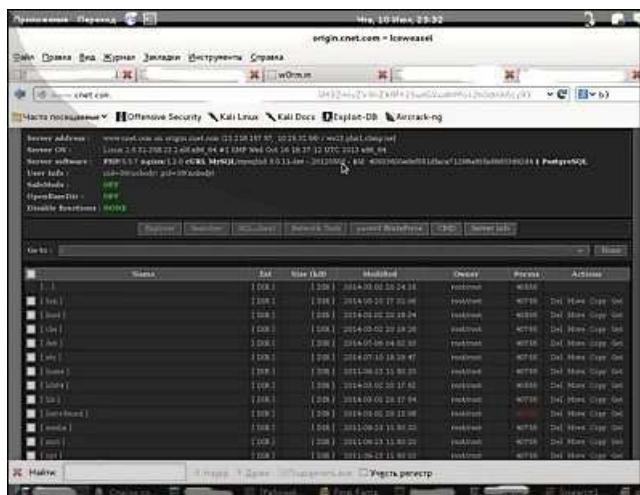


Az eddigi adatok szerint a támadás a Symfony PHP frameworkben található sebezhetőség miatt következett be, erre az említett keretrendszerre épült a CNET oldala. A ransomware-ekhez hasonlóan valószínűsíthető, hogy nem fognak a támadókkal üzletelni, naivság is lenne megbízni bennük (addig álljanak az oroszok fél lábán, amíg az 1 Bitcoin átutalja nekik a CNET;-). [Jen Boscacci szóvivő](#) szerint az oroszországi támadók állítólag nem tervezik a jelszavak dekódolását vagy a megszerzett adatbázis értékesítését (látszólag valóban nem a pénzhűség, hanem a nyilvános megszegényítés volt a céljuk, de erre azért senki ne vegyen mérget, az is lehet, hogy már el is készültek vele ;-).



A szóvivő azt közölte még, hogy megoldották a problémát és már uralják a helyzetet: "We identified the issue and resolved it a few days ago. We will continue to monitor [the situation]." Hogy ez aztán mennyire fedi a valóságot, azt mindenki döntse el ki-ki maga.

Mindenesetre a szokásos remedy vár most minden regisztrált jutzerre, különösen azokra, akik lustaságból ugyanazt a password-öt használják aktívan máshol is.



A nekünk most egy szólanc játékban végig kellene mondani az összes jelentős jelszóvesztős databreach esetet az elmúlt három évből, biztosan nem sikerülne mindent Adobe-tól egészen a **LinkedIn-ig fejből felsorolni**. A biztonságos jelszavakkal kapcsolatos szájbarágós részt - legyen erős, legyen egyedi, stb. - most nem ismételjük el részletesen hetvenezredszer, de mivel valóban fontos, ezért természetesen belinkeljük mindazoknak, akiknek ez még új és hasznos információ lehet.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **PinIt** **+1**

Ajánlott bejegyzések:

[Lopott Minecraft jelszavak szivárogtak ki](#)
[Munkavállalói adatok szivárogtak az Nvidia-tól](#)
[Kiszivárgott jelszavak - ránk váró teendők](#)
[Hogyan védjük meg Twitter fiókunkat?](#)
[A jelszó érték, vigyázzunk rá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6512925>

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.

Júniusi vírusstoplista

2014.07.18. 10:05 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [radar](#) [adatok](#) [június](#) [nod32](#) [havi](#) [report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. júniusában a következő 10 károkozó terjedt a legnagyobb számban.



Az előző havi eredményekhez képest változatlanul a **mentéseket törölő Win32/Bundpil féreg az első, immár kilencedik hónapja listavezető**. Bár minden alkalommal elmondjuk, de sose lehet elégszer kihangsúlyozni, hogy **fontos feladat a saját munkák rendszeres külső adathordozóra készülő mentése**. A hatékony védelem érdekében az is lényeges, hogy ne csak egyetlen backup példánnyal, hanem párhuzamosan több különböző verziójú, mentéssel is rendelkezünk.



Második helyen viszont most a **JS/Kryptik trójait** találjuk, vele még 2009-ben találkozhattunk utoljára. Ez tulajdonképpen egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlan **összezárt JavaScript kódoknak**, amely a **különbő HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját**.

Régi-új szereplő található a **kilencedik helyen is a HTML/Iframe.B.Gen vírus** személyében, amely fertőzött weboldalakon keresztül terjed. A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek **HTML weboldalak Iframe tageibe ágyazódva egy megadott kártékony URL helyre irányítja át a böngészőt** a felhasználó tudta és engedélye nélkül.



Az ESET Radar Report e havi kiadásában ezúttal az **Apple háza táján nem rég történt incidensről** olvasható egy alapos összefoglaló. Mint emlékeztet, 2014. májusában ausztrál lapok számoltak be arról, hogy néhány iPhone és iPad felhasználót kizártak a készülékükből. A közösségi oldalak beszámói, és blogbejegyzések szerint az áldozatok korábban egy kértlen üzenetet kaptak a Find My

iPhone funkció nevében, amely azt írta "Hacked by Oleg Pliss. For unlock device YOU NEED send voucher code by 100 \$/eur one of this (Moneypack/Ukash/PaySafeCard) to [email address]", vagyis az állítólagos feltörés segítségével végrehajtott zárolás feloldásáért cserébe váltásdíjat követel egy állítólagos Oleg Pliss, ellenkező esetben nem kapjuk vissza a hozzáférést.

Biztonsági szakértők szerint azonban sokkal inkább arról lehetett szó, hogy a támadó vagy a támadók teljesen más helyszínről és más forrásból megszerzett jelszavaikat elkezdték szépen kipróbálgatni az Apple Find My iPhone szolgáltatáson, hátha valaki itt is ugyanazt használta, és ez trükk szemlátomást bejött nekik.

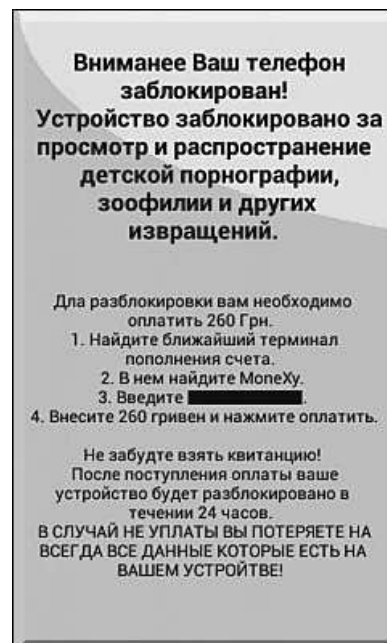


Ezzel kapcsolatosan érdemes kihangsúlyozni a védekezés és a megelőzés fontosságát. Akiknek még esetleg nincsen szinkronizált mentésük az iTunes-ban vagy iCloud-ban, akkor hozzanak létre ilyen, mert hasonló incidens során onnan például egyszerűen helyre tudják állítani az előző állapotot. Emiatt történhetett meg a fenti esetben, hogy akiknek viszont nem volt ilyen, az adatvesztés nélkül nem úszta meg a visszaállítást.

Emellett érdemes bekapcsolni a két faktoros autentikációs opciót is, és javasolt rendszeresen menteni az iCloud, az iTunes, illetve a Time Machine segítségével, vagy akár párhuzamosan ezek mindegyikével. És nem utolsó sorban használjunk erős és egyedi - vagyis kitalálhatatlan, helyszínenként különböző és szótár alapon nehezen törhető - jelszót az Apple ID-hez.

Weak	Medium	Strong
All numbers or all letters	Alphanumeric	Alphanumeric with a mix of upper and lower case letters
beckerisc00l	becker2cool	B3cker2C00l

Júniusi fontosabb blogposztjaink között szót ejtettünk arról, hogy megjelent az első váltásdíjas titkosító kártevő Androidon. [A vadonatúj trójai zsaroló programként terjed és titkosítja mobil eszközeink SD kártyáját](#). Érdekeség, hogy a kártevő az orosz nyelven megírt zsaroló üzenetben a váltásdíjat ukrán nemzeti valutában, hrivnyában kéri.



Emellett hírt adtunk róla, hogy [a foci VB kezdete egyben az ezzel a témával foglalkozó csalások tömeges megjelenésével is járt](#). Ezúttal például az állítólagos ingyen lottós pénznyereményünk mellé csak most csak nekünk ingyen jegyet is ígértek a foci VB-re. Egy korábbi kimutatás szerint már májusban nagyjából a spam termés ötöde foci VB-s apropóval érkezett. Félelmetes mennyiségű hamis jegyet megpróbáltak különféle árverési portálokon értékesíteni, ám a látszatra igazi jegyekben azonban nincsen azonosító chip, ami általában már csak későn, a beléptetőkapuknál derül ki.



Terítékre került a nyár, a bikini szezon apropóján egy Twitteren és Pinteresten terjedő spam kampány is, amely az általa hirdetett fogyókúra készítményt mint varázsszert mutatta be, ám [a méregdrága tabletták általában hatástalanok, a csodálatos fogyást bemutató képek pedig többnyire Photoshop manipulációval](#) készülnek. Érdemes minden hihetetlen és minden gyógyszerrel kapcsolatos kéretlen hirdetést gyanakvással és fenntartással kezelni.



Végül írtuk arról is, hogy az elmúlt hónapban nem csak hogy ellopták Michael Schumacher orvosi kartonját és az adatokat pénzért árulták az interneten, hanem pár nappal később, a magánklinikára való szállítása után **ismeretlenek a formula egyes pilóta hamis halálhírét keltették a Facebookon**. Ami természetesen nem volt igaz, célja a naiv látogatók kattintása utáni rapidstockprofit doménnel kapcsolatos pénzkereset volt. Sajnos az ilyen átveréseket sokan gondolkodás nélkül már alaptól is továbbbocsítják, és az is [szomorú, hogy vannak olyan gátlástalan emberek, akik mások baján, nyomorúságán igyekeznek ilyen szánalmas kattintásvadász módszerekkel pénzt keresni](#).



Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2014. júniusában a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 15.14%-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.



01. Win32/Bundpil főreg

Elterjedtsége a júniusi fertőzések között: 2.59%

Működés: A Win32/Bundpil főreg 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.



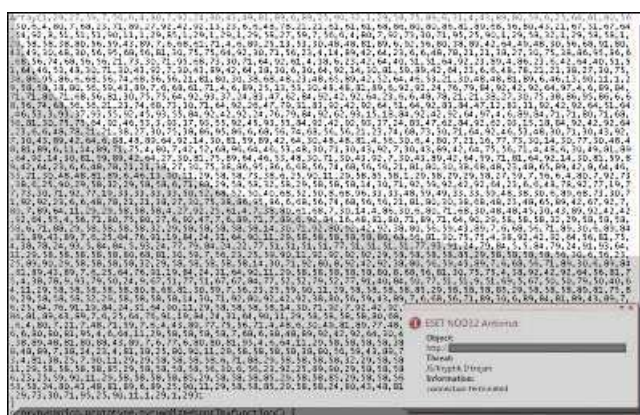
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



02. JS/Kryptik trójai

Elterjedtsége a júniusi fertőzések között: 2.35%

Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlanul összezavart JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját.



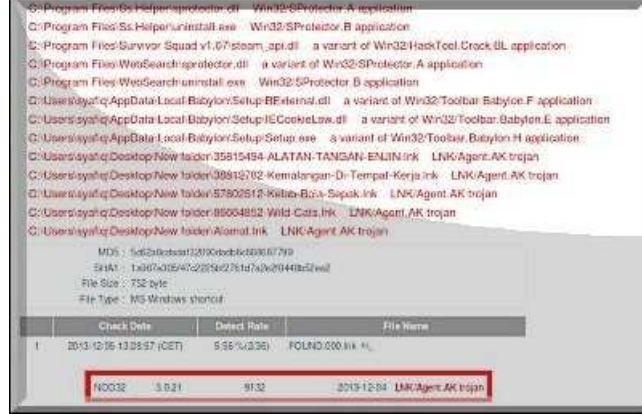
Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail



03. LNK/Agent trójai

Elterjedtsége a júniusi fertőzések között: 1.91%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatokot 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. Viruselemzők 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



04. Win32/Sality vírus

Elterjedtsége a júniusi fertőzések között: 1.49%

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.



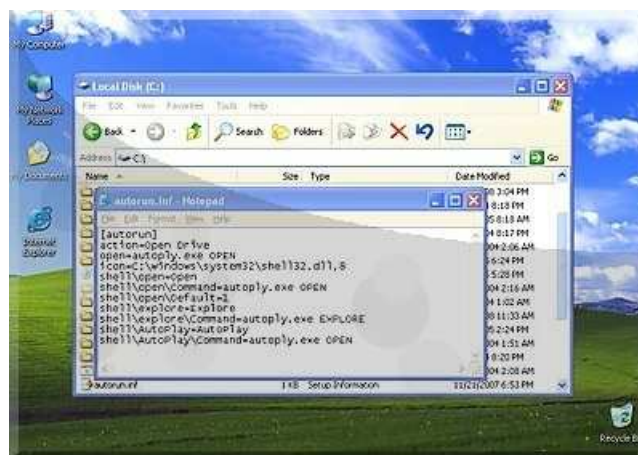
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



05. INF/Autorun vírus

Elterjedtsége a júniusi fertőzések között: 1.38%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájl használó károkozónak. 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>

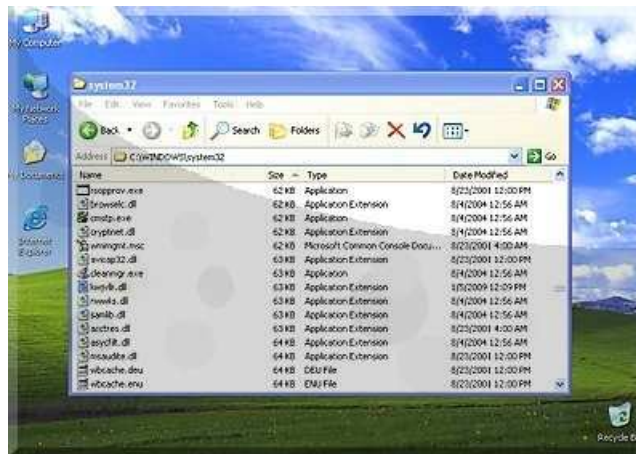


06. Win32/Conficker férgek

Elterjedtsége a júniusi fertőzések között: 1.20%

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 eljárásn keresztül, majd távoli szerverekkel lép kapcsolatba, hogy azokról további kártékony kódokat töltsön le. Emellett a féreg módosítja a hosts

Íjált, 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.



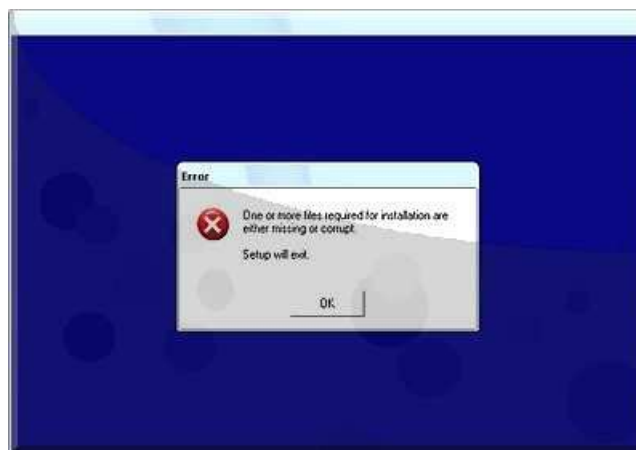
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21conficker>



07. Win32/Ramnit vírus

Elterjedtsége a júniusi fertőzések között: 1.16%

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. Végrehajtáskor 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.



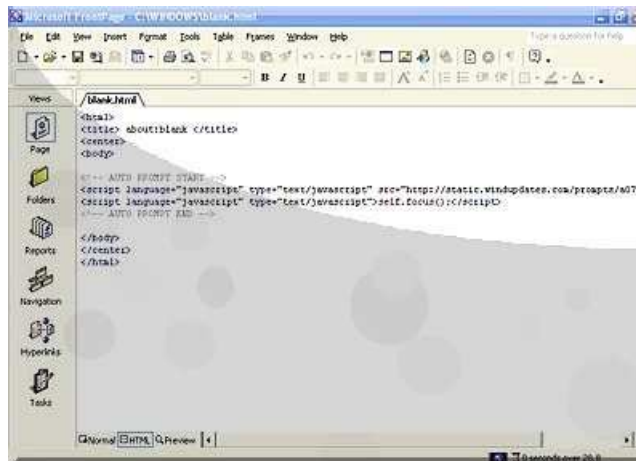
Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en



08. HTML/ScrInject trójai

Elterjedtsége a júniusi fertőzések között: 1.06%

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/scriinject-b-gen>

09. HTML/Iframe.B.Gen vírus

Elterjedtsége a júniusi fertőzések között: 1.04%

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



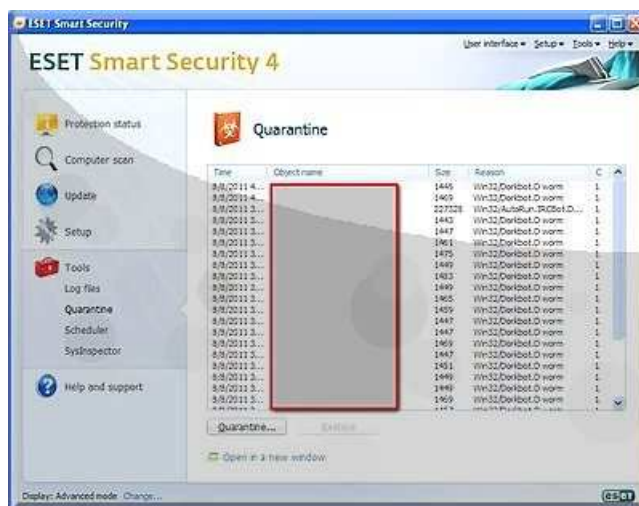
Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description



10. Win32/Dorkbot féreg

Elterjedtsége a júniusi fertőzések között: 0.96%

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

 Tetszik [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[A HTML trójaiak riogattak minket októberben](#)

[Végre kiesett a Conficker féreg](#)

[Vírusstoplista 2014. augusztus hónap](#)

[Júliusi vírusstoplista](#)

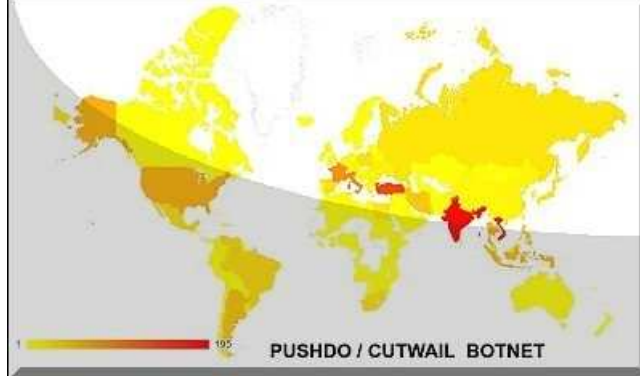
A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6517839>

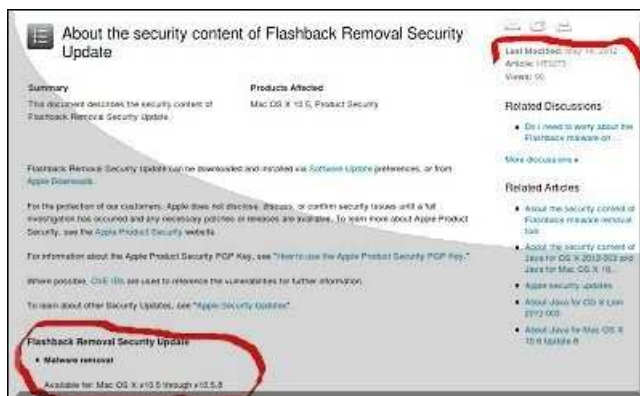
Kommentek:

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.



Joseph Demarest, az FBI helyettes igazgatója szerint a botnetek óriási pénzügyi veszteségeket okoznak, adataik szerint [az amerikai lakosságnak 9 milliárd USD kárt okoz, világszerte pedig 110 milliárd dollár értékű kárt szenvednek el a zombihálózatok támadásai miatt](#). Csak érdekességképpen azt is érdemes mindehhez hozzátenni, hogy egy Macintosh rendszerre való átállás nem jelenti automatikusan azt, hogy attól kezdve biztosan kártevőmentes lesz az életünk, hiszen sebezhetőségek ott is léteznek, [gondoljunk csak a 2012. márciusában elindult, és egy Java sérülékenységre miatt kialakult, több mint 600 ezer gépet megfertőző OS X-es FlashBack botnetre](#). Hogy általában mégis miről ismerhetjük fel, hogy esetleg mi is esetlegesen egy botnet hadsereg részei vagyunk, arról korábban írtunk már egy hosszabb részletes összefoglalót. Ezek [a jelek nagy vonalakban ma is épp olyan jellegzetesek, vagyis a gép erőteljes lelassulása, illetve a nevünkben rejtve küldött üzenetek, vagy éppen a rendszerfrissítések elérhetőségének letiltása](#) is árulkodó lehet, **a biztos információt azonban mindig az alapos víruskeresés adhatja meg.**



És végül mit lehet tenni a hatékony védekezéshez? **[A megelőzésre koncentrálni a legsikeresebb stratégia, így a naprakész vírusvédelmi program futtatása, ne kapaszkodjunk a már támogatás nélkül maradt és sérülékeny Windows XP rendszerbe, az operációs rendszerünk és alkalmazói programjaink teljeskörű rendszeres frissítése és folyamatos frissen tartása a hibajavító foltokkal, de részben idetartozik a megfelelően erős jelszavak használata is.](#)** És persze a telepítendő programjaink alapos megválasztása is lényegbevágó, hiszen [a trójaiak az utóbbi években alaposan feladták a leckét minden felhasználónak](#), és a különféle platformokon rengeteg fertőzést okoztak világszerte.

Tetszik 4 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

[Gépeinket is támadják a zombik](#)
[Hogyan védekezzünk botnetek ellen?](#)
[Amikor a marketing üzenet már kevés](#)
[Van új a Nap alatt: Napolar](#)
[Anyu, hogy lett Apuból egy zombi?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6529171>

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 váltságdíjas titkosító kártevő visszatér

2014.07.23. 11:42 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [mobil trójai](#) [android titkosítás](#) [adatvesztés](#) [eset kártevő váltságdíj](#) [aes zsaroló ransomware](#) [welivesecurity.com](#) [simplocker](#) [decryptor](#)

Nem sokat kellett várni na nem a Jedi, hanem az androidos váltságdíjas titkosító kártevő visszatérésére. Az új verzió számos tekintetben különbözik a még június elején felfedezett elődjétől, amiből arra lehet következtetni, hogy valószínűleg tetszik ez a csapásirány a kártevő készítőknél. Láthatóan erősen bíznak az új pénzszerzési technikájukban, és bár sokakat talán sikerül így pénzzel lehúzni, de szerencsénkre a mobilos trójai kódja technikailag még messze van az olyan tökéletestől, [mint például a Windows alatt futó PC-s CryptoLocker](#).



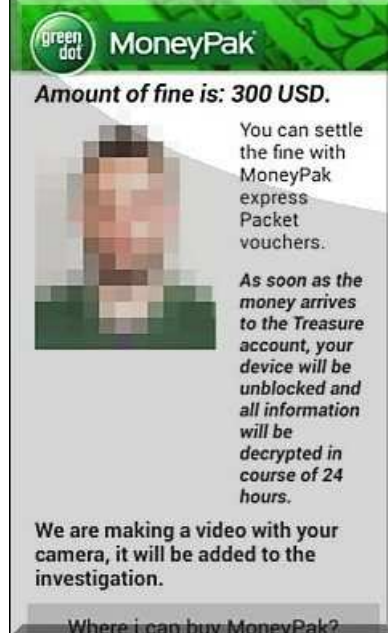
Az [első verziós](#), és sok tekintetben kísérleti PoC, azaz Proof of Concept malware kód sok érdekességet mutatott, például hogy az okostelefon SD kártyáján található jpeg, jpg, png, bmp, gif, pdf, doc, docx, txt, avi, mkv, 3gp, mp4 kiterjesztéssel rendelkező fájljainkat AES (Advanced Encryption Standard) kódolási eljárás használatával titkosította, majd az állományok helyreállításért cserébe a váltságdíjat ukrán hrivnyában kérték.

Ugyancsak érdekes, de logikus húzás volt részükről, hogy a hatásosabb védelem és anonimitás érdekében a távoli vezérlő C&C szerveret egy nehezebben nyomon követhető TOR .onion domain-en regisztrálták.



A mostani új változat már nem éri be a legutóbbi 260 ukrán hrivnya, azaz nagyjából 16 eurónak, illetve közel 5000 forintnak megfelelő összeggel, ennél most jóval többet követel, 300 amerikai dollárt, ami bőven több, mint tízszerese a korábbi fejpénznek. De nem csak a megnövekedett étvágy és mohóság változott, hanem egyúttal bővült az elkódolt állománytípusok köre is. Ez gyakorlatilag azt jelenti, hogy **immár titkosítja az olyan archív fájlokat is, mint a ZIP, 7z és RAR**.

Ez a "frissítés" rendkívül kellemetlen következményekkel járhat számunkra, hiszen tanulva az előző esetből valószínűleg sokan választottak maguknak valamilyen Androidos biztonsági mentést végző eszközt, amelyek előszeretettel használják a fenti állománytípusokat. **Így viszont ha a mentés nem volt kimásolva külső adathordozóra is, akkor lényegében véve az egész nem ér semmit, hiszen a fertőzés végén a tömörített mentés is titkosítva lesz.**

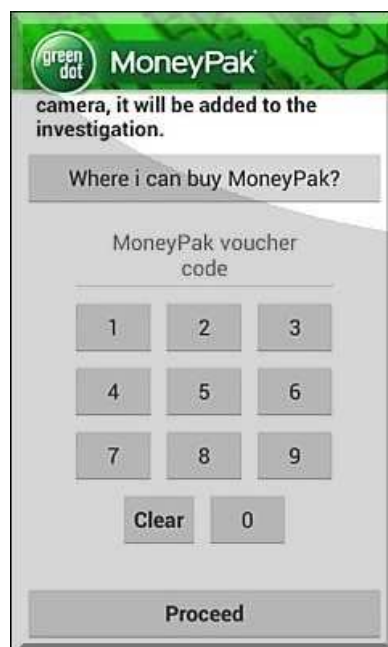


Akik korábban sokat olvasták az antivirus blogot, azoknak [a rendőrségi zsaroló programok biztosan ismerősök lehetnek](#). Ezek a korábbi hamis antivírusokból fejlődtek ki, eleinte RIAA és egyéb szerzői jogvédelemmel kapcsolatos szervezetek nevében riogatták a felhasználókat védelmi pénzt szedve, aztán ez az irány a jogvédelem helyett **a sokkal ijesztőbb hamis pedofil vád irányába ment el, és a látszólagos feladó is a CIA, FBI vagy éppen az aktuális ország lekérdezésével a felhasználó saját rendőrsége lett, anyanyelven zsarolva az áldozatokat.**



Nos ez a korszak látszik újraéledni most az Androidon is, amikor azt igyekeznek elhitetni, hogy a készüléket az FBI blokkolta amiatt, mert illegális tartalmakat, gyermekpornográfiát vagy hasonló jogsértő tevékenységet észlelt. A további változások között szerepel még a fizetési módzat újragombolása is, amely [ezúttal a MoneyPak használatát jelenti](#).

Vagyis szemben a korábbiakkal, ahol nem jelent meg egy fizetési kódot bekérő mező, hanem ehelyett a távoli C&C szerver parancsára várt, itt most ehhez kapunk egy egyedi kódbeírásra alkalmas képernyőt is.



A kártevő fejlesztők az eltávolítást is igyekeztek az előzőkhöz képest valamivel jobban megnehezíteni, ami szerencsénkre elég

kezdetelegesen sikeredett. Míg a korábbi SimpLocker verzióknál a kártevő maga gondoskodott a saját védelméről, [az új változatnál már a Device Administrator segítségével teszi ezt.](#)

Természetesen ez sem ördögösség, mindössze egy minimális plusz nehezítés a gyakorlatlanabb felhasználóknak, hiszen így az eltávolításnál először mindenféleképpen itt kell megvonni a kiterjesztett jogosítványokat, és csak utána tudjuk majd a rosszindulatú programot valóban törölni.



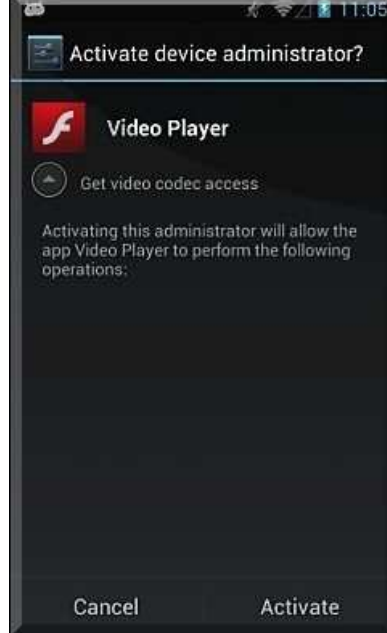
A másik gyenge pont továbbra is a titkosítási algoritmus, amely szerencsére változatlanul messze van még a tökéletestől. A lényeg, hogy a malware készítője elkövetett egy kapitális szarvashibát, ugyanis a [dekódolási jelszót konstansként tárolta](#), így ehhez szerencsére bárki hozzá tud férni. Az ESET elkészített egy [ESET SimpLocker Decryptor nevű alkalmazást](#), amely segít biztonságosan helyreállítani és olvasható, használható formában visszanyerni a kártevő által elkódolt, titkosított állományainkat.

A vírusirtó cég folyamatosan fejleszti ezt a helyreállító segédprogramot is, de arra nincs semmilyen garancia, hogy bűnözők a fenti titkosítási hibát egyszer a jövőben nem fogják majd kijavítani. Így a CryptoLocker-hez hasonlóan sose felejtjük el, hogy a megelőzés a legfontosabb, így a naprakész vírusvédelmi programok használata mellett adatainkról csak akkor gondoskodunk megfelelően, ha azokról rendszeresen készítünk biztonsági másolatokat, és ezeket a mentéseket egy másik, elkülönített külső adathordozón tároljuk.



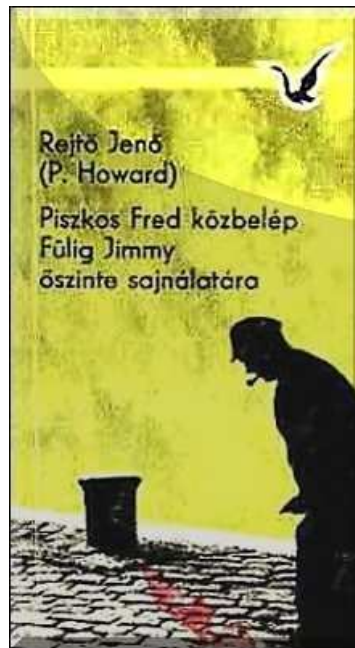
A harmadik gyenge pont pedig maga a "terjedés", vagyis az ilyen trójai programok elsősorban social engineering, tehát emberi megtévesztéssel képesek csak becsapni a felhasználókat. Így például újra találkozhatunk [a PC világból már unalomig ismert primitív kodek telepítési trükkel](#), ami állítólag a flash videó lejátszásához kell.

Vagyis összegezve mindent, pánikra nincs ok, már ami a kártevő pillanatnyi képességeit illeti, de ismét ki kell hangsúlyozni, hogy ennek ellenére [alaposan válogassuk meg, mit és honnan telepítünk fel](#). Illetve természetesen javasolt [valamilyen vírusirtót, állandó védelmi programot is használni](#) az Android alapú okostelefonon, tableten, amely képes blokkolni a hasonló kártékony támadási kísérleteket. Emellett bár az ESET szakemberei találkoztak élesben ezzel az új verzióval, de [az angol nyelvterületeken való széleskörű terjedést](#) egyelőre szerencsére nem mutatnak a statisztikák.



□s végül már csak a nyár miatt is, lezárásként következzen egy kis látóköör tágító érdekesség arról, hogy [pontosan milyen rafinált, agyafúrt és furmányos átverési trükkök terjednek világszerte, amellyel a hétköznapi embereket, turistákat igyekeznek lehúzni, meglopni, átverni.](#)

A fentiek fényében bátran elmondhatjuk, [ez az iparág is fényéveket fejlődött a Rejtő Jenő: Pizskos Fred közbelép című könyvéből megismert gazdag turisták autója elé való műesés óta.](#) Emiatt mind a nyaraláskor, mind a számítógép előtt érdemes óvatosnak lenni, és figyelemmel kísérni az aktuális csalásokat - ez a fajta korszerű és naprakész ismeret lehet biztonságtudatosságunk egyik záloga.



"Rócsildnak azért hívták, mert esz ety gazdag svéd mágnás, s egyszer amilyen szerencsés esz a Bökezű, elütötte őt autó következtében. És akkor fizetett sokat, mer a haverok, akik ety kapu alá vitték asz elgászolt Bökezűt, kicsit hozzásegíték a lábát ety töréshez. Még azt is megtették neki (barát asz barát!), hogy a fejit odaütögették, úgy hoty mire kijöttek a mentők, már kórházképes volt és elvitték. Így asztán a Rócsild 1. csomó pénct fizetett, és ha a Bökezűnek esze van, akkor halgat a Buszkó Mocsingra, aki aszt monta, hoty gyorsan tolják ki asz egyik szemét, mert ami biztos asz biztos. Akkor élete végéig kosztja van, mert eszért ételjáradék illeti a törvényből és a szeméből kifolyóan. De hiába a Buszkó Mocsing bolondos jó szíve (felsékedet sem zaklatá asz őt dollárért, pedig mostanában nem dúskál és hiába nyúl a zsebébe, továbbá másokéba: örekszik). Szóval ételjáradék nem lett, pedig az elgázolóval szemben igazi kitolás esz a szem lett volna. A bal. Nem is lett volna kár, mert teljesen dijoptriásá rövidült a látása. Így is sok pénct kapott, mert mire a kórházig értek amennyire lehetet ő maga is meglassította két ujját a foglalatukba és ütyesen, a mentősekrén oldalával, hasítást végzett a lábán. Talán ha kicsit messzeb van a kórház, elhatároszta volna hoty kitolja magának a feleslegesb szemit, amit könnyelműség volt, hoty nem teve. És akkor ő fizetett minden barátjának 1 liter bort és 10 cigarettát! Pedig eszek segítettek neki. Csak én magam két bordáját nyomtam be a hüvelykujjammal! (Mer barát asz barát!)"

[Megosztom](#)
[tumblr.](#)
[Tweet](#)
[Pin it](#)
[+1](#)

Ajánlott bejegyzések:

[Itt az első váltásdíjas titkosító kártevő Androidon](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Véddij a CryptoLocker terjesztőjének fejére](#)
[A CryptoWall bevétele átlépte a milliós határt](#)
[Az androidos titkosító kártevő újra boncolása](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6537217>

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 MH17 áldozatok hamis Facebook profiljai

2014.07.25. 11:05 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

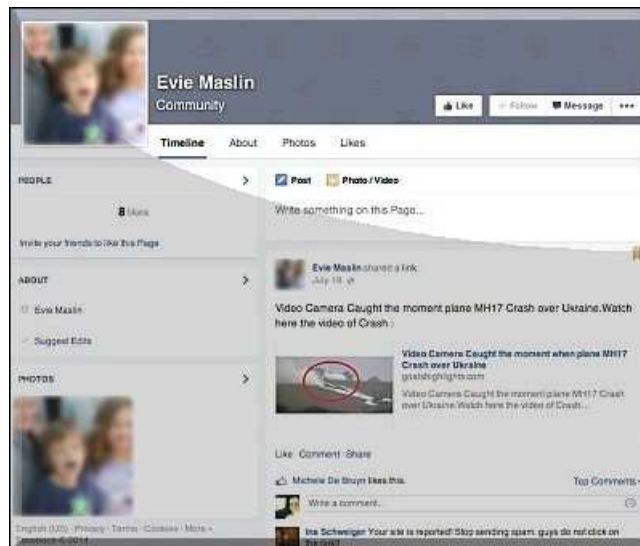
Címkék: [profil](#) [facebook](#) [repülő](#) [holland](#) [csalás](#) [átverés](#) [bankkártya](#) [hamis](#) [maláj](#) [clickjacking](#) [lelőtt](#)

Nincs tabu, nincs tisztelet, legyen az ünnep, Karácsony, vagy akár a kómából lábadozó Forma-1 autóversenyző kórházi kezelése - a csalások kieszelői nem csak villámgyorsak, de minden egyes közérdeklődésre számot tartó eseményre gátlástalanul, és érzéketlenül lecsapnak, miközben nincsenek tekintettel semmire és senkire. **Ezúttal öt olyan ausztrál halott nevében hoztak létre hamis Facebook profilt, akik a lelőtt maláj utasszállítógépen veszítették életüket.**



A beszámolók szerint [ezeken az oldalakon aztán olyan linkeket posztoltak, amelyek azt állították, hogy részletes információkat tartalmaznak a lezuhant repülőgéppel kapcsolatosan](#). Azonban, ha a felhasználó rákattintott a hivatkozásokra, akkor a képernyőt elárasztották a pop-up hirdetések, illetve böngészőjét észrevétlenül kártékony hivatkozásokra irányították át. A hamis profilekat szerencsére a Facebook gyorsan megszüntette, így a kértlen reklámok, valamint a clickjacking, azaz a látogatók észrevétlen átirányításával történő kattintásos pénzkeresés leállt ezeken az oldalakon.

Az érdeklődést mindenesetre ez a repülőgépes eset is alaposan felcsigázta, és bár már angol szakértők ellenőrzik a két fekete dobozt, forensic vizsgálattal először azt nézik meg, hogy a négy napra eltűnt és újra előkerült eszközök adatait nem manipulálták-e utólag. Emellett arról is [folynak konspirációs találgatások, hogy állítólag szándékosan megzavarták a szakadárak rakétaindító-rendszerének radarjait](#), hogy azok ne észleljék a civil gépet, hanem csak az amögött szálló másik harci repülőt, és így mivel csak az utóbbit látták, tévedésből arra lőttek.



Visszatérve a hamis profilekra, nem ez volt az egyetlen visszataszító esemény ezzel a tragédiával kapcsolatosan, **egy Facebookos beszámoló szerint a helyszínre érkező "katasztrófa turisták" hamar összegyűjtötték a halottak ékszereit, bankkártyáit és az ott talált készpénzt.** A poszt szerzője, az ukrán illetőségű Anton Gerashchenko még arra is felhívta a figyelmet, hogy a bankoknak tanácsos lenne azonnal befagyasztani az áldozatok számláit, nehogy a hullarablók megszapolják azokat.

Erre reagálva a holland Bankszövetség azt nyilatkozta, nem fagyasztják be a kártyákat, mert akkor a közeli rokonok, hozzátartozók sem férhetnének hozzá a pénzekhez, és mert szerintük PIN kód nélkül ezek nem használhatók a tolvajok számára. Azért mindezt kiegészítette azzal, hogy [amennyiben mégis gyanús tranzakciók történének az áldozatok bankkártyáival, úgy a hozzátartozókat mindenképpen kárpótolni fogják.](#)



Emlékezz, hogy a korábban [rejtélyesen eltűnt másik repülőgépről már többször jelentek meg hamis](#) hírek az állítólagos megtalálásról, míg [Michael Schumachernek egyenesen hamis halálhírét keltették](#) a kattintásvadász csalók. Mindenesetre egyfelől szomorú, hogy ekkora a gátlástalanság, másfelől tanulság is, hogy hasonló esetekben mire lehet számítani, milyen átverési forgatókönyvek érkehetnek, amiket jobb, ha elkerülünk.

És még mindig nincs vége a trükkök tárházának, mert sajnos gyakran vannak olyan csalók is, akik a sajnálatot, a szánalmat és a megdöbbenést kihasználva e-mailben, Facebookon, Twitter üzenetben, de akár személyesen, SMS-ben vagy telefonhívással [gyűjtenek állítólagos adományokat, ám az önzetlen segítség helyett lelépnek a pénzzel](#). Emiatt érdemes alaposan utánanézni, rákérdezni az adományt gyűjtő szervezetre, mielőtt támogatnánk azt.



Szenzációs hírekkel kapcsolatban a szokásos mantránkkal zárunk. Eszerint **sose higgyük el, ha egy kéretlen link valami meghökkentőt ígér!** Ne dőlünk be, bármit is ígérnek egy lájkért, és látatlanban előre ne lájkoljunk, ne osszuk meg semmit! Ha bármit telepítenünk kellene ahhoz, hogy megnézzünk egy videót (video kodekes átverés), ne tegyük! **Ha valóban megtalálták a gépet, valóban meghalt valaki híresség, azt a CNN vagy a BBC híroldal mindenféle kattintási, lájkolási, vagy megosztási kötelezettség nélkül szabadon olvasható módon amúgy is megírja.**

Tetszik 6 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pin it** **g+1**

Ajánlott bejegyzések:

[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Megtalálták az eltűnt maláj repülőt! Vagy mégsem?](#)
[Schumacher hamis halálhíre az új átverés](#)
[Figyeld a kígyót! Nem semmi. Hanem átverés :-\)](#)
[R.I.P. Hannah Montana](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6543211>

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](#).



Piiistu • <http://www.soternyelviskola.hu/> 2014.07.25. 13:27:35

hát nagyon vigyázni kell hova kattintunk :S

Válasz erre

Be nem fizetett számla. Vagy mégsem?

2014.07.28. 10:36 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [vámhivatal](#) [finnorszag](#) [vagy csalás](#) [hamis számla](#) [phishing](#) [tartozás](#) [adathalászat](#) [mégsem behajtóintézet](#)

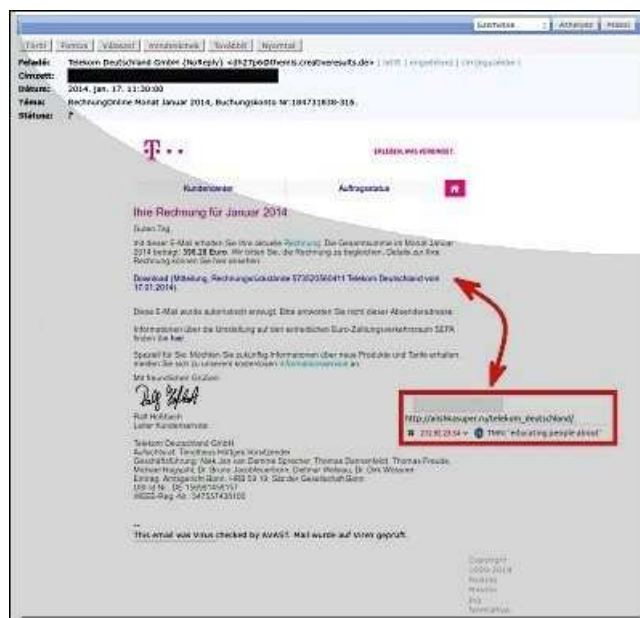
Bár egy pár évvel ezelőtti [felmérés tanúsága szerint a nőket nem annyira érdekli a védekezés](#), mármint ami az antivírus használatot illeti - egy dologban látszólag mégis sokkal precízebbek a férfiaknál: hamarabb rendezik a tartozásaikat, és erre a csalók is felfigyeltek. Erre kihegyezve terjed **ismét az a fajta átverés, amelyik egy állítólagosan be nem fizetett számla miatti figyelmeztetés formájában érkezik.**



Ha számlát kapunk e-mail üzenetben, az manapság egyáltalán nem számít rendkívüli eseménynek, ám **ha az a számla kéretlenül érkezik - vagyis nem egy rendszeres és szokásos folyamat része, esetleg úgy kapjuk, hogy nem is vagyunk a szolgáltató ügyfelei, vagy pedig nem pontosan attól a szolgáltatótól érkezik, akivel mi szerződésben vagyunk - nos ezek már bőven adhatnak okot az alapos gyanakvásra.**



Emellett a fenyegetési/sürgetési faktor szokta még nagyban segíteni a csalókat az ilyen játszmákban, hiszen **ha valaki mérges, ideges, vagy zaklatott, akkor sokkal könnyebben elveszti az önuralmát és ilyenkor hajlamos arra, hogy mégis rákattintson az állítólagos tartozást, vagy vásárlást "bizonyító" mellékletekre.** Erre jó példa a magyar e-mail címekre is tömegesen érkező [nagyobb összegről szóló hamis Telekom](#) számla, vagy [a PayPal nevében küldött és egy olyan Invicta óráról szóló állítólagos fizetési meghagyás](#), amit pedig mi nem is vettünk.



Mostani történetünkben is egy állítólagos be nem fizetett számla játssza a főszerepet, az erről szóló tájékoztatást kapják meg egy ideje számos Finnországban egy helyi bankra hivatkozva. **Az SMS-ben, illetve elektronikus levélben azt írták különféle adósság**

behajtointézetek, vagy éppen a helyi Vámhivatal nevében, hogy az elmulasztott befizetés miatt bajbakerülhetnek, ám most kaptak egy utolsó lehetőséget, hogy a tartozást a mellékelt linken bejelentkezve mindenféle hátrányos következmény nélkül befizethessék.

Természetesen be nem fizetett számla a valóságban nem is létezik, és a megadott URL hivatkozás segítségével ilyenkor adathalász oldalként ellopták az ügyfelek banki bejelentkezési adatait. [A finn rendőrség külön figyelmeztetést is kiadott az ilyen átverésekkel kapcsolatban](#), mert a hiszevény áldozatoktól - akiknek 95%-a nő, talán valóban ők a lelkiismeretesebb befizetők - már több, mint 500 ezer eurót csaltak ki ezzel a trükkel a bűnözők. Az év elején egyébként már letartóztattak egy olyan hatfős finn bűnbandát, akik hasonló módszerekkel ügködtek még 2011 és 2012 között.



Mivel nem kétséges, hogy [sajnos életünk szerves része lett az állandó támadás](#), emiatt az ilyen kísérletek időben történő felismerése hétköznapi feladattá kell, hogy váljon minden felhasználó számára. Az pedig, hogy a nők kifejezetten célzottan kerülnek a támadók célkeresztjébe, szintén nem teljesen újdonság, hiszen például a [társkereséssel kapcsolatos átveréseknél kifejezetten a jó módú, középkorú elvált és hiszevény nőket](#) pécézik ki a csalók.

A hamis adósságbehajtó bizniszben emellett létezik egy olyan, országunkénti átlagfizetéstől függő **elvi összeghatár, amely még éppen nem elég nagy ahhoz, hogy a címzett gyanút fogjon, vagy azonnal reklamáljon, ám ahhoz elég kicsi, hogy a kuncsaft legyintve inkább gyorsan fizessen, csak hogy túl legyen a kellemetlenségen**. Igazából viszont az lenne a kívánatos, ha minden egyes, még a legapróbb indokolatlan vagy vitatható levonási tételnél is haladéktalanul közvetlenül a bankunkhoz fordulnánk, és emellett sosem kattintanánk kéretlen üzenetben kapott linkekre.

 Tetszik 11 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A számlalevelek meg egyre csak jönnek Telekom számla vagy mégsem?](#)
[A játék nyertese pedig nem más, mint Te. Írt nekünk a CERT - vagy mégsem](#)
[Email a YouTube-tól. Vagy mégsem?](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6551101>

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](#).

[Monsieur 2014.07.28. 23:48:13](#)

sajnos nálam ez teljesen aktuális.. a telefonkönybe bekerült megjelenéssel kapcsolatosan hitették el velem hogy még nem fizettem be a szerződött összeget és bizony csúnyán lehúztak mire rájöttem hogy átverés áldozata vagyok..

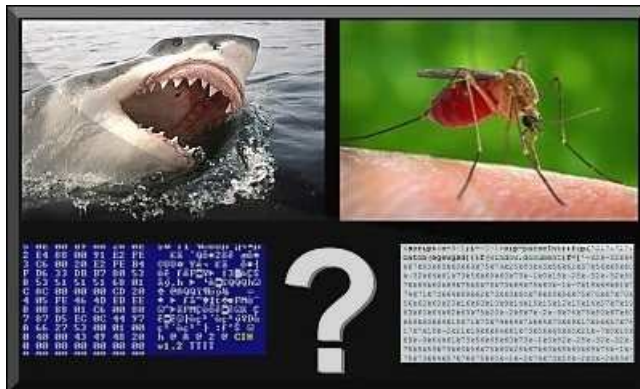
Válasz erre

Hagyományos vírus VS. JavaScript kártevő

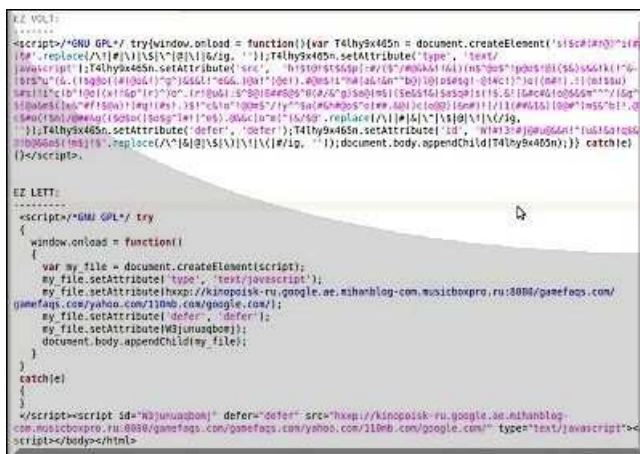
2014.07.30. 13:29 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [protected javascript](#) [biztonság](#) [vírus](#) [veszély](#) [klasszikus script](#) [view noscript](#)

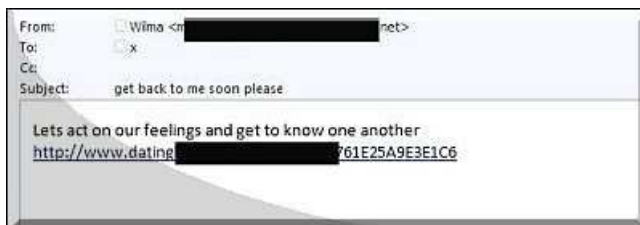
Egy érdekes kérdést tettek fel a minap egy biztonsági fórumon: vajon mi a veszélyesebb, egy klasszikus vírus vagy egy JavaScript nyelven írt kártevő? Nos nézzünk utána - **bár a döntetlen esélyes felvetésnél mindig az a veszélyes, ami a saját gépünkön éppen sikerrel betámad** - és keressünk ezzel kapcsolatos tényeket, példákat.



Ott ragadva a fórumon természetesen érkeznek is rendre az olyan válaszok, amelyek stílszerűen ahhoz hasonlítják a dolgot, mintha valaki azt kérdezné, melyik a veszélyesebb állat: a szúnyog vagy a fehér cápa? Első látásra persze mindenki a cápát gondolja, de a kérdés valójában eldönthetetlen. [Nyilván másként látja mindezt egy mélytengeri bűvár és egy afrikai misszionál dolgozó orvos](#), és nem értenek abban egyet, hogy melyik miatt érdemes többet aggódni. Ám **ha viszont azt nézzük, évente hány ember hal meg moszkítócsípés miatt maláriában, akkor vastagon lekörözné ez a számadat a cápatámadások áldozatainak mennyiségét**, bár természetesen az áldozatokat egyformán sajnáljuk.

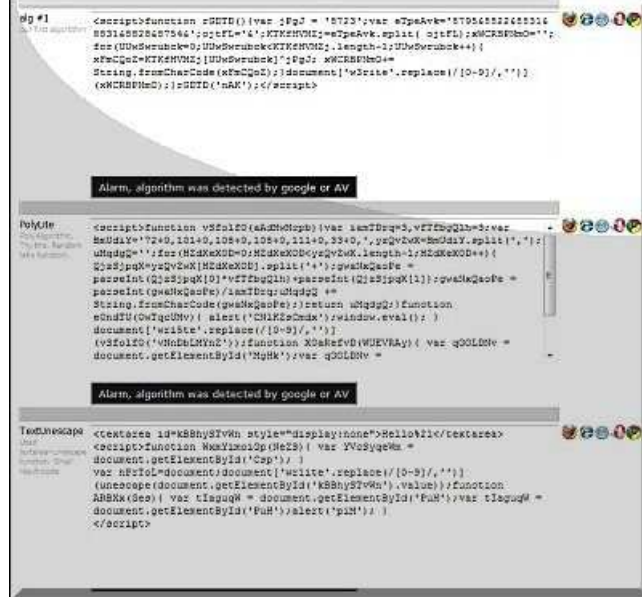


Ez tulajdonképpen egy kicsit retro-szerű kérdés, mert [korábban valóban sokan helytelenül erőteljesen alábecsülték a scriptes kártevők által okozott veszélyeket](#). A lényeg inkább ott van, ha valamelyik fenyeget minket, akkor mindegy, mert mindig amiatt kell aggódni, ami épp szembejön. A veszély pedig nagyjából egyforma, magyarul az okozható károk tekintetében nincs érdemi különbség, rombolásban résztvenni lehet ezzel is lehet rendesen.

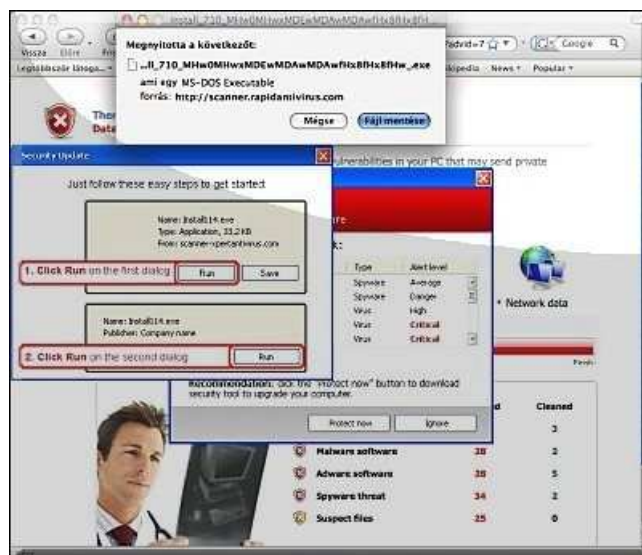


Az eredetileg 1995-ben megjelent kliensoldali JavaScript nyelvet manapság már rengeteg helyen használják, webes alkalmazásokban éppúgy, mint asztali alkalmazásokban, böngésző pluginekben, a Firefox OS-ben vagy akár éppen szerver démonokban is megtalálhatjuk. **Manapság általános felállásnak számít, hogy a hagyományos kártevők fertőzés után a megtámadott rendszeren a háttérben további kártékony JavaScript állományokat kísérlelnek meg magukból kidobni, vagy letölteni, és aztán azokat lefuttatni.**

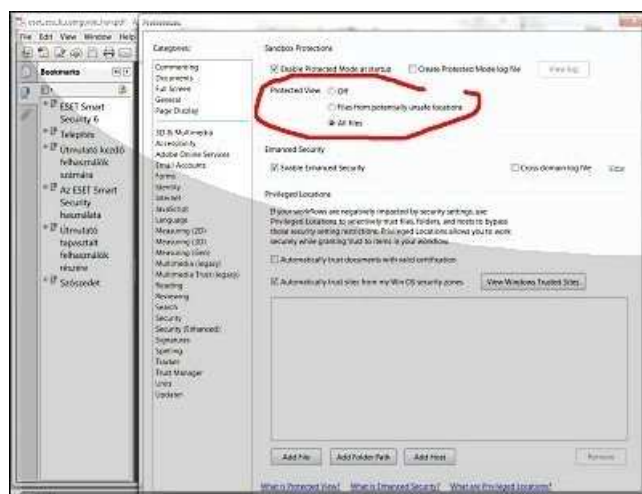
Híres kártevőkből sincs hiány - ilyenek még a havi toplistákon is rendszeresen elő szoktak fordulni, de 2013-ban például egy olyan kártevő ténykedett Brazíliában - amelyik **amellett, hogy az ellopott belépési adatokat éppen egy feltört brazil kormányzati weboldalon keresztül küldte tovább a támadóknak - JavaScript kód segítségével egy Chrome böngésző plugin segítségével lopta el az áldozatok személyes banki adatait.**



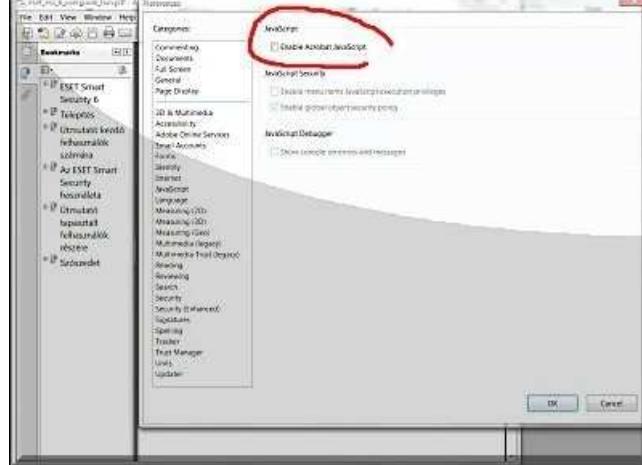
Összegezve tehát jól látszik a fentiekből, a kérdés nem kérdés, a veszély e tekintetben nagyjából független a programozási nyelvtől bár általános esetben a JavaScript azért legtöbbször megfelelő engedélyekkel bír, és a homokozójában fut. Ám ha eközben megnézzük a leggyakoribb böngésző háttérben történő átirányítást végző kártékony kódok többsége script, elsősorban javascript alapú, amiket tulajdonképpen bárki könnyedén gyárthat. Tehát ez is lehet épp olyan veszélyes, mint bármely más vírus, hiszen ugyanúgy sebezhetőséget használhat ki, eredményesen támadva gyenge pontokat az operációs rendszerekben, alkalmazásokban, böngészőkben, így közvetett szerepe van a fertőzésekben és főként az exploitok letöltésében.



Egyébként kevés viccesebb dolgot lehetett annak idején látni, mint a hamis antivírusok hőskorában, amikor [a kezdeti rogue AV programok rendre benézték a Linuxot és a Macintosht](#), emiatt a böngészés közben az automatikusan lefutó JavaScript kódok Debianon és OS X-en is ugyanúgy felrajzolták a Windows .EXE kártevőket "észlelő" ablakokat, mint Microsoft Windows alatt :-)



Annyi különbség viszont mégis elmondható, hogy míg a klasszikus vírusok ellen csak az antivírus csomagok futtatása, és [persze a biztonságtudatosság](#) (nem kattintunk mindenre, nem telepítünk akármit) a fő védelmi lehetőség, addig a scriptes kártevők támadásai ellen az előbbieket mellé azért tehetünk még további extra módszereket. Ilyen lehetőség például egy [biztonságosabb böngésző kliens](#) használata, vagy olyan internet security csomag választása, amely már böngészés közbeni védelmet is biztosít.



De ugyanígy [figyelhetünk az alapértelmezett Adobe Reader beállításokra](#) - Protected View kiválasztása, és ne legyen default a **JavaScriptek** futtatása - illetve választhatunk valamilyen alternatív PDF megjelenítőt is. Sőt visszatérve az internetezésre például olyan, a scripteket menet közben blokkolni képes böngésző kiegészítők telepítése és használata is rengeteget segíthet ez ügyben, [mint amilyen a NoScript](#).

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Újra itt van a proxy-s Javascriptes kártevő](#)
[Önök kérték, mi teljesítjük I.](#)
[Nézzünk a forrásba!](#)
[Védtelenül hagyja a bootoló PC-t a 2009-es Norton](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6559383>

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.

Hogyan NEM nyerünk majd iPhone 6-ot?

2014.08.04. 09:57 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam facebook átverés nyeremény esély 99.9% iphone6](#)

Bár az iPhone 6 hivatalos megjelenésének időpontja kicsit még odébb van - [ez állítólag 2014. október 14. lesz majd](#) - addig is a felfokozott várakozás és az ingyen nyeremények iránti gyermekien naiv, olthatatlan vágyakozás kielégítésére máris megjelentek az ilyen témájú hiánypótló átverések a Facebook oldalán.



Ha valaki ingyen kaphat valamit, mániákusan hinni akar benne, hogy ez igaz, legyen az [Bill Gates ingyen lottó keretében](#) elosztogatott vagyonkája, ingyen [Rolling Stones koncert](#) belépőjegy, örökös nélkül elhunyt [gazdag afrikai állítólagos rokon](#) vagy éppen egy potom [1000 dolláros Victoria's Secret ajándékutalvány](#). Ilyenkor az agyak hátramenetbe kapcsolnak, és a lehetetlen is sokak számára hihetővé válik. Háttha, talán most és mi van ha tényleg. Pedig ahogy sem ingyen ebéd, sem pedig a [korábban keringő legendák szerinti ingyen nyerhető iPhone 5](#) nem létezik, úgy ez a mostani ingyen iPhone 6 is sokak bánatára sajnos ordas nagy kamu.



Nézzük akkor ezek után a mostani részleteket. Ingyen, azaz egy lájk segítségével nyerhető iPhone 6, ugyanis [állítólag egy nagyobb mennyiséget ajánlottak, amit majd augusztus 31-én fognak a lájkolók között kiosztani](#), na persze tök hihető a történet. **A teendő ugyanis semmi más, mint 1. lájkolni, 2. beírni, milyen színűt szeretnénk, és 3. megosztani a falunkon.** Aki pedig ezek után még kattint is rá, az biztos, hogy a fent emlegetett posztokat nem olvasta. A szívárvány minden színében pompázó ajánlat egyébként sem ismeretlen elem a rutinos olvasóknak, hiszen például [a színes Facebook oldal is hasonló szemkápráztató trükkkel próbálja átverni a felhasználókat körülbelül negyedévente](#). Szóval az állítólagos nyereshez nem kell más, osszuk meg és nyerünk.



Valószínűleg nem olvashatta a csalás készítője Prékopa András: Valószínűségszámítás című alapkönyvét, mert az ingyen, azaz egy lájk segítségével nyerhető iPhone 6 esélyeinél rögtön ezt írja: "1 like = 99.9% to Win". Ilyen esélyű játék nem létezik, mert a szervező azonnal csődbe menne. De ha valaki veszi a fáradságot, és eltűnődik-számolgat, eleve képtelenség, hogy ha csak 500 darab iPhone 6-ost adnak ingyen, akkor hogyan lehetne 28,807 lájkoló esetében is 99.9% esély a nyeresre. Még ha nem is nőne tovább ezek száma - ami valószínűtlen egy ilyen remekbe szabott és megbízható ajánlatnál ;-) - már akkor is biztosan marad 28,307 csalódott iPhontalan kuncsaft.

De ha már számolunk, elhiszi valaki, hogy 500 darab szorozva kb. 200 ezer azaz cirka 100 millió forintot csak úgy a vakvilágba elosztogat manapság valaki? Ez egyáltalán nem tűnik életszerűnek. Emellett utána néztünk, és időközben látszólag számtalan "winiphone6.com" és hasonló hangzású domain tömkelegét foglalták már le a trükkös csalók.



Összegzésül, nézzünk szembe a jéghideg rögválósággal, és mindig gondolkodjunk józanul, még akkor is, ha valamilyen extrém kedvező ajánlatot látunk. Nem, még mindig nincsen ingyen ebéd, ahogy erről már sokszor és sokat beszéltünk korábban. Ahogyan sajnos ingyen iPhone 6 sem várható belátható időn belül egyetlen megosztásért cserébe. Nem véletlenül szerepel az iPhone-ok árcéduláin 200 ezer feletti ár, hiszen senki nem vásárolna ilyen ennyi pénzért, ha közben meg über primitív lájkolgatásért ingyen is meg lehetne kapni. Welcome back to Reality!

Tetszik 18 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pinit** **+1**

Ajánlott bejegyzések:

[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Ismét nyertünk 450.000 eurót :-\)](#)
[Itt a foci VB, jönnek az átverések is](#)
[A Facebook nevében](#)
[Facebook átverés - haladó csoport](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6572005>

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](#).

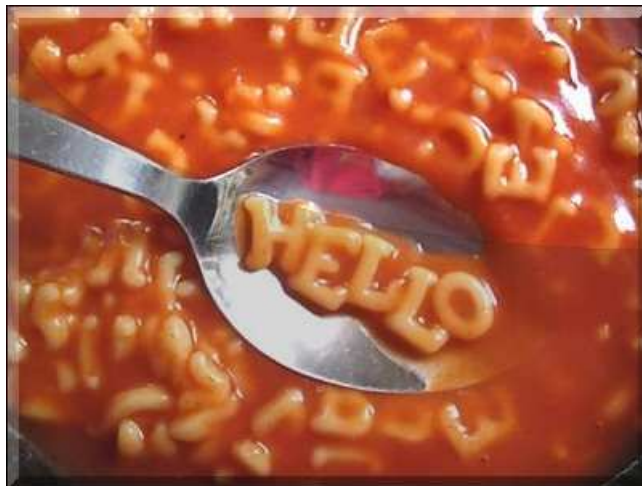
Nincsenek hozzászólások.

Kiszivárgott jelszavak - ránk váró teendők

2014.08.06. 13:46 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [jelszó](#) [cnet](#) [mozilla](#) [hash](#) [rendszeres](#) [jelszócsere](#) [salted](#)

Lassan tényleg odáig fajul a helyzet, hogy ha csak óvatlanul pislant egyet az ember, közben is éppen kikerülnek valahonnan a személyes adataink, jelszavaink. [Hol egy Target áruházlánc](#), [hol egy Domino Pizza](#), [hol egy Adobe](#) vagy most [éppen a CNET](#) és a Mozilla áll a szőnyeg szélén a kikerült jelszavak miatt.

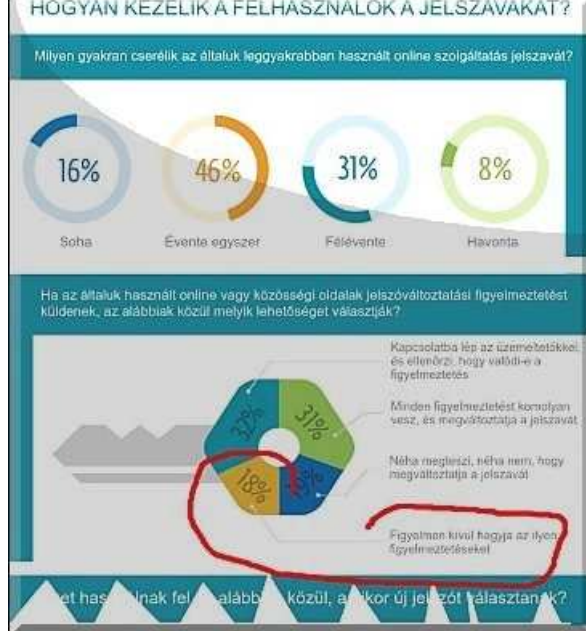


Nemrég derült fény arra, hogy a Mozilla fejlesztői hálózatába korábban beregisztrált 76 ezer személy adata, például e-mail címe és körülbelül 4000 jelszó hash lenyomat egy incidens folytán illetéktelen kezekbe kerülhetett. [Az Ars Technika szerint](#) salted hash alkalmazásával készült jelszavakról van szó. Stormy Peters, a Mozilla igazgatója [augusztus 1-én egy blogbejegyzésben írt arról](#), hogy egy részletes adatokat tartalmazó adatbázis dump június 23-án véletlenül kerülhetett fel a kiszolgálójukra, és nagyjából egy hónapon keresztül volt elérhető, mire észrevették. Elmondása szerint nem észleltek illetéktelen behatolást ezen a szerveren, de ez ugye nem jelenti azt, hogy ilyesmi nem is történhetett, emiatt jelszócserere figyelmeztették a felhasználóikat.



Hogy manapság milyen mértékű is a jelszavak ipari lopása, arra jól rámutat az a nemrég leleplezett közép-orosz illetőségű jelszó tolvaj hálózat, ahol [420 ezer weboldalról származó 1.2 milliárd rekordot tartalmazó felhasználói adatbázist találtak](#) a hatóságok. A banda egy tízfős, fiatal férfiakból álló szervezet, akik kis csapatokban, jól összedolgozva elosztották egymás közt a feladatokat, a kártevők terjesztésétől, a botnetek használatától kezdve egészen a jelszóadatok precíz begyűjtéséig.

Nyilván ezek az eredmények elképesztőek, de azért tegyük gyorsan hozzá, hogy mindez semmiképp menti fel az olyan üzemeltetőket és szolgáltatókat, akik még ma sem használnak salted hasht, vagy éppen horror clear textben tárolják az azonosítóinkat.



Egyszer már pedánsan [összefoglaltuk azokat az azonnali teendőket, lépéseket, amiket a valós vagy félt kiszivárgások után elvégezni érdemes](#), így ezeket most nem is ismételjük meg részletesen. Ám a 2010-es poszthoz képes valószínűleg már mindenki érzi, hogy a jelszó rendszeres cseréje, [valamint annak erőssége és egyedisége](#) mennyire fontos kulcskérdéssé nőtte ki magát az idők folyamán. Egyszerűen el kell fogadnunk, hogy a nyilvánosságra kerülő hasonló temérdek incidens ránk is ró teendőket ezzel kapcsolatban. Ami természetesen nem csak a fentieket jelenti, hanem akár azt is, hogy [szemben a 2010-ben mért 18% aránnyal](#) mi semmiképp ne hagyjuk figyelmen kívül a jelzést, ha az általunk használt online vagy közösségi oldal jelszócsereire figyelmeztető üzenetet küld.

Tetszik 4 személy kedveli ezt [Regisztrálg](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [G+1](#)

Ajánlott bejegyzések:

[Munkavállalói adatok szivárogtak az Nvidiatól](#)
[A CNET-nek is reszeltek](#)
[Tudom mit adtál meg jelszónak tavaly](#)
[Lopott Minecraft jelszavak szivárogtak ki](#)
[Twitter bejelentkezés másképpen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6578911>

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](#).

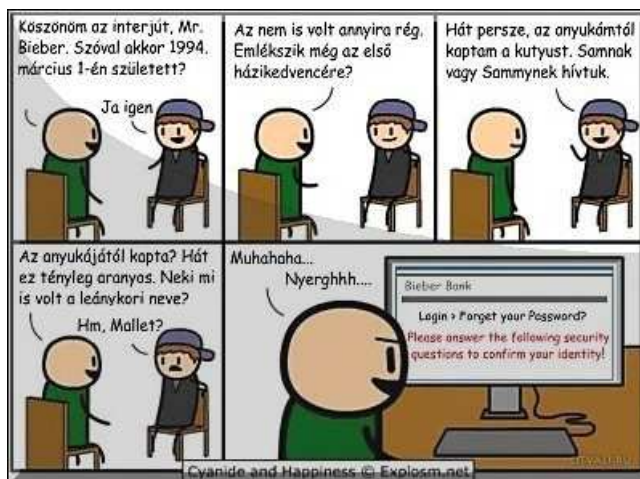
Nincsenek hozzászólások.

Az a bizonyos emberi tényező

2014.08.08. 11:49 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [social figyelmetlenség](#) [emberi justin megtevesztés](#) [palin sarah engineering tényező](#) [bieber közlékenység](#)

Időnként visszatérő témánk ez, hiszen a **legjobb technikai felszereltség és a leghatékonyabb védelmi programok használata mellett is utat ad a támadóknak a túlzott naivság, figyelmetlenség, vagy hiszékenység.** El kell fogadni, hogy a biztonságtudatosság még inkább lényegi elem lett, ahogy azt is, hogy a statisztikák szerint az informatikai incidensek egy jelentős részében emberi hiba, szándékos károkozás vagy mulasztás történik.



Ezt a jó kis Cyanide kockát nézve talán sikerül szemléletesen bemutatni, hogy személyesen, e-mailben, de főként a közösségi oldalakon milyen hátrányt jelent a túlzott közlékenység. **Emlékezhetünk például arra a nevezetes social engineering esetre is, amelynél 2008-ban Sarah Palin Yahoo! alatti levelezését tudta feltörni a támadó. Mit használt ehhez? Úrtechnológiát? Ehhh. Alvilági chatszobákban vásárolt drága exploit kité? Dehogy. Csak az eszt, ahogy annak idején Kevin Mitnick is.**

A módszer nem feltörés, nem jelszó találgatás volt, hanem egyszerűen új jelszó igénylése. A születési hely és idő megszerzése nem okozott neki semmilyen gondot, [a titkos ellenőrző kérdés pedig az volt, hol ismerkedtek meg annak idején a férjével.](#) "Természetesen" ez is ki Googlízható volt, mert Palin erről is beszélt már a nyilvánosság előtt - ez pedig egy középiskola neve volt.



A PEBKAC, a Problem Exists Between Keyboard And Chair rengetegszer tud problémákat okozni, gondoljunk csak [a legutóbbi Mozillás szerveren jó egy hónapig fent felejtett SQL adatbázis dump](#)ra.

De az is egy szemléletes példa volt, amikor egy magyar cég egy támadás nyomai miatt soron kívül etikus hackerekkel végeztetett vizsgálatot, majd az audit után a támadást lehetővé tevő hiba ellen javasolt javítást elvégezve **hátradőlvén a karosszékekben arra számított, mostantól megszűnnek a korábbi adatlopások.** Ám 1-2 hónappal később újra megismétlődött ugyanaz a biztonsági esemény, amire mindenki nagyon ideges lett. Végül aztán kiderült, a javasolt javítást mégsem végezték el, mert a cég helyi programozója véletlenül kikommentezve hagyta azt a kódban, így az nem is védhetett.



Ha alaposan végiggondoljuk, **senki sem védett egy alaposan megkonstruált és precízen testreszabott megtévesztés ellen, ezt talán jól demonstrálta a 2013-as New York Times szerkesztősége ellen végrehajtott adatlopás.** Kínai hackerek ehhez az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége) és az USA közötti kereskedelmi kapcsolatokkal kapcsolatos egyezmény tervezetét használták fel csalinak. Nagy számú magánszemélynek és ügynökségnek küldték szét azokat az e-maileket, akiket ez a bizonyos szakmai téma érdekelhetett - köztük a szerkesztőség újságíróinak is - és ez sikeresen fel is keltette az általuk kiszemelt célpont érdeklődését.

Természetesen ezek rosszindulatú hivatkozást tartalmazták, és ezzel elérték, hogy rákattintsanak, majd [a történet végét már ismerjük: több hónapig rejtve futott egy kémprogram a szerkesztőség gépein, amit aztán csak három hónappal később, 2013. decemberében vettek észre.](#)



De ennek ellenére, mert emberből vagyunk, nem kell bedobni a lovak közé a gyeplőt azzal, hogy kár vigyázni. [Érdemes küzdeni - sőt a munkaadónk ezt el is várja](#) - és tanulni, odafigyelni, nyomon követni az aktuális csalási formákat, hogy legalább ne egy [überprimitív trükkön vérezzünk el.](#) Erre pedig tulajdonképpen mindenki képes (lenne) [némi kis erőfeszítés és állandó odafigyelés, folyamatos gondolkodás árán.](#) És persze emiatt (lenne) lényeges a dolgozók rendszeres biztonságtudatossági képzése is.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A Justin Bieber átverés](#)
[Hamis rendszerüzenetek II.](#)
[A social engineering 1000 arca](#)
[Kormányzati e-mailek kontra biztonság](#)
[Újabb adathalász kísérlet a Yahoo! ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6587597>

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.

Júliusi vírustoplista

2014.08.18. 10:42 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [radar](#) [adatok](#) [július](#) [nod32](#) [havi](#) [report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. júliusában a következő 10 károkozó terjedt a legnagyobb számban.



Az előző havi eredményekhez képest továbbra is a mentéseket törő Win32/Bundpil féreg vezeti a mezőnyt lassan tizedik hónapja. Megszívlelendő tanács ezzel kapcsolatban, hogy a saját munkák rendszeres külső adathordozóra készülő mentését sose hanyagoljuk el, hiszen a legjobb stratégia a megelőzés. A hatékony védelem érdekében az is lényeges, hogy ne csak egyetlen backup példánnyal, hanem párhuzamosan több különböző verziójú mentéssel is rendelkezünk.

Második helyen maradt az előző hónapban felbukkant JS/Kryptik trójai. Ez egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlaná összezavart JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját.



Harmadik helyre küzdötte fel magát az újonc Win32/RiskWare.NetFilter, melynek segítségével megfertőzhetik a számítógépünket, illetve a kompromittált rendszert később távolról is irányíthatóvá teszik. A távoli támadás során tipikusan adatokat lopnak el így a megfertőzött gépről, illetve távoli utasítások segítségével további kártékony kódokat telepítenek fel rá. Emellett **hetedik helyen szintén új szereplőt találunk a Win32/Adware.MultiPlug** személyében. Ez egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kéretlen reklámokat jelenít meg az internetes böngészés közben.

Végül a **tizedik helyezett Win32/TrojanDownloader.Zurgop** is egy új kártevő a listánkon. Róla röviden annyit érdemes tudni, hogy a Zurgop kártevő család olyan rosszindulatú kódokat hordoz, amelyek a megfertőzött rendszereken aztán további kártékony programok letöltését okozza. Az antivírusok felismerésének elkerülése miatt olyan különféle futásidejű tömörítési technikákkal próbál rejtőzködni, mint például a PEncrypt vagy PECompact.



Az ESET Radar Report e havi kiadásában ezúttal egy egészen rendkívüli esetről volt szó. A világ egyik legnagyobb ételkiszállító rendszerét, a Domino Pizza-t feltörő Rex Mundi hackercsoport váltságdíjat követelt a tulajdonosoktól. Fenyegetésük szerint amennyiben négy napon belül nem kapják meg a 30 ezer eurós összeget, úgy a megszerzett mintegy 600 ezer, elsősorban francia és részben belga ügyfél személyes adatát nyilvánosságra hozzák.

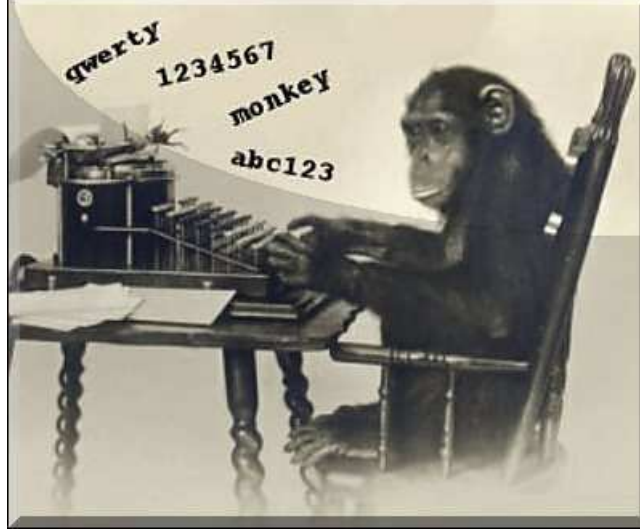
Elsőre sokaknak talán kicsit viccesen hangzik, hogy az az információ, kinek mi a kedvenc pizzája, túsul ejthető, **de ne felejtjük el, hogy emellett a teljes név, a lakcím, az ügyfelek telefonszáma, e-mail címe, valamint jelszava, és a részletes rendelési információk is illetéktelen kezekbe kerültek.** Bár a beszámolók szerint a francia és belga ügyfeleken kívül más ország felhasználóinak adatai állítólag biztonságban voltak, de egyfelől egy ilyen nagy nyilvánosságot kapó incidens erősen ronthatja egy ilyen vállalkozás hírnevét.

Másfelől pedig nem lehetünk abban sem biztosak, hogy valóban megfelelően kezelték a személyes adatainkat, például a jelszavakat sima szöveggént vagy annak csak a hash-ét tárolták, **nem tudjuk használták-e sózást (salted hash) annak elkerülése érdekében, hogy a szivárványtáblákkal történő egyszerű visszafejtést megakadályozzák.** Érdekes módon ezt a plusz biztonsági elemet a LinkedIn is csak a 2012-es feltörése után vezette be a jelszavak hash értének kódolt tárolásánál.

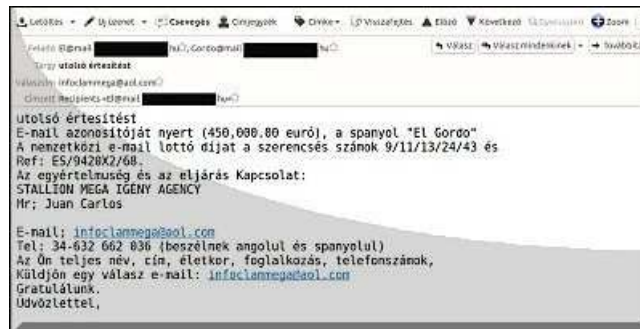


Nagyon fontos, hogy aki bármilyen hasonló incidensben érintett lesz, **az a jelszavát haladéktalanul változtassa meg. Emellett lényeges még, hogy ugyanazt a jelszót sose használjuk több helyen, illetve a jelszavunk ne legyen túl szimpla.** Ez amiatt fontos, mert a kiszivárgott jelszó hashek elsősorban az egyszerűbb, rövidebb jelszavak tulajdonosaira jelentenek kiemelt veszélyt, hiszen azok villámgyorsan visszafejthetők.

Azt sem szabad elfelejteni, hogy **egy-egy ilyen feltörés után gyakori forgató könyv az is, hogy ismeretlenek olyan e-mail kampányokat indítanak látszólag az érintett cég nevében az ügyfelek felé, melyben jóvátételként törzsvásárlói tagságot, hűségesek ügyfeleknek szánt ajándékot ajánlanak fel** vagy éppen biztonsági figyelmeztetést küldenek, ám a levél valamilyen kártevőre mutató link hivatkozást vagy fertőzött mellékletet tartalmaz.



Júliusi fontosabb blogposztjaink között **beszámoltunk egy olyan e-mailes átverésről, amelyben arról tájékoztatnak bennünket, hogy állítólag 450,000 eurót nyertünk a nemzetközi e-mail lottó díjjal.** Remélhetőleg nem csak a helyesírási hibák, de a hihetetlen és képtelen ingyen nyereményekről szóló történeteket már mindenki értékén kezeli, és nem dől be a személyes adatok begyűjtésére vagy kártevőterjesztésre specializálódott elkövetők trükkjeinek.



Helyet kapott havi válogatásunkban egy, **célzottan a kisvállalkozásoknak szánt biztonsági összefoglaló** is. Nincs mindenki tisztában azzal, hogy a kis és közepes vállalatok, vállalkozások biztonsága mennyire kulcsfontosságú és kritikus terület, **pedig a kiemelt nagyobb célpontok elleni kibertámadások esetében először legtöbbször a gyengébben védett beszállítói kört, és az alvállalkozókat szokták támadni ugródeszkaként, és onnan lépnek tovább.**



A dolgok internetéről manapság sokat hallunk, és a gyors fejlesztések gyakran hagynak a szoftverekben lehetséges gyenge-pontokat a szakképzett támadónak. Ezúttal **egy okostelefonról szabályozható izzóról derült ki az, hogy kihasználható kritikus hibát** tartalmaz. A biztonsági kutatók saját üzenetsomagokat is be tudtak injektálni a rendszerbe, ezzel pedig a beállításokat tetszés szerint úgy tudták megváltoztatni, hogy ahhoz semmilyen előzetes hitelesítés nem kellett, illetve ezekről a manipulációkról semmilyen riasztás, figyelmeztetés nem keletkezett. **A gyártó az etikus hacker szakemberekkel együttműködve adott ki soron kívüli javítást, amely bezárta a sebezhetőséget.**



Július közepén "elesett" a népszerű technológiai hírek és vélemények weblapja, a [CNET is](#), és ezzel körülbelül 1 millió felhasználói jelszó került veszélybe. A CNET megerősítette a feltörés tényét, így mindenkinek a gyors jelszócsere segíthetett a helyzet normalizálásában. Érdekes módon a W0rm nevű orosz hacker csapat 1 Bitcoin (körülbelül 130 ezer forint) váltságdíjat kért azért, hogy az ilyen helyzetek elkerülését szolgáló biztonsági tanácsokkal szolgáljon a hírportál részére.



Értesülhettünk arról is, hogy [az FBI külön figyelmeztetést adott ki a botnettel fertőzött számítógépek számának erőteljes emelkedése miatt](#). A beszélő számok tanúsága szerint évi több, mint 500 millió számítógépet fertőznek meg a botnetek, ami másodpercenként 18 kompromittált gépnek felel meg, emiatt fontos a hatékony védekezés, és az elavult Windows XP rendszer mihamarabbi lecserélése.



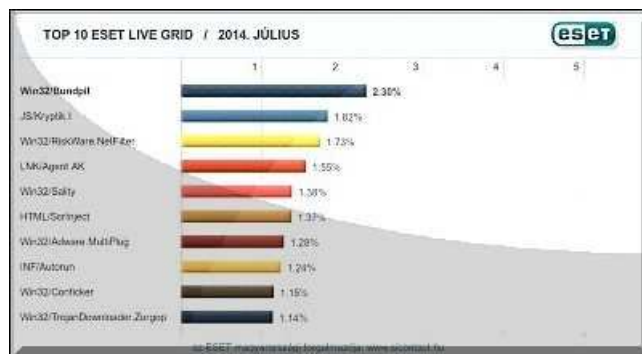
Végül arról is írtunk, hogy [visszatért az androidon futó váltságdíjas titkosító kártevő](#). Az első verziós, és sok tekintetben még kísérleti változathoz képest ezúttal már titkosítja az olyan archív fájlokat is, mint a ZIP, 7z és RAR, emiatt a helyi mentéseink is elveszhetnek, ha azok nem voltak kimásolva külső adathordozóra is. Az új verzió immár jóval több pénzt is követel az áldozatoktól - 300 amerikai dollárt - ami több, mint a tízszerese a korábbi fejpénznek.

Bár nem lehet elégszer hangsúlyozni, hogy a megelőzés a legfontosabb feladat, szerencsére [az ESET elkészített egy SimplLocker Decryptor](#) nevű alkalmazást, amely a bajba jutott felhasználóknak segít biztonságosan helyreállítani és olvasható, használható formában visszanyerni a kártevő által elkódolt, titkosított állományait.



Vírstoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2014. júliusában a következő 10 károkozó terjedt világszerte a legnagyobb számban, és volt együttesen felelős az összes fertőzés 14.96%-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.



01. Win32/Bundpil féreg

Elterjedtsége a júliusi fertőzések között: 2.30%

Működés: A Win32/Bundpil féreg hordozható külső adathordozókra 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.

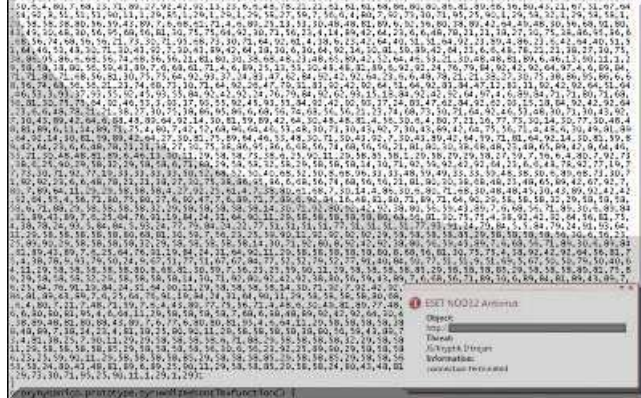


Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description

02. JS/Kryptik trójai

Elterjedtsége a júliusi fertőzések között: 1.81%

Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlan összezárt JavaScript kódoknak, amely a különféle HTML oldalakra rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját.



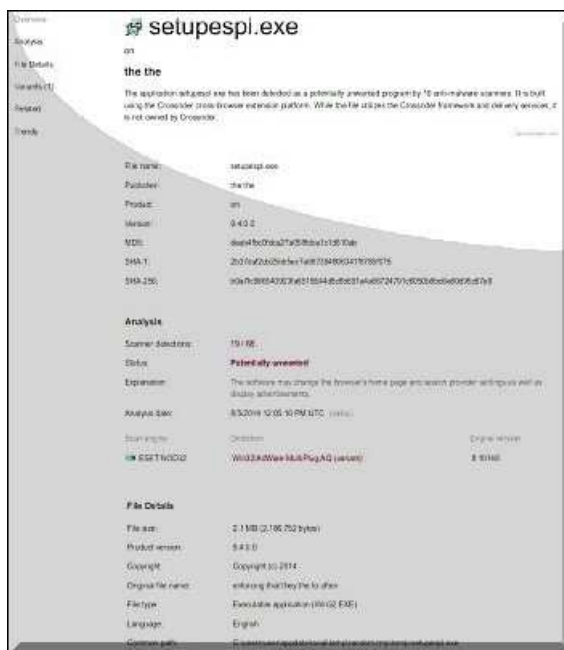
Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail



03. Win32/RiskWare.NetFilter riskware

Elterjedtsége a júliusi fertőzések között: 1.73%

Működés: A Win32/RiskWare.NetFilter egy olyan alkalmazás, amely magában hordoz olyan rosszindulatú kódokat, amelyek segítségével megfertőzhetik a számítógépünket, illetve a kompromittált rendszert később távolról is irányíthatóvá teszik. A távoli támadás során tipikusan adatokat lopnak el így a megfertőzött gépről, illetve távoli utasítások segítségével további kártékony kódokat telepítenek fel rá.



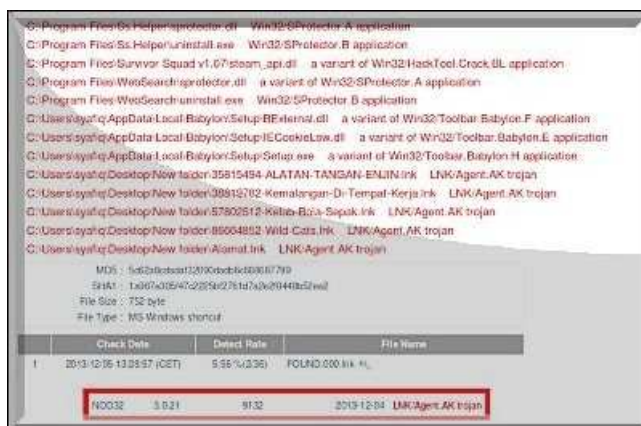
Bővebb információ: http://www.virusradar.com/en/Win32_RiskWare.NetFilter.A/description



04. LNK/Agent trójai

Elterjedtsége a júliusi fertőzések között: 1.55%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasításokat generáljon, 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. Vírusselemlzők 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



05. Win32/Sality vírus

Elterjedtsége a júliusi fertőzések között: 1.38%

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.



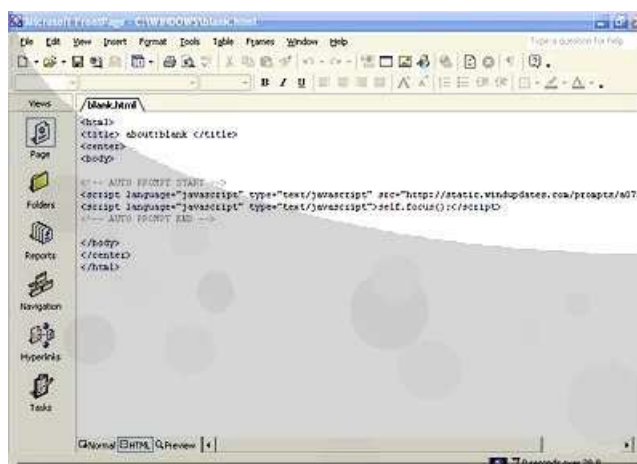
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



06. HTML/ScrInject trójai

Elterjedtsége a júliusi fertőzések között: 1.37%

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.



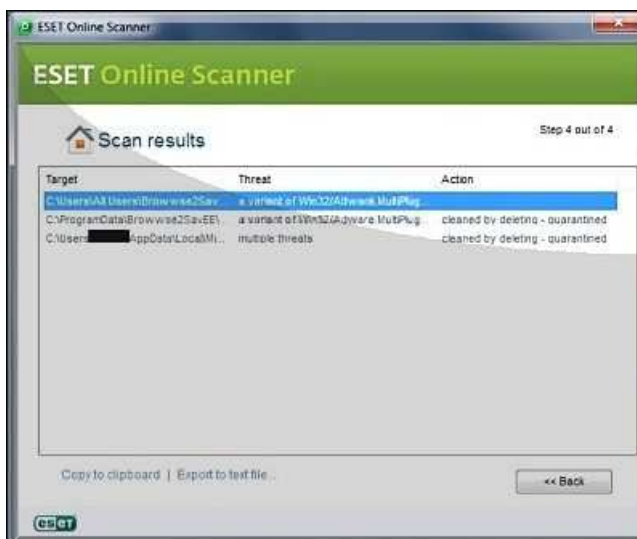
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scrinject-b-gen>



07. Win32/Adware.MultiPlug adware

Elterjedtsége a júliusi fertőzések között: 1.28%

Működés: A Win32/Adware.MultiPlug egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kényszerű reklámokat jelenít meg az internetes böngészés közben.



Elterjedtsége a júliusi fertőzések között: 1.24%

[illegible]

Elterjedtsége a júliusi fertőzések között: 1.15%

[illegible]

Elterjedtsége a júliusi fertőzések között: 1.14%

Installation

When executed, the trojan copies itself into the following location:

```
%appdata%\%variable2%\variable3.exe
```

In order to be executed on every system start, the trojan sets the following Registry entries:

```
reg add  
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]  
"variable1" = "%appdata%\%variable2%\variable1.exe"  
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run]  
"variable1" = "%appdata%\%variable2%\variable1.exe"  
reg add
```

A string with variable content is used instead of %variable1-%3.

The trojan may create the following files:

```
%startup%\%variable2%.lnk
```

The file is shortcut to a malicious file.

Bővebb információ: http://www.virusradar.com/en/Win32_TrojanDownloader.Zurgop.BI/description

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[A HTML trójaiak riogattak minket októberben](#)

[Végre kiesett a Conficker féreg](#)

[Vírustoplista 2014. augusztus hónap](#)

[Júniusi vírustoplista](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6612323>

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.

Robin Williams utolsó telefonhívása. Vagy mégsem?

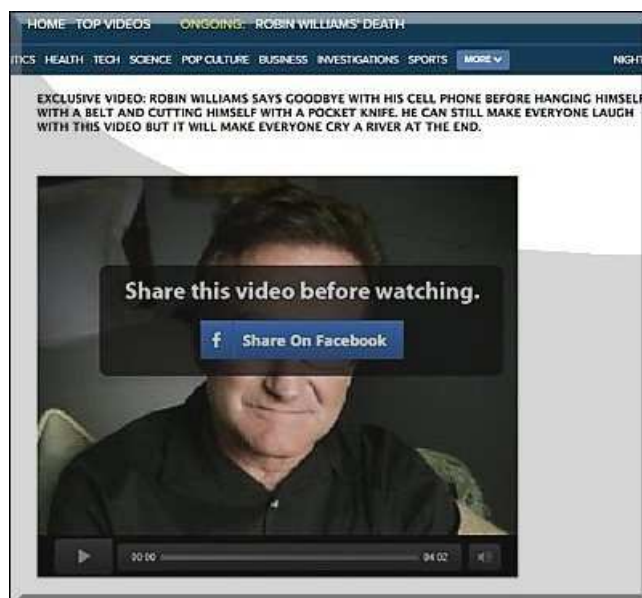
2014.08.19. 13:29 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [videó facebook](#) [öngyilkosság](#) [vagy williams utolsó átverés megosztás előre mégsem robin telefonhívás lájkolás](#)

Nem váratott magára sokáig a következő Facebook-on terjedő átverés, amelynél az elkövetők valóban mint "vérszagra gyűlő éji vad", itt sem ismernek kegyelmet, illetet vagy tiszteletet. [A júniusban történt Michael Schumacher hamis halálhírével](#) kattintásokat gyűjtő átverés után most egy Robin Williams utolsó telefonhívását bemutató állítólagos videó terjed a közösségi oldalon.



Mostani történetünkben a csalók arra hivatkoznak, hogy Robin Williams utolsó telefonhívását bemutató videót láthatunk, de előtte hogy megnézhessük, meg kellene osztanunk a hivatkozást: "Share this video before watching". A szövegben azt írják, a színész híresség mobil telefonján készült öngyilkosság előtti búcsúját lehet majd látni, mielőtt felakasztotta volna magát.



Valójában azonban ilyenkor [az ígért videók helyett internetes űrlapok kitöltögetésével foglalkozó weboldalakon találjuk magunkat](#), vagy kártevőket próbálnak a gépünkre feltelepíteni a csalók. Jelen esetben úgynevezett "Age Verification", azaz életkor ellenőrzés címén próbálnak meg előtte állítólagos ingyen nyeremény iPaddal vagy iPhone-nal kecsegtetve különféle űrlapkitöltögetésekre rávenni bennünket.



Sajnálatos, hogy sokan ennyire nincsenek tekintettel az elhunytak hozzátartozóira és mások baján, nyomorúságán igyekeznek ilyen szármalasan pitiáner kattintásvadász módszerekkel pénzt keresni. **Mi mindenesetre úgy vigyázhatunk, hogy olyan szenzációt ígérő videóra, amely csak előre lájkolás vagy előre megosztás után tekinthető meg, sosem kattintunk.**

Ne felejtsük el, ezzel az óvatossággal nem csak saját magunkra vigyázunk, hanem a közösségi oldalon velünk kapcsolatban álló családtagjainkat, barátainkat, és ismerőseinket is megvédjük a felesleges kockázatoktól, átverésektől. Ha meg is osztunk valamit az ismerőseinkkel, az csak olyan megbízható tartalom legyen, amit már előtte a saját szemünkkel láttunk, valamint amit hitelesnek és veszélytelennek találtunk.



Érdekes mellékszál, hogy egy utolsó videó felvétel valóban létezik a YouTube-on, amit állítólag tényleg az öngyilkossága előtt küldött el e-mailben egy rajongójának. [Ebben egy végső stádiumában lévő rákbeteg új-zélandi lánynak küldött videóüzenetet](#), amelyet halála előtt nem sokkal rögzíthetett webkamerájával.

Ezt a felvételt azonban mindenféle [előre lájkolás és előre megosztás nélkül is bárki megtekintheti a YouTube oldalon](#), még csak belépni sem kell hozzá semmilyen közösségi oldalra, sem pedig magára a video megosztóra.

Tetszik 17 személy kedveli ezt [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr.** **Tweet** **Pint** **+1**

Ajánlott bejegyzések:

[Ingyenes Rolling Stones jegyek. Vagy mégsem?](#)
[Figyeld a kígyót! Nem semmi. Hanem átverés :-\)](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Nyerjünk 250 ezer eurót. Vagy mégsem?](#)
[Itt a kamu Look Back videó](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6617105>

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 trükkök a hamis antivírusoktól

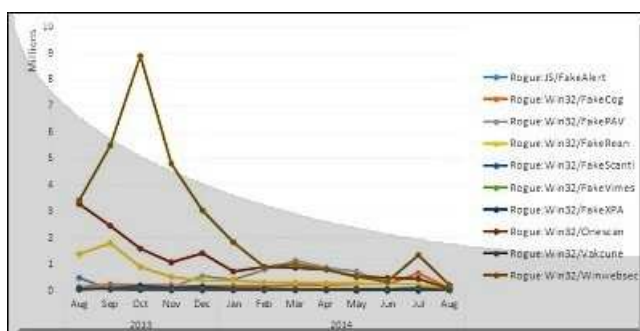
2014.08.22. 11:48 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [böngésző oldal hamis riasztás](#) [antivirus scareware](#) [blokkolás](#) [letiltott defru](#)

Bár a klasszikus ál-antivírusok sosem tűntek el teljesen, aktivitásuk az utóbbi időben jelentősen háttérbe szorult. Betudható ez az újabb [RIAA, FBI és hasonló hamis szerzőijogi, rendőrségi vagy állítólagos pedofil vádakkal kapcsolatos pénzlelőzések](#) átveréseknek, no meg [lemeztitkosítással operáló CryptoLockernek](#) és társainak. Most azonban úgy tűnik, mégis lehet egy csavarással újabb bőrt lehúzni a régi bevált hamis vírusriasztással ijesztgető módszerről.



A hamis antivírusok előfordulása a különféle mérések és statisztikák szerint tavaly október óta csökkenő tendenciát mutatott, ám most szemlátomást [visszatért](#), és [igyekszik egy kicsit még ijesztőbb lenni, mint korábban](#). Ehhez pedig nem tesz mást, mint hogy a Defrunak nevezett új kártevő megfertőzve a Windowsos gépeket figyelmeztet és [blokkolja a felhasználó által látogatott bizonyos weboldalakat](#), és éppen ezen linkek helyett jeleníti meg a szokásos hamis riasztásokat mutató ablakot.

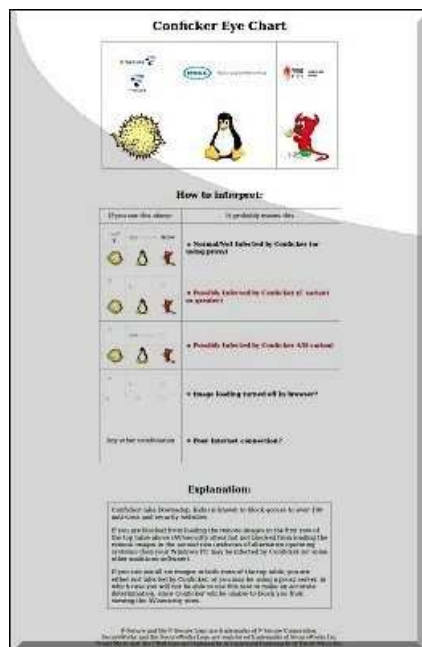


A Microsoft szerint [a friss kimutatások alapján területileg elsősorban Ázsiában fordulnak elő ilyen incidensek és ezen belül az orosz nyelvterületek is jelentősen érintettek](#), amivel a kártevőterjesztők igyekeznek újból visszahódítani és ismét felfuttatni ezt a "semmiért pénzt" zsaroló üzletágot.



Már a korábbi weboldal blokkolások is gyakran manipulálták a felhasználók gépén található "hosts" állományt, és így végezték el észrevétlenül a tiltásokat, illetve a káros linkekre való rejtett átirányításokat. Biztos sokan emlékeznek még a 2008. novemberében

felbukkant [Conficker fereg](#)re, és annak későbbi teszt ábrás oldara, ahol szemléletesen látszott a webhelyek szerinti blokkolásból a fertőzés jelenléte.



Az új, az egyes látogatott konkrét weboldalak helyett megjelenő figyelmeztetési módszer miatt a bűnözőknek sajnos gyaníthatóan megint sokakat sikerül majd becsapniuk. [A kártevő jelenleg mintegy 300 különféle weboldal helyett mutatja a PC Defendert vagy hasonló gagyi ál-antivírust.](#) Szokás szerint felajánlja a fizetés fejében való frissítés utáni mentesítést, azonban ezt most sem nem tanácsos elfogadni. Helyette inkább bízunk a valódi, kereskedelmi termékekben, illetve [az antivírus teszteken folyamatosan stabil és jó eredményt elérő](#) neves vírusirtó programokban.

 **Tetszik** Egy személy kedveli ezt. [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A hamis antivírus halott és élvezi](#)
[Hamis antivírus örökkön örökké](#)
[Öt új kiberbűnözői név az FBI listáján](#)
[Safe mód a Mechagodzilla ellen](#)
[Több ezer WordPress oldal fertőződött meg](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6625577>

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.

Védelmi tippek az iskolakezdésre

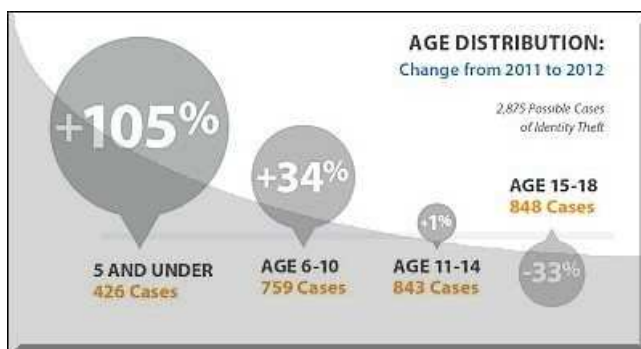
2014.08.26. 11:15 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [wifi](#) [privacy](#) [iskola](#) [privátszféra](#) [védekezés](#) [jelszavak](#) [iskolakezdés](#) [lopásvédelem](#)

Lassan vége a nyárnak, és vele a szünidőnek, ami egyúttal sok gyerek számára az iskola kezdést, illetve a folytatást is jelenti. **Érdemes lehet átismételni, mire vigyázzunk, hogy személyes adatainkat ne lophassák el, számítógépünket és mobiljainkat pedig hogyan használhatjuk a legbiztonságosabban.**



[A statisztikák szerint](#) a személyiség-, illetve adatlopási eseteknél a diákok sokkal sebezhetőbbek a felnőttekhez képest, jóval többször **lesznek áldozatok**, akár úgy is, hogy mindezt észre sem veszik. Mit tehetünk most, hogy újra vár bennünket az iskolapad, könyvtár, középiskola, egyetem, labor, vagy kollégium - ehhez adunk néhány tippet.



Első helyen [mindenképpen védjük fizikailag is a készülékünket, legyen az akár asztali gép, notebook, tablet vagy mobil](#). Ne hagyjuk őrizetlenül az osztályban, az iskola területén, de még az étkező asztalnál se. Sose hagyjuk bekapcsolva, ha nem vagyunk mellette, és ne tároljuk ezeket még rövid időre sem a gépkocsiban. Védjük mindig PIN kóddal, jelszóval a belépésünket és mindig legyen időzített automatikus zárolás is, amely meggátolja, lockolja a hozzáférést, ha más valaki próbálkozna.

A fizikai védelem emellett azt is jelenti, hogy arra is vigyázni kell, hogy a kezünkől se kaphassa ki senki, illetve sok lopásnál szaladnak el a márkás notebook táskával, aminek aztán bottal üthetjük a nyomát. Ha nem akarjuk feltűnően vinni a noteszgépünket, egy semleges kinézetű hátizsákban hordva segíthetünk ezen.



A fenti ponthoz kapcsolódva **mindig legyen rendszeres mentésünk külső adathordozón, amely egy esetleges lopás vagy elvesztés**

esetén a pótolhatatlan saját munkáinkat - például leckék, vagy diplomamunkák - megőrzi. Itt sokan hajlamosak csak a számítógépes adatokra gondolni, pedig a telefonos címjegyzékünk is tartalmaz sokszor pótolhatatlan bizonyuló adatokat. [Érdemes lehet titkosítva tárolni mind a mentéseinket, mind pedig a készülékeken a saját adatainkat.](#) Emellett [használhatunk nyomkövető alkalmazást is](#), ennek legismertebb módja az androidos mobilok esetén a készülék távolról való keresése, esetleg üzenet a tolvajnak/megtalálónak, illetve [végső esetben az eszköz távoli blokkolása, távtörlése is elvégezhető.](#)

Ugyanezt igénybevehetjük hagyományos PC esetében is, például a 6-os verziótól már lopásvédelemmel is ellátott ESET Smart Security szoftverrel is. Ennek segítségével lehetőségünk nyílik információkat nyerni az elvesztett vagy elloptott eszköz későbbi aktivitásáról, megtekinthetjük például az automatikusan készülő képernyőképeket, illetve az eszköz webkamerájával készült képeket is, [bekapcsolt WiFi esetén pedig az IP-cím alapján még az eszköz feltételezett fizikai helyét is megtudhatjuk.](#)



Az adathalászat ellen a hatékony védekezéshez saját **biztonságtudatosságunkon felül mindenképpen érdemes valamilyen internet biztonsági program használata is.** A jelszavakról már sokszor esett szó, itt most röviden csak annyit mondunk, hogy ez minden helyszínen legyen különböző és megfelelően erős - [bővebb útmutató erről a témáról itt olvasható.](#)



Ezenkívül hasznos óvatosnak lenni a publikus Wifi hálózatok használatánál. Ehhez alkalmazzunk VPN programot, de ha ezt mégsem tesszük, legalább az **étterem, kávézó, iskola, reptér, pályaudvar nyitott wifijénél sose bankoljunk, ne indítsunk innen vásárlást, és ne lépünk be a levelezésünkbe jelszóval védett accountjainkba.** Ha mégis szükséges lenne idegen gépen valahová bejelentkezni, úgy hazaérve első dolgunk legyen az idetartozó jelszavunk haladéktalan megváltoztatása.

Emellett érdemes vigyázni az iskolában közösen használt gépeknél is, ahol sosem tudhatjuk, ki ült ott előtte, ki és mit telepített fel oda, így készüljünk a **legrosszabbra.** Jobb helyeken egyébként bekapcsoláskor mindig tiszta állapot keletkezik egy lementett alap image fájl alapján, ez esetben például egy újraindítás is tisztába teheti a dolgokat.



A közösen használt gépnél használat után érdemes lehet kitörölni az előzményeket, vagy [elvégezni Privát ablakban látogatni az oldalakat, amely így \(elvileg\) nem gyűjti és tárolja el helyben a böngészési információkat.](#)

Összefoglalva bár a gyerekek, illetve fiatalok sokszor nem tulajdonítanak jelentőséget saját személyes adataik fontosságának, az incidensek tanúsága szerint a bűnözők nem válogatnak, életkortól függetlenül ellophatják személyazonosságunkat, bizalmas adatainkat. A fenti egyszerűen alkalmazható tippek betartásával viszont máris sok ezzel kapcsolatos esetleges fejfájástól kímélhetjük meg magunkat.

Ajánlott bejegyzések:

[6 tipp személyazonosságunk megvédésére](#)

[Így változtunk Snowden óta](#)

[Kormányzati e-mailek kontra biztonság](#)

[Biztonsági konferencia - nyitott wifi honeypot-tal](#)

[Kell-e aggódjunk a Regin kémprogram miatt?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6636617>

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.

Megint hamis appok a Play Store-ban

2014.08.28. 12:23 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

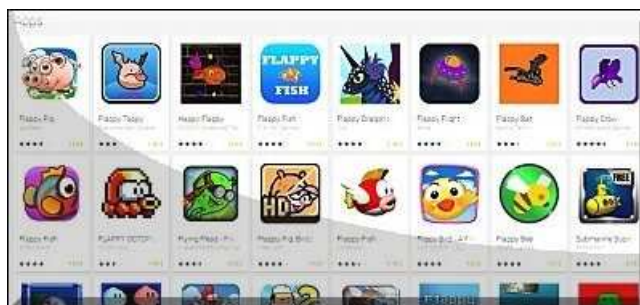
Címkék: [google](#) [nguyen](#) [klón](#) [play](#) [hamis](#) [swing](#) [android](#) [app](#) [store](#) [bird](#) [dong](#) [flappy](#) [copters](#)

A Flappy Bird klónokkal kapcsolatos biztonsági aggályokról már sokszor és sok helyen volt szó, amióta Dong Nguyen idén februárban nyilvánosan bejelentette, hogy felhagy a játék fejlesztésével. Úgy tűnik azonban, ez a terep még jó ideig tartogat további kiaknázható lehetőségeket a kártevőterjesztők számára, mert [a módszer sikeres, és a figyelmetlen felhasználók sok esetben önként és örömmel sétálnak bele](#) a hasonmások csapdáiba.



Mint emlékeztetés, a [2014. februári bejelentés után](#) ("I just cannot keep it anymore.") mind az App Store-t, mind pedig az androidos piacot előzőnlőtték a Flappy Cupido, Flappy Plane, Fly Birdie, Ironpants és hasonló nevű hasonmások. Még az Angry Birds programot fejlesztő világhírű Rovio is beszállt az örületbe, és kiadta saját Retry nevű játékát, bár ott legalább ismerjük a fejlesztők valódi kilétét, szemben a szedett-vedett noname hasonmásokkal.

Mind a Google, mind pedig az Apple deklarálta harcot hirdetett az olyan kétes alkalmazások ellen, amelyek nyilvánvaló klónjai más korábbi híres és sikeres játékoknak, illetve [amik egyértelműen a felhasználók megtévesztésére, becsapására](#) íródnak.



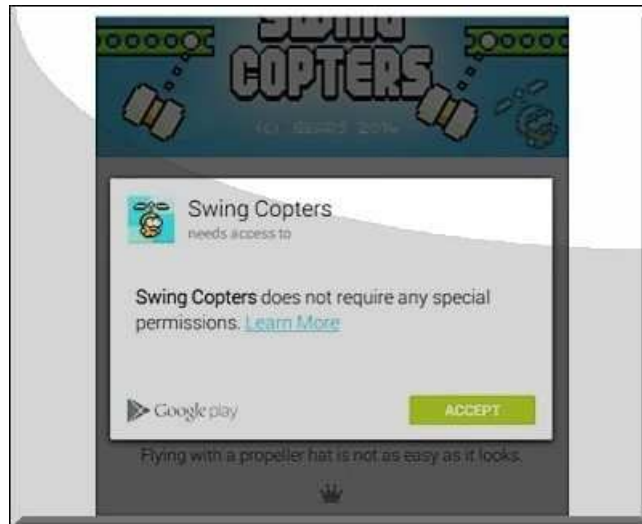
Időközben talán a "van az a pénz" jegyében vietnami fejlesztőnk mégis beadta a derekát és ismét belevetette magát a dolgok közepébe, és előállt a helikopteres ötletével. Ha most megnézzük a Swing Copters nevezetű programját, amely újra szinte a semmiből jött, de máris vagy 1-5 millió telepítést mondhat a magáénak. Nem véletlen, hogy ez a tetszetős eredmény [ismét bevonzotta a klóngyártókat, és felbukkantak a sikeres játék nevére, kinézetére hajazó kétes másolatok](#).

Vegyük azonban észre, hogy a Dong Nguyen által jegyzett eredeti Swing Copter nem tart igényt semmilyen különleges felhasználói engedélyre, szemben a többi hasonmás applikációval, amik ennél azért mindig sokkal kíváncsibbak. ("Mindenki hülye, csak én vagyok helikopter ;-)")



Egy korábbi posztunkban már pedánsan összeszedtük azokat a hasznos ismérveket, amelyek alapján mindenki elsajátíthatja, **hogyan szűrjünk ki, ismerjünk fel idejében hamis appokat**. Mindenesetre mindig legyünk óvatosak, ha egy bizonyos konkrét programot keresünk, és telepítés előtt ne csak simán az app nevét, hanem a gyártóját is ellenőrizzük.

Eközben arra sem árt figyelni, létezik-e arra a platformra egyáltalán az általunk keresett program :-) Vigyázzunk az alternatív piactereken, és bár Android alatt rendre a Google Play-t mondják a viszonylag legbiztonságosabbnak, pár napba azért itt is beletelt, mire a hasonló szemeket kitakarították.



Használjunk antivírust Androidon is, mindig csekkoljuk figyelmesen az engedélyeket, és lehetőleg ne mi legyünk az elsők, akik Unabomber módra kipróbálunk egy vadonatúj ismeretlen "Low Reputation Apps" programot, inkább várjuk meg előbb a felhasználói véleményeket, értékeléseket. Ezzel általában elkerülhetjük, hogy telefonunkon a látszólag jelentéktelen, ártalmatlan és ingyenesnek tűnő alkalmazások a háttérben súlyos pénzbe kerülő, vagy adatszivárgási következményeket okozzanak.

 Tetszik

Ajánlott bejegyzések:

[A Google Play vigyáz rám](#)
[Ingyenes ESET app az Androidos törlés ellen](#)
[Kalandok Bouncerföldén](#)
[Megjelent a Google Play-en az ESET for Android](#)
[My name is Instagram, Fake Instagram](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6644281>

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.

limchi 2014.08.29. 15:30:05

Az azért érdekes, hogy ugyan a swing copters nem kér semmi engedélyt mégis megjelenít reklámot, csatlakozni akar a play services-hez. Alapból ezekhez 3 engedély is kellene, internet elérés, fiókok kezelése, hitelesítő adatok kezelése. Csodálkozok, ha ezek nélkül is használható kódból a play services API.
Válasz erre

A CryptoWall bevétele átlépte a milliós határt

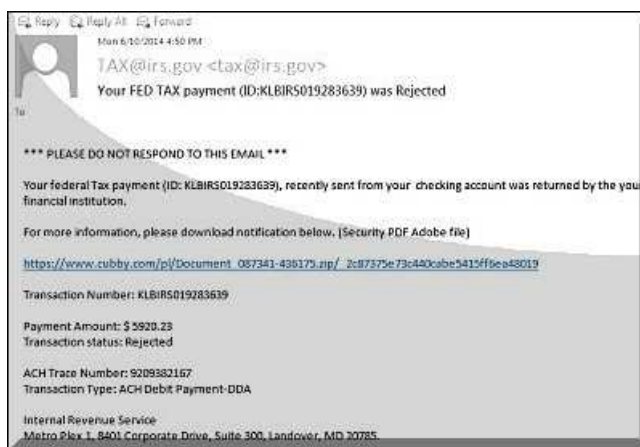
2014.09.01. 12:20 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [fejlesztés](#) [dell](#) [titkosítás](#) [tor](#) [kárttevő](#) [váltságdíj](#) [ransomware](#) [ctu](#) [cryptolocker](#) [cryptowall](#)

A CryptoLocker, CryptoWall zsaroló kártevők tavalyi megjelenésük óta ezidáig már több, mint 1 millió dollár védelmi pénzt kasszíroztak be az áldozatoktól. Minden más vásárlásnál rettenetesen örülne az ember, ha az volna odaírva: "Discount: -25%", ám itt a legkártékonyabb malware esetén emiatt valahogy mégsem tudunk önfeledten mosolyogni.

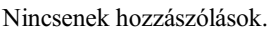


A Dell SecureWorks Counter Threat Unit (CTU, de nem 24 :-)) jelentése szerint ez a fajta kártevő végzi a legnagyobb pusztítást, [a tavaly megismert CryptoLocker](#) után a 2013. novemberében felbukkanó, majd 2014. februártól már erőteljes támadásokat végző CryptoWall hihetetlen károkat okozott már világszerte. A statisztikák szerint idén márciustól augusztus végéig bezárólag közel 625,000 számítógépes rendszert fertőzött meg, ezzel pedig több mint 5.25 milliárd fájl kódolt el olvashatatlanná és használhatatlanná téve.



A begyűjtött adatok alapján a legtöbb fertőzést láthatólag [az USA szenvedte el, ahol a világszerte regisztrált összes CryptoWall incidenses eset 40.6 százaléka történt](#), ezek jelentős részét igen [nagy valószínűséggel az angol nyelvterületeket támadó, fertőzött e-mail mellékletes Cutwail spamek okozhatják](#).

Emellett a második leggyakoribb terítési módszer pedig a böngészők javítatlan biztonsági sebezhetőségeinek kihasználása a weboldalak drive by download típusú támadásával. A fertőzött weboldalakon található Upatre nevű downloader kártevő a tapasztalatok szerint nem csak a Zeus GameOver, hanem a CryptoWall terítésében is aktív szerepet játszik, ehhez pedig [gyakran a különféle felhőszolgáltatásokon belül regisztrált, illetve már kompromittált fiókokhoz tartozó Dropbox, Mediafire vagy hasonló linkeket használ](#).



Köszönjük megrendelését!

2014.09.03. 15:33 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

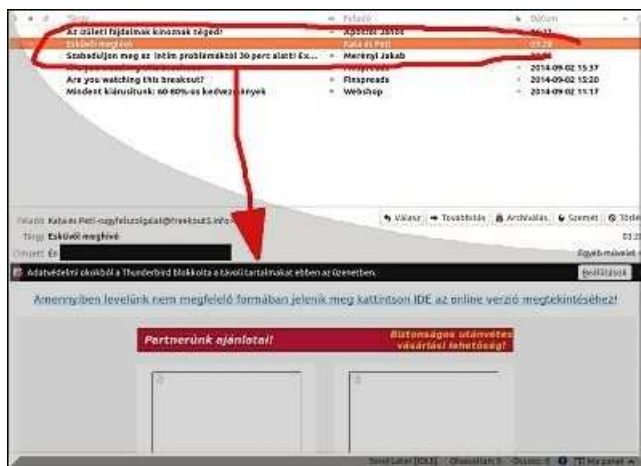
Címkék: [spam megrendelés](#) [virustotal](#) [kártékony megerősítés](#) [visszaigazolás melléklet](#)

A kártékony kódok, linkek terjesztésének rengeteg féle módja létezik. Ha csak a kéretlen üzeneteket nézzük, akkor volt itt [már csomagküldő cég PDF](#) mellékletétől kezdve a [be nem fizetett telefonszámlán](#) át egészen a [Picasa albumunkban állítólagosan megosztásra került új képekig](#) minden. Úgy tűnik azonban, ha arról kapunk levelet, hogy állítólag rendeltünk valamit, pedig ilyen nem történt, ám az üzenetben a pénz sikeres leemeléséről van szó, akkor mindenki dühösen és gondolkodás nélkül kattint.



[Nem új ez a jelenség, egyik első előfordulásánál még tavaly tavasszal](#) megemlékeztünk róla azzal a történettel, amikor az állítólagosan általunk rendelt Invicta karórával kapcsolatos visszaigazolásban látszólag a PayPal írt nekünk: "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."

Fontos, hogy ilyenkor is hideg fejjel gondolkodjunk, és a felfokozott izgalmi állapotban se kapkodjunk, vagy kattintsunk mérgesen és óvatlanul. Egyébként már a magyar nyelvű spamok is állítólagos halálhírek, látszólagos esküvői meghívók, vagy néha egyenesen "rendelésének visszaigazolása" tárgyissal érkeznek.



Azonban világosan látszik, hogy egyre gyakrabban köszön vissza a fenti trükk, valószínűsíthetően mert kiemelkedően jó kattintárát produkál. Ezúttal az [írországi képviselőnk](#) botlott bele egy ilyen akcióba, ahol szintén megrendelésnek álcázott levél érkezik a [postafiókunkba](#) a Sales Department munkatársától, Roxanne Bowdon kisasszonytól. A megrendelésünk "megerősítése" elvileg 199.18 angol fonttal - hozzávetőlegesen 78 ezer jó magyar forinttal könnytén meg a számlánkat, ahol persze maga az e-mail levéltest semmilyen támpontot vagy konkrétumot nem tartalmaz.

Így a "ki rendelt, mit rendelt, mikor rendelt" kérdésekre egyedül csak a mellékelt order_2014-09-02_09-57-58_91243513363.arj nevű állományból remélhetnénk válaszokat, ami persze mondanunk sem kell, hamis remény. Mert a melléklet természetesen nem számla, hanem kártevő, és az ESET termékei Win32/TrojanDonloader.Elenooocka néven azonosítják.



Fontos megjegyezni, hogy semmilyen kéréstlen üzenet esetén se legyünk túl hiszékenyek. Az állítólagos megrendeléseinkkel kapcsolatban pedig ne hagyjuk magunkat sem sürgetni, sem pedig felbosszantani. Sokat segíthet az is, ha [az "ismert fájl típusok rejtése" nevű idióta Windows opciót](#) az alapértelmezett rejtésről átállítjuk láthatóra, mert akkor a többszörös kiterjesztéssel trükköző - például JPG képnek álcázott, de valójában futtatható EXE - fájlra nem fogunk véletlenül rákattintani.

Másrészt az ismeretlen fájl még ekkor is **jobb, ha nem nyitjuk meg azonnal, hanem előzetesen** töltsük fel inkább az **immár magyarul is beszélő VirusTotal weboldalára**, [ahol már 50 különféle antivírus motor nézi át tüzetesen](#). Ha ezek nem találnak semmit, még ez sem jelent ugyan 100%-os garanciát, de ezzel a módszerrel azért elég hatásosan megóvhatjuk magunkat attól, hogy óvatlanul belegyalogoljunk valamilyen aktuális spamkampány kártékony víruskódjába.

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Telekom számla vagy mégsem?](#)
[Spammelés antivírus cégek nevében](#)
[Kártevő a Vodafone nevében](#)
[Adathalász levelek a Wikipedia nevében](#)
[PDF: csak megnyitom, és már indulok is...](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6665647>

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 security újratöltve

2014.09.05. 14:04 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

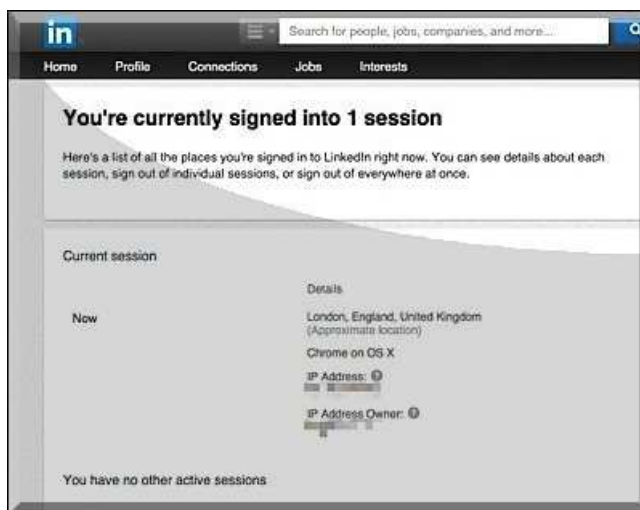
Címkék: [biztonság](#) [linkedin](#) [autentikáció](#) [welivesecurity.com](#) [2faktor](#)

Ha valaki emlékszik még a [tavalyi Linkedines adathalász akcióra](#), vagy a még ennél is hírhedtebb és kevésbé kellemes [2012-es incidensre](#), ahol 6.5 millió jelszó került illetéktelen kezekbe, annak most jó hírekkel tudunk szolgálni. Egy szerdai hivatalos blogbejegyzés ugyanis jelentős biztonsági javulásról számol be, illetve mutatja be ezek részletes használatát.

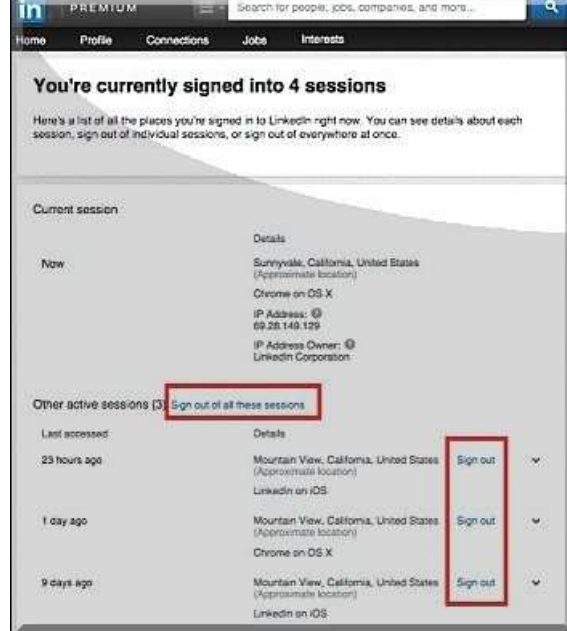


Hogy azért a 6.5 milliós múltbeli dolog mellett se menjünk el azért teljesen szó nélkül, idézzük fel ezt röviden. 2012. júniusában magát a portált támadva 6.5 millió felhasználó adata került illetéktelen kezekbe.

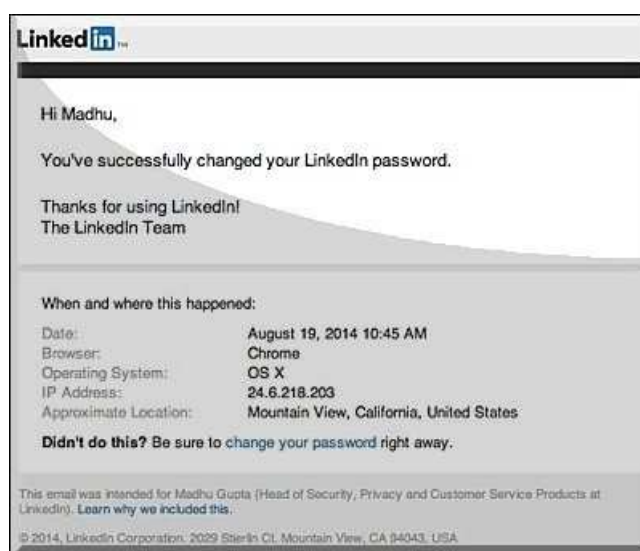
A weboldal üzemeltetői itt nem csak abban hibáztak, hogy egyáltalán megtörténhetett ez a jelszólopási incidens, hanem amint később kiderült, magánál a jelszó hashek kódolt tárolásánál az úgynevezett **SHA-1 algoritmust szimplán használva nem támaszkodtak olyan megbízható kiegészítő technikákra, mint például a jobban véletlenszerűsítő, ezáltal a feltörésnek jóval ellenállóbb úgynevezett Salted eljárás, megnövelve ezáltal a jelszó hash hosszát, és egyúttal a bonyolultságát is.** A felhasználóknak akkoriban csak a gyors jelszó csere segíthetett a tűzoltásban.



[A LinkedIn blogbejegyzésében most arról olvashatunk](#), hogy három új elemet is használhatunk a nagyobb biztonság érdekében. Az első **a bejelentkezéssel kapcsolatos kontroll**. Ha például otthonról belépünk, de nem vagyunk biztosak abban, hogy egy másik, például a munkahelyi gépünkön kijelentkeztünk-e vagy valaki megszerezte az accountunkat és a világ másik felén épp a nevünkben garázdálkodik. Ez mostantól könnyen ellenőrizhető, ha a settings beállítások közül a "click on See where you are logged in" menüpontra kattintunk.



Ha itt egzotikus országok, ismeretlen IP címek, szokatlan böngésző kliensek nevei jelennek meg, akkor gáz van, azonban a mellékelt kép ha valaki éppen Londonban dolgozik, akkor egy teljesen normál helyzetről tudósít bennünket. Arra is van lehetőség, hogy az elfelejtett kilépés vagy gyanús aktivitás miatti bejelentkezéseket távolról megszakítsuk és őket kiléptessük. **Ha ez a helyzet, akkor az azonnali jelszó csere mellett érdemes a két faktoros autentikáció lehetőségét is igénybe venni.**



Az is egy hasznos feature, hogy a **jelszóváltotatásról külön e-mailes emlékeztető értesítést lehet kérni, ki mikor, milyen böngésző, milyen operációs rendszer alól, milyen IP címről és földrajzilag nagyjából honnan kezdeményezte mindezt.**



Végül arról is tájékoztatják a felhasználókat, hogy lehetőség van a saját adataink mentésére is. **Ha ezt kezdeményezzük, akkor amint a rendszer sikeresen összegyűjtötte az adatokat, arról e-mailben kapunk értesítést és ezután belépve megkapjuk a mentéshez tartozó letöltési linket.**

Összességében, **[ahogy Graham Clueley is megfogalmazta a Welivesecurity oldalon](#)** - ezek egyike sem új technológia, ennek ellenére azért mégis jó látni, hogy a fejlesztők mostanra súlyt helyeztek a felhasználói biztonság emelésére. Már csak használnia kellene mindenkinek...

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

[Napi 160 ezer Facebook account esik el](#)
[Kormányzati e-mailek kontra biztonság](#)
[Biztonsági konferencia - nyitott wifi honeypot-tal](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Így költjük a pénzt az online vásárlásoknál](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6672599>

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](#).

Bélabácsi 2014.09.06. 10:04:38

"click on see ..."

Nem találom a settingsben sehol - se a "Profile", se a "Communications", a "Groups..." ill. az "Account" alatt sincs.

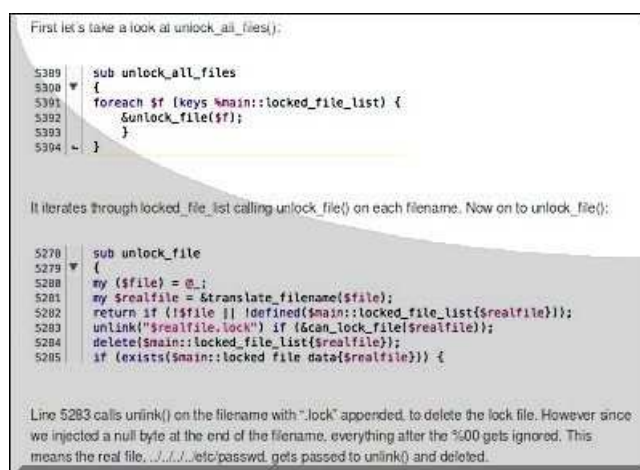
Magyarisztán még nincs aktiválva ezek szerint ?

Válasz erre

Bónuszként egy olyan payload is volt benne, amely [figyelte a dátumot, és ha az éppen október 16-a volt, akkor 5% esély volt rá, hogy a főreg a Windows mappa minden alkönyvtárát és fájliját kitörölje, így ebben az esetben a gép már nem is indult el](#). Mára pedig talál [a CryptoLocker az egyik legkellemetlenebb kártevő, amely 2048 bites egyedi RSA kulccsal titkosítja az adatainkat](#) a számítógépünkön, sőt az azon lévő csatlakoztatott meghajtókon is. A visszaállításért cserébe pedig váltságdíjat követel, emiatt a saját mentésekre létfontosságú szerep hárul.



Lehetne ezeket még napestig sorolni, hiszen a 26 év roppant hosszú idő, és mi akik a vírusokat az elejétől végigkövettük, a megtett utat hosszúnak is éreztük. Jöjjön viszont most egy aktuális érdekesség, a mai Unixos történetünkben - ami bár nem egy klasszikus Remote Code Execution, ennek ellenére itt is van károkozás - **a Webminben sikeresen lehet vele kellemetlenkedni. Ugyanis a hiba segítségével lehetőség nyílik a szerverekről bármilyen tetszőleges fájlt törölni**, akár például az etc/passwd mappából. A következményeket mindenki képzelje el maga, a mosolyunk nem őszinte, igaz, [szerencsére azóta létezik már javítás rá](#). A május 20-án megjelent 1.690-es változat már nem tartalmazza ezt a sebezhetőséget, így ha valaki eddig nem tette volna meg, annak érdemes gyorsan frissítenie.



Úgy általánosságban nézve a rengeteg exploitot ismertető oldal kapcsán nehéz eldönteni, meddig jó, hogy publikusan megosztják a részletes sebezhetőség kihasználási információkat, mert ez egyszerre hasznos - hurrá, tudunk róla, tanulunk belőle, és sokszor a fejlesztők is csak ilyenkor ébrednek és látnak neki végre a javításnak - de közben egyszerre veszélyes is, hiszen a rossz-fiúk is azonnal birtokba vehetik. **Hogy ez a későbbi támadások gyarapodása szempontjából milyen hatást vált ki, persze jó kérdés, azonban nem igazán lehet ellene tenni semmit, az ismereteket lehetetlen légmentesen elzárni.**



Az viszont biztos, hogy amikor olyan részletességű útmutatók is megjelennek a gyenge-pontok kihasználásáról, mint például a GSM hálózatokban bárki nyomkövetését lehetővé tevő SS7-es módszer kapcsán a Verint Skylock leírása, akkor ez már gyaníthatóan akaratlanul is segíti és bátoríthatja a későbbi incidenseket. És persze a harc az örök.

Tetszik [Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.](#)

Ajánlott bejegyzések:

[Sebezhető-e vagy?](#)
[Védekezés exploitok ellen](#)
[Samsung lock Oleg Pliss nyomdokain](#)
[Sokkoljon-e minket a Shellshock?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6688721>

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.

Vírstoplista 2014. augusztus hónap

2014.09.15. 11:00 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

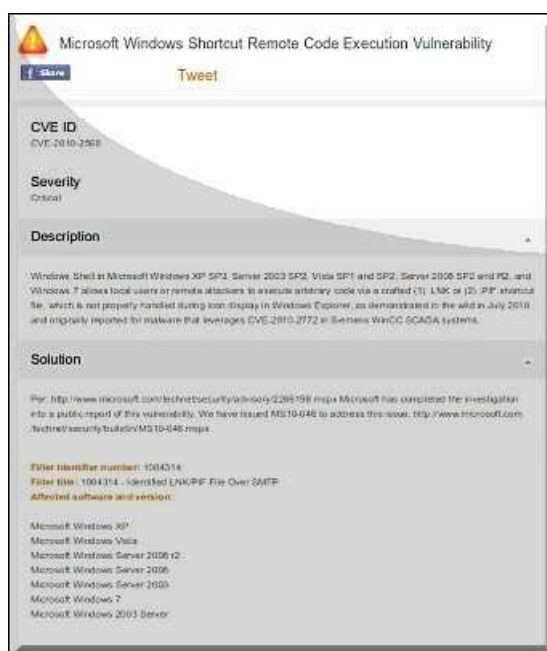
Címkék: [statisztika](#) [radar](#) [adatok](#) [augusztus](#) [nod32](#) [havi](#) [report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. augusztusában a következő 10 károkozó terjedt a legnagyobb számban.



Az előző havi eredményekhez képest **továbbra is a mentéseket törölő Win32/Bundpil féreg vezet a mezőnyt** lassan tizenegyedik hónapja. Ennek kapcsán sose felejtjük el a saját munkáink rendszeres külső adathordozóra készülő mentését, mert a legjobb stratégia a megelőzés.

Harmadik helyezett lett a múlt hónapban debütált Win32/Adware.MultiPlug. Ez egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kéretlen reklámokat jelenít meg az internetes böngészés közben.



Ismét listatag lett a **Win32/Ramnit**, a kilencedik helyre elegendő teljesítményével. Ez egy olyan fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefutva DLL és EXE formátumú állományokat képes megfertőzni, valamint 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 fertőzött számítógépen.



Végül velünk **maradt a Conficker fereg is, igaz ezúttal az utolsó, tizedik pozíciót őrzi.** A Win32/Conficker egy olyan hálózati fereg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjed. Bár az ezzel kapcsolatos hibajavítás már nyolcadik éve elérhető, a frissítést sokan mégsem végezték el azóta sem, így emiatt már évek óta szerepel a toplistánkon.



Az ESET Radar Report e havi kiadásában ezúttal a spam kampányokról volt szó. Bár már jó 10 éve, hogy 2003 júniusában Bill Gates, akkori Microsoft elnök tett egy olyan merész kijelentést, hogy két éven belül teljességgel meg fogja szüntetni a kórtelen leveleket, ám ez azóta sem sikerült sem neki, sem senki másnak. Sajnos továbbra is rendszeresen érkeznek a szemétlevelek postaládáinkba, néha kórtelen reklámokat hordoznak, néha kártévót vagy kártékony URL link-hivatkozást kínálva fel, és egyre gyakrabban láthatjuk, hogy **mind precízebben testre szabják az üzeneteket a támadók.**

Ehhez egyfelől a címzettől szereznek be személyes információkat, másfelől az is bevett trükk, hogy valódi incidenseket használnak ki, ahol például magukat a szolgáltatóknak kiadva, állítólagos gyors segítséget ígérő linket, számlát vagy jelszó-információt ígérő mellékletet küldenek a gyanútlan felhasználóknak. Aki ilyenkor figyelmen kívül kattan, az jó eséllyel egy kártévőnek, vagy kémprogramnak nyitja meg az utat a számítógépén.



Egy friss írórszági beszámoló szerint erőteljes spam kampányok figyelhetők meg például a Bank of Ireland, az Apple iTunes, a PayPal fizetesköztetítő és a Microsoft nevével visszaélve. A hamis üzenetekben arra hivatkoznak, hogy állítólag gyanús bejelentkezést tapasztaltak a nevünkben, és egy mellékelt link segítségével felajánlják a login információink azonnali ellenőrzését. Ha valaki bedől ennek az átverésnek, akkor sajnos éppen ezzel nyújtja át tálcán a belépési accountját a bűnözőknek.

Nagyon lényeges, hogy minden kórtelen levél esetén még a rákattintás előtt ellenőrizzük le a linkeket, és a valódi feladót. Ha a legkisebb kétség is felmerül, haladéktalanul töröljük a levelet. Emellett pedig kulcsfontosságú, hogy a levél linkjére közvetlenül sose kattintsunk. **Ha pedig valóban ellenőrizni akarjuk a jelenlegi név-jelszó párosunk működőképességét, azt mindig a böngészőbe kézzel begépelte vagy a könyvjelzőnkéből előhívott URL cím segítségével tegyük.**



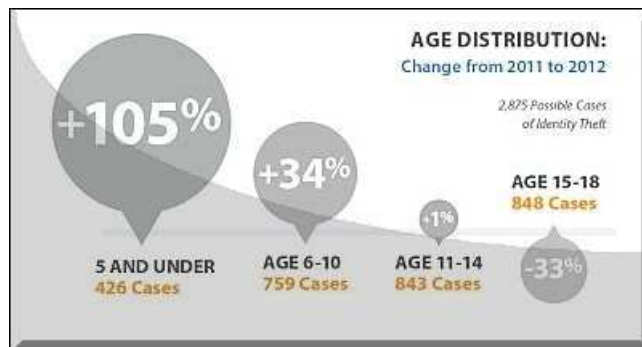
Augusztusi fontosabb blogposztjaink között beszámoltunk egy olyan Facebookos átverésről, amelyben **állítólag mindössze egy lájk és egy megosztás segítségével volt nyerhető iPhone 6.** A csalást kifundálók ráadásul 99.9% eséllyel ígérték a nyeresre, ami végiggondolva gyakorlatilag nem csak hihetetlen, de lehetetlen is.



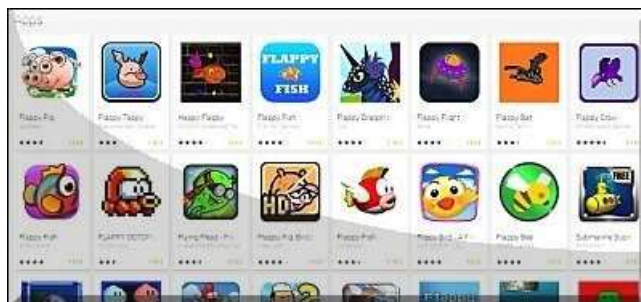
A tavaly elkezdődött [nagy adatszivárgási incidensek](#) - Target áruházlánc, Domino Pizza hálózat, Adobe, LinkedIn vagy most éppen a [CNET](#) és a [Mozilla](#) - kapcsán összefoglaltuk az azonnali teendőket, lépéseket, amiket a valós vagy vélt kiszivárgások után elvégezni érdemes, beleértve ebbe az erős és egyedi új jelszó választását.



A közösségi oldalak gyakran adnak terepet a különféle csalásoknak, így [Robin Williams öngyilkossága után egy olyan átverés jelent meg](#), amely az elhunyt utolsó telefonhívását bemutató állítólagos videó ígéretével terjedt a közösségi oldalon, ám helyett ingyen nyeremény iPaddel vagy iPhone-nal kecsegtetve különféle űrlapkitöltőgetésekre próbált meg rávenni bennünket.

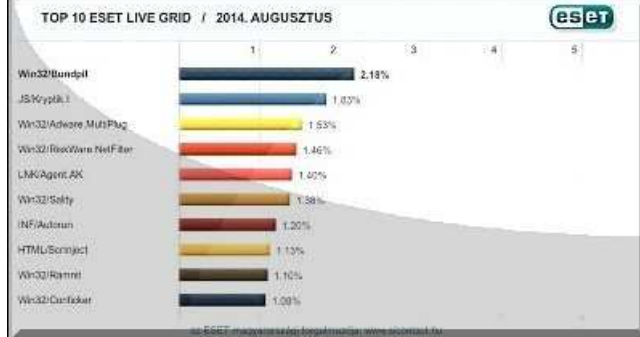


Augusztus utolsó napjaiban egy olyan aktuális témát tűztünk napirendre, mint [az iskolakezdést](#). Ezzel kapcsolatban [védelmi tippeket gyűjtöttünk csokorba annak érdekében](#), hogy személyes adatainkat ne lophassák el, számítógépünket és mobiljainkat pedig hogyan használhatjuk otthon és az iskolában a legbiztonságosabban.



Végül arról is posztoltunk, hogy a [korábbi Dong Nguyen által jegyzett Flappy Bird mobiljátékot másoló klónokhoz hasonlóan az újabb slágerjátékának a nevével visszaélve ezúttal a Swing Copters nevezetű program hasonmásai bukkantak fel a Google Play piactér kínálatában](#).

Védekezésül érdemes antivírust használni Androidon is, továbbá mindig alaposan nézzük utána a telepíteni kívánt alkalmazás előéletének, engedélyeinek és a vele kapcsolatos felhasználói visszajelzéseknek is.



Vírustoplista

Az ESET több millió felhasználó visszajelzéseire alapuló statisztikai rendszere szerint **2014. augusztusában a következő 10 károsító terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 14.29%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megítézéséről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.



01. Win32/Bundpil féreg

Elterjedtsége az augusztusi fertőzések között: 2.18%

Működés: A Win32/Bundpil 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 megkísérli további kártékony komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



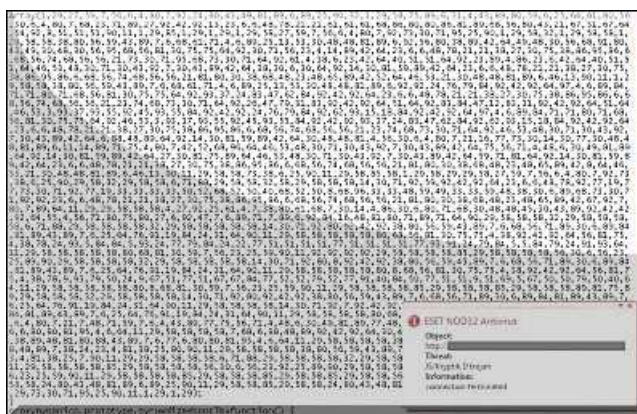
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



02. JS/Kryptik trójai

Elterjedtsége az augusztusi fertőzések között: 1.83%

Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlan összezárt JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalak irányítja át a felhasználó böngészőprogramját.



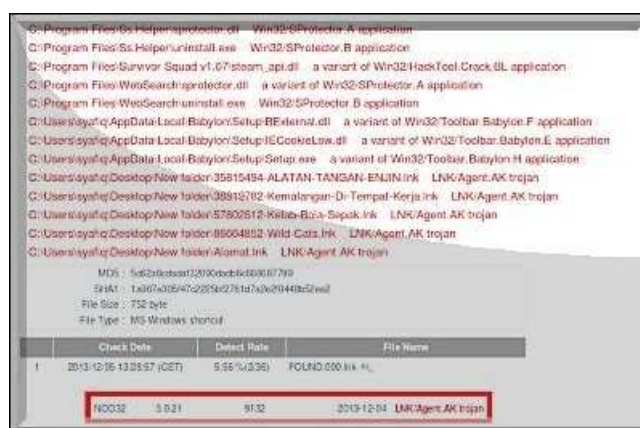
Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail



03. Win32/Adware.MultiPlug adware

Elterjedtsége az augusztusi fertőzések között: 1.53%

Működés: A Win32/Adware.MultiPlug egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kényszerűen reklámokat jelenít meg az internetes böngészés közben.



Bővebb információ: http://www.virusradar.com/en/LNK_Agent.AK/description



06. Win32/Sality vírus

Elterjedtsége az augusztusi fertőzések között: 1.38%

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.



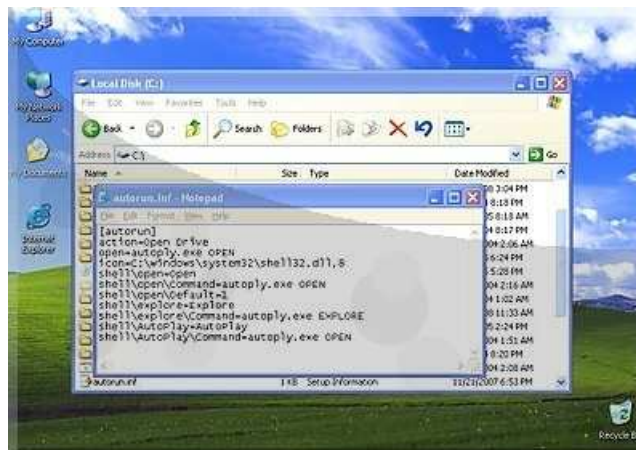
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



07. INF/Autorun vírus

Elterjedtsége az augusztusi fertőzések között: 1.20%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájl használó károkozónak. 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>



08. HTML/ScrInject trójai

Elterjedtsége az augusztusi fertőzések között: 1.13%

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.

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[A HTML trójaiak riogattak minket októberben](#)

[Végre kiesett a Conficker féreg](#)

[Júliusi vírusstoplista](#)

[Júliusi vírusstoplista](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6696897>

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.

Olvas-e az Apple IT security blogokat?

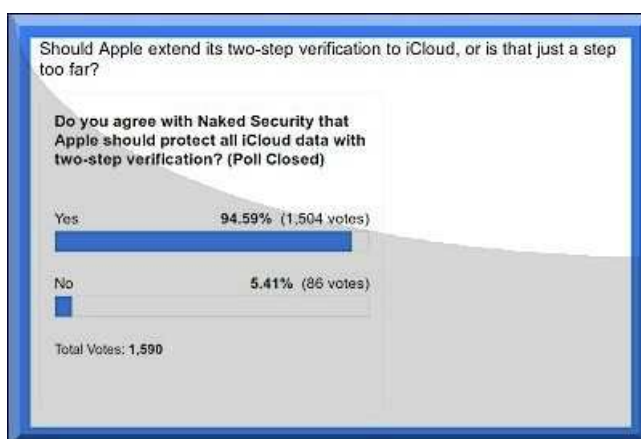
2014.09.18. 09:56 | [Csizmazia Darab István \[Rambo\]](#) | [2 komment](#)

Címkék: [apple biztonság backup felhő feltörés azonosítás icloud bruteforce kétfaktor ibrute](#)

A rövid válasz szerint: nem tudjuk. A hosszú válasz szerint pedig talán igen, valószínűleg olvasnak ilyeneket, de jól titkolják ;-). Mindez annak kapcsán került most terítékre, hogy augusztus végén [számtalan híresség - például Jennifer Lawrence, Kate Upton, Kirsten Dunst, Avril Lavigne - meztelen képe jelent meg](#) váratlanul a Reddit és a 4chan oldalain.



Mint arról sok helyen olvashattunk, nagyjából száz ismert ember privát fényképei, videói kerültek ki a nyilvánosság elé. A történeteket az is érdekesebbé tette, hogy [sok híresség azt állította, ezeket a képeket állítólag már rég törölte a telefonjáról és az iCloudból is](#). Az Apple első reakciója is beszédes, vizsgálatot indítottak az ügyben, és [úgy nyilatkoztak, hogy "nem az iCloud rendszer hibája vezetett a fotók jogtalan megszerzéséhez", pedig azért ehhez a biztonsági szakértőknek is volt egy-két szava](#). A NakedSecurity oldalán pedig [elindult egy szavazás az iCloud kétfaktoros azonosításáról](#).



A támadásnál valószínűsíthetően a Find My iPhone szolgáltatásban rejlő gyenge-pontot használták ki, és ennek segítségével tudtak hozzáférni a fiókokhoz. Az úgynevezett brute-force támadás lényege ugyanis az, hogy folyamatos ismétléssel addig próbálgatják a valószínű jelszavakat, amíg egyszer csak nem járnak sikerrel. Az ilyen támadások ellen csak az nyújt védelmet, ha korlátozott a lehetséges próbálkozások száma - meg persze ha nem "abc123" a jelszó, de erről majd később.

Míg ez a limit például az iCloud rendszerben már korábban is be volt állítva, sajnos a támadás idején a Find My iPhone funkcióra viszont nem. Persze utóbb aztán az Apple aktiválta a brute-force védelmet a Find My iPhone szolgáltatásra is, csak hát ugye későn. Végül aztán - vége jó, minden jó - [kétlépcsős azonosítást kaptak az iCloud backupok is](#), valamint e-mail értesítést is bevezettek, melyben [a felhasználóknak azonnal jelzik, ha valaki megpróbálja megváltoztatni az Apple ID jelszavukat, vissza akarja állítani az iCloud adataikat](#) vagy amikor éppen először jelentkeznek be egy új eszközön a felhasználói fiókjukba.

```
MacPro:ibrute kmax$ ./id_brute.py
Working with: *****@hotmail.com
Trying: *****@hotmail.com Password1
Trying: *****@hotmail.com Princess1
Trying: *****@hotmail.com Password
Trying: *****@hotmail.com Password
Trying: *****@hotmail.com Michael1
Trying: *****@hotmail.com Blink182
Trying: *****@hotmail.com lQAZ2vwx
Trying: *****@hotmail.com Charlie1
Trying: *****@hotmail.com Anthony1
Trying: *****@hotmail.com lqaz!QAZ
Trying: *****@hotmail.com Brandon1
Trying: *****@hotmail.com Jordan23
Trying: *****@hotmail.com C*****
Got It! *****@hotmail.com C*****
Trying: *****@hotmail.com lqaz!Vsx
^Z
[3]+ Stopped ./id_brute.py
MacPro:ibrute kmax$
```

Az érdekesség kedvéért [érdemes vissza idézni Vladimir Katalov 2013. május 30-i blogposztját az iCloud biztonságával kapcsolatban](#). Láthatóan ez sem szerepelt a kedvenc olvasmányok között, ugyanis itt éppen az Elcomsoft Phone Password Breaker segítségével férnek hozzá a felhasználók személyes adataihoz, mint például a korábbi mentés, vagy hogy a bekapcsolt kétfaktoros autentikáció ellenére a biztonságos ellenőrző kód a lezárt készülék képernyőjén is olvasható formában érkezik.

Jól láthatóan a biztonság egy olyan bonyolult struktúra, ahol nem elég egyszer beledobálni a buzzwordokat, majd hátradőlni a karosszékekben, hanem folyamatosan oda kell figyelni arra, hogy a védelem minden lehetséges szintre terjedjen ki. Kiegészítve mindezt azzal, hogy az újonnan felfedezett támadási formák miatt állandóan javítani, fejleszteni is szükséges, hiszen a támadók felkészültek, és láthatóan roppant leleményesek.

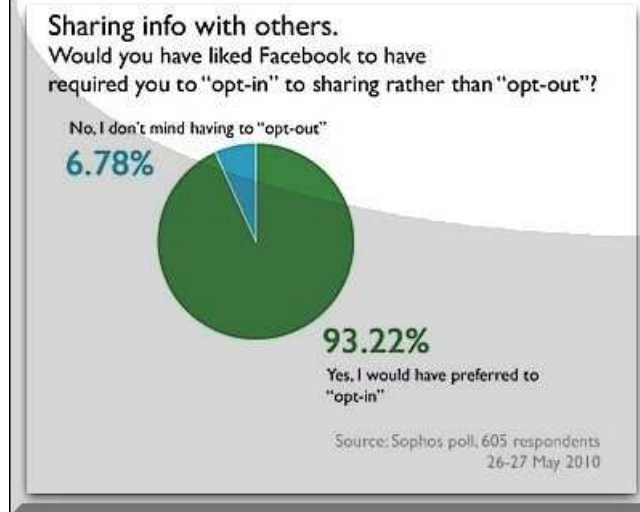


Itt egyébként még egy dologgal érdemes előhozakodni. Minden nagyobb adatlopási incidens esetén a média, és a bulvárlapok hajlamosak azonnal a számítógépes rendszereket, és a technológiát szidni, hibáztatni. Ebben persze részben - ahogy a fentiek is mutatják - van is némi igazság, ám ez mindenképpen csak az érem egyik oldala. Ugyanis legtöbbször emberi hiba, felhasználói mulasztás is okozza az ilyen incidensek jelentős részét.

Sok esetben - például Google, Facebook - rendelkezésre áll ugyan a 2FA lehetőség, sokan mégsem élnek vele. De emellett ha valaki gyenge és primitív jelszót használ, ráadásul ugyanazt több helyen is, vagy pillanatok alatt kitalálható biztonsági kérdéseket alkalmaz, akkor ő is vastagon felelős a kialakult helyzetért. **Vagyis minden hibázó félnek, mulasztó szereplőnek le kell vonnia a tanulságot az ilyen esetekből.**



Zárásképpen említsük meg, hogy volt már korábban is [olyan NakedSecurity szavazás, ahol a mi legyen az alapértelmezett megosztás a Facebookon](#) kérdésre egyértelmű túlsúllyal jelezték a válaszadók, hogy az lenne a jó, hogy defaultból legyen minden privát, és majd a felhasználó megosztja, amit éppen akar. Ennek ellenére ismert, hogy ennek pont az ellenkezője igaz, és csak győzze az ember visszavenni a publikus információkat szolgáló pipákat. **Vagyis viccesen mondvá a Facebooknál viszont szemlátomást azóta sem olvasnak IT security blogokat ;-)**



 Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Napi 160 ezer Facebook account esik el](#)
[Twitter bejelentkezés másképpen](#)
[Így vigyázz a Bitcoinodra](#)
[Bízunk-e a felhőkben?](#)
[Sebezhetőségek a Safari-ban](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6708125>

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](#).

[antyg 2014.09.18. 11:22:53](#)

Ez egy nagyon jó, és érdekes Cikk! Mindenkinek javasolnám az elolvasását! :):):)
TETSZIK!!! :)
Válasz erre

[dr. trafik nomac 2014.09.19. 10:57:37](#)

Jo cikk, de ez egy irtó amator hiba, ehhez nem kell IT security szakertonek lenni, sajna az apple (is) kb. ennyire alapos minden masban.
Válasz erre

Túlélőkészlet webáruházi adatlopások ellen

2014.09.22. 13:12 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [jelszó](#) [bank](#) [home](#) [adatok](#) [megelőzés](#) [tanácsok](#) [adatlopás](#) [teendők](#) [depot](#) [welivesecurity.com](#)

Úgy tűnik, nem pusztán arról van szó, hogy [a 2013-as esztendő a gigantikus ügyféladat lopások éve volt](#), hanem egyre inkább fogalmazhatunk úgy, elkezdődött egy folyamat, ahol a kiszivárgott személyes, és banki információk mennyiségét tízmillió nagyságrendben mérhetjük. Ilyenkor ugyan nem az ügyfél az incidens okozója, de mégis érdemes végiggondolni, mit tehetünk mi magunk is, ha már beütött a baj.



Bár a hírekből jobbra tengeren túli esetekről olvashatunk, ez csak azt jelenti, hogy az ottani nyilvánosságra hozatali kötelezettség rendben működik, de semmiképpen nem nyújt garanciát arra, hogy ez mással és máshol nem történhet majd meg (vagy már meg is történt, csak éppen nem tudunk róla). Mit tehetünk, ha tudjuk vagy gyanítjuk, hogy áldozatul estünk egy olyan áruházi rendszert ért adatsértésnek, mint amilyen a Target vagy [a szeptember 8-i Home Depot barkácsáruház-lánc elleni támadás](#) volt és veszélyben lehetnek a fizetési adataink?

Ez utóbbi esetben például rekord mennyiségű, **56 millió bankkártya adat került a feltehetően orosz illetőségű tolvajok kezébe**, akik [a privát adatokat már közzé is tették a neten a Rescator.cc weboldalon](#). A fizetési adatok kifürkészésével járó Home Depot támadásnak egyébként a veszteségeit is felbecsülték már, ez [hozzávetőleg 62 millió dolláros kárt jelent, ami igen jelentős összeg](#).



1. Ellenőrizzük rendszeresen a számlamozgásokat

Ha egyenlegünkön akármilyen csekély összegű megmagyarázhatatlan terhelés tűnik fel, és teljesen biztosak vagyunk abban, hogy azt nem mi kezdeményeztünk, akkor haladéktalanul keressük fel bankunkat és kérjük, vizsgálják ki, mi történt, tegyünk bejelentést. Azt sem szabad elfelejteni, hogy **amíg a bűnözők ilyen mennyiségű kártyaadatot piacra dobnak, az akár több hónapba is beletelhet**. Érdemes tehát az elkövetkező időszakban is folyamatosan figyelni a banki pénzmozgásainkra.

2. Kártya és/vagy esetleg számlaszám csere

Ha biztosak vagyunk abban, hogy a számla adatokat ellopták, kérhetjük a kártya cseréjét, illetve a számla megváltoztatását is a banktól. Bankkártya esetén ha azt mi kezdeményezzük, akkor ez valamekkora többletköltséggel jár, de még mindig jobb, mint egy esetleges sokkal nagyobb veszteséget elszenvedni. Új számlaszám esetében érdemes észben tartani, hogy a korábbi esetleges automatikusan ütemezett fizetési megbízásokat (hitel, törlesztés, közüzemek) a kártya és/vagy számlaadatok változása után újra át kell vezetnünk az új számlánkra.

	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

3. Másik erősebb PIN kód választása

Bár a lehetőségek itt látszólag szűkebbek a 4 karakteres hossz miatt, de a változtatás itt is hasznos paranoiának számít, lévén hogy a tolvajok által kezdeményezett PIN próbálkozások száma szerencsére limitált. **Ahogy a klasszikus jelszavak világában is léteznek egyszerű sémák: "abc123", "password", stb, úgy itt is érdemes elkerülni a könnyen megjegyezhető "1111", "1234", és hasonló primitív formákat, és valamilyen nehezebben kitalálható változatot beállítani.**

4. Esetleges hitelkérelmek ellenőrzése

A csálók időnként nem csak a számlát igyekeznek megcsapolni, de a részletes személyes adatok birtokában további kellemetlenségek is okozhatnak nekünk, **például adót igényelnek vissza a nevünkben**, vagy ami még rosszabb, hitelt vesznek fel az ellopott személyazonossággal. Ennek kezelése és ellenőrzése ország- és bankfüggő, mindenesetre például a Home Depot esetben [az FTC, azaz U.S. Federal Trade Commission is tud ebben segíteni az USA-ban élőknek](#).



5. Jelszó változtatás az adatsértést elszenvedett webáruházban

Itt **egyszer már alaposan kiveséztük azokat a tudnivalókat**, amelyek egy vélt vagy valós jelszó lopás utáni teendőket foglalta csokorba. **Dióhéjban az új legyen "kellően" erős :-)** és egyedi. Emellett pedig ha kapunk jelszóváltoztatást tanácsoló levelet a szolgáltatótól, akkor fogadjuk meg az ajánlást.

Egy korábbi felmérés eredménye ebben például siralmas képet festett, **a felhasználók 18%-a sajnos egyszerűen figyelmen kívül hagyja a jelzést**, ha az általa leggyakrabban használt online oldal jelszócsereire figyelmeztető üzenetet küld neki. **Érdemes nagyobb figyelmet szentelni a jelszavak kérdésének**, mert sok esetben nem zseniális hackerek ügyködnek új technológiával, hanem a felhasználók követnek származó jelszavazástási gyakorlatot.

6. Számítsunk utóhatásokra, testre szabott spamekre és célzott megfélemlítésekre

Minden kikerült személyes adatnak lehet egy olyan utóélete is, amikor a bűnözők **ezeket az információkat felhasználva éppen az incidenst elszenvedő cég nevében (Például Target, Adobe, LinkedIn, stb.) írnak levelet az áldozatoknak.**

Ezekben nevükön szólítják őket, és különböző **social engineering trükkökkel** - például állítólagos új jelszó a kéretlen levél PDF mellékletében, vagy a számlája azonnali letiltásra kerül, kivéve ha a mellékelt linke kattint az ügyfél, stb. - látszólag segítenek, ám valójában további kártevőre mutató linkeket, vagy kémprogramokat igyekeznek rájuk sózni. Emiatt **érdemes minden kéretlen üzenetnél gyanakvónak lenni, és persze tartuk frissen az elmaradhatatlan vírusvédelmi programunkat is.**



+1 Virtuális bankkártya használata

Mi inkább azt tanácsolnánk, hogy ma már minden banknál létezik külön internetes vásárlásokhoz való elektronikus (unembossed card) virtuális kártya, amelynek **a számát bátran megadhatjuk, akár még a három jegyű CVV ellenőrző kóddal együtt is**. Ám erre az alszámlára csak a vásárlás előtt közvetlenül a netbankunkon vezessük át a vásárláshoz szükséges pontos összeget, ami csak pár percig legyen rajta, egyébként a számla nyugodtan legyen üres. Ezzel a módszerrel nem tudnak tőlünk lopni, és így **az "igazi" bankkártyánk adatait sosem kell megadnunk**.

Tetszik 2 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Egészségügyi adatokat loptak az USA-ban](#)
[Magyarországra is megérkezett a CTB-Locker](#)
[Lopott Minecraft jelszavak szivárogtak ki](#)
[Munkavállalói adatok szivárogtak az Nvidiatól](#)
[Twitter bejelentkezés másképpen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6719189>

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](#).

Horvath Ernone 2014.10.15. 00:23:40

Internetes szokásaim több odafigyelést igényelnének, mert túl szabadon mozgok és túl kevés szabályt ismerek .

Ki tudna segíteni P.O. Box címek azonosításában?

Választ várok a zeneszerzo66@citromail.hu email címemre.

Köszönöm.
Válasz erre

Célzott támadás Ukrajnában és Lengyelországban

2014.09.25. 11:33 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

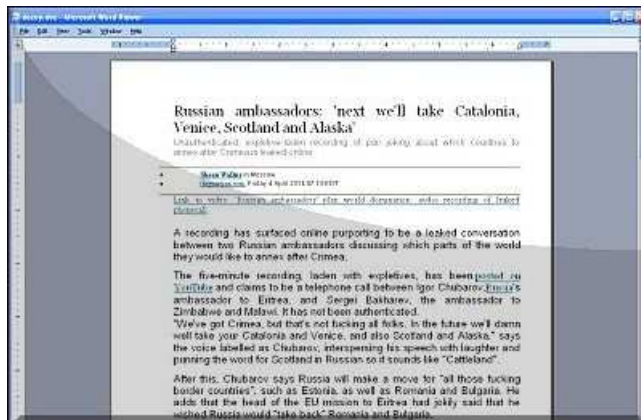
Címkék: [orosz ukrán politikai trójai konfliktus](#) [kártévő kémprogram](#) [lite welivesecurity.com](#) [blackenergy](#)

Lassan már senki nem kapja fel a fejét, ha a hagyományos politikai zavargásokat, fegyveres konfliktusokat - amelyek zömmel, de nem kizárólag elég jól beazonosítható felek között zajlanak - rendre követi, kíséri valamilyen kibertérben is zajló támadás. Ezúttal a lassan egy éves orosz-ukrán szembenállás margójára írhatunk egy ilyen fejezetet, ugyanis nem rég egy olyan kártévő tűnt fel a színen, amelynek kiemelt célterülete Ukrajna és Lengyelország.



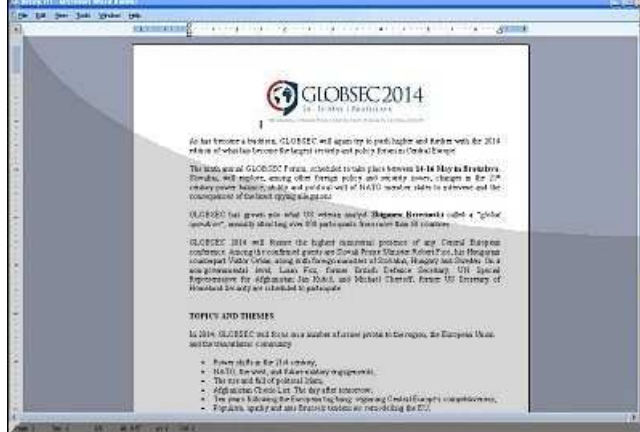
A [welivesecurity.com](#) oldal beszámolója szerint 2014. augusztusában észlelték először azt a távoli kód futtatást és adatlopási funkciót tartalmazó kártévőt, amely a korábban ismert BlackEnergy egy új variánsa. Az eredeti kártévő 2007-ben még csak DDoS támadásra volt alkalmas, és az Arbor Networks készített róla annak idején egy alapos elemzést. Később 2010-ben a BlackEnergy 2 már rootkites rejtőzködéssel is kiegészült a Dell Secureworks jelentése szerint.

A fejlődés azonban szemmel láthatóan nem állt meg, hiszen a kártévő család legújabb verziója BlackEnergy Lite néven már láthatóan egy kritikus geopolitikai helyzetben igyekszik célzottan támadni, és eszköztárában az UAC elkerülés, a driver meghajtóprogramok aláírásának kijátszása is szerepel.



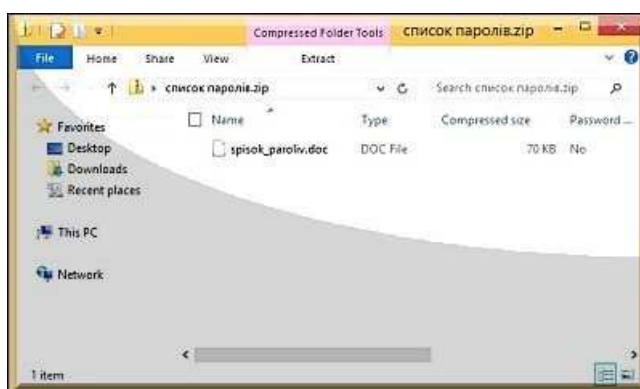
A kártévő terítésekor jellemzően olyan adathalász e-maileket küldözgettek a támadók, amely valamilyen érdekes információt ígértek az ukrán válsággal kapcsolatban, ám a levelek mellékletébe az CVE-2014-1761 sebezhetőséget kihasználó rosszindulatú Microsoft Office dokumentumokat helyeztek például olyan hamis hírrel, hogy abban állítólag orosz nagykövetek bizalmas beszélgetését lehet olvasni.

Egyébként ezt a sérülékenységet többek közt a híres-hírhedt MiniDuke támadási vektorai között is megtalálhatjuk. A 2014. nyarán átírt kártévő fő célja szemlátomást [a kiszemelt számítógépek merevlemezéről történő célzott adatgyűjtés, kémkedés](#).



Az ESET szerint több, mint száz esetben történt ilyen kísérlet **lengyel és ukrán állami szervezetek, különféle cégek, vállalkozások ellen hasonló családi Word dokumentumokkal. Emellett rosszindulatú Power Point állományok, illetve Java sebezhetősége kihasználó kódok is napvilágot láttak már, továbbá egy "jelszavak listája" nevű csalogató ZIP fájl is elküldésre került.** Ez utóbbinál nem lehet pontosan eldönteni, hogy ez is a támadás része-e, vagy csak hibáztak, és mellényomtak a támadók.

A friss téma [az idei VirusBulletin konferencián is soron kívül helyt kapott](#). Természetesen indokoltak látszik a további folyamatos adatgyűjtési és részletes elemzési munka, hogy később sikerüljön még pontosabb képet kapni a kártevő részletes viselkedéséről, illetve C&C kommunikációjának megfigyelésével az esetleges eredetéről is kiderülhessenek információk.



Természetesen - ahogy azt a [2007-es Észtország](#), vagy a 2008-as [Grúzia elleni kibertámadásnál is már láttuk](#), ilyenkor rendre nem határozható meg egyértelmű felelős vagy konkrét elkövető, hanem mindössze sejteni vagy találgatni lehet részint a **technikai részletadatokból, részint pedig az érdekek áttekintése révén.** Éppen ezért lehet érdekes, hogy [a walesi NATO csúcson](#) egyértelműen deklarálásra került, hogy kibertámadás ellen akár hagyományos fegyverekkel is reagálhat majd válaszcsepásban az USA. Az elkövetők pontos beazonosítása nélkül ez egyelőre elég elképzelhetetlennek látszik.

Egy biztos, a különféle konfliktusos övezetekben a hagyományos fegyvernemek mellett a felek, vagy szimpatizánsaik előbb-utóbb ha nem is hivatalosan, de a különféle kibertámadásokat is egyre gyakrabban bevetik.

Tetszik 8 személy kedveli ezt [Regisztrárl](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

[A váltásdíjas titkosító kártevő visszatér](#)
[Sanita ismerkedne - fotóval](#)
[Rejtett előfizetéssel trükköző cégek](#)
[Megfertőzheti-e számítógépünket az e-cigaretta?](#)
[Itt az első váltásdíjas titkosító kártevő Androidon](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6730045>

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](#).

Bicepsz Elek 2014.09.25. 19:34:46

Jajajjj!!! Az USA es Izrael is kyber-tamadta Irant. Csak azt tamadjak, akit mernek hagyomanyos fegyverekkel. Kemkedni meg mindenki

kemkedik mindenhol. Ez nem lehet az USA monopoliuma..

Válasz erre

Sokkoljon-e minket a Shellshock?

2014.09.29. 10:35 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [linux](#) [hiba](#) [patch](#) [macintosh](#) [javítás](#) [unix](#) [router](#) [sebezhetőség](#) [shellshock](#) [welivesecurity.com](#)

"Ami sok, az sokk", amely megállapítást már a klasszikus mozifilmből korábban is a magunkévá tehattünk. Az előző [nagy visszhangot](#) kiváltott Heartbleed hiba után nem is olyan sok idő elteltével máris itt a hasonló volumenű Shellshock sebezhetőség. Windowsos vagyok mit tegyek?, Mac-es vagyok vajon érint-e engem?, vagy Linuxot használok mi a teendőm? - megpróbáljuk kicsit összeszedni a Shellshockkal kapcsolatos adekvát választ, és mindazon konkrét információkat, amik egy hétköznapi felhasználót érinthetnek, érdekelhetnek.



A jó 20 éve létező hibával kapcsolatosan már jó pár cikk született, abban azonban szinte [minden biztonsági szakember egyetért, hogy a javítás egy erősen elhúzódnó folyamat lesz](#). Ennek elsősorban nem is az az oka, hogy a sztenderd operációs rendszerek frissítései nagyon késnek majd, illetve hogy a felhasználók azokat nem futtatnák azonnal, bár ez is egy jelentős veszélyforrás.

Azonban [sokkal több gondot fognak okozni a világ minden táján megtalálható Linux alapú olyan hálózati eszközök, NAS adattárolók, otthoni routerek, intelligens fogyasztásmérők, és egyéb intelligens készülékek](#), okos autók, és más eszközök, amikről nem is gondoljuk azonnal, hogy érintettek. És akkor még nem is beszéltünk az olyan korosabb eszközökről, ahol a gyártók akár már évek óta semmit nem frissítenek.



Nézzük akkor először röviden, [mi is a hiba lényege](#), aztán megpróbáljuk összeszedni, mennyiben érint mindezt bennünket. A Shellshock egy olyan sebezhetőséget rejt magában, amely a Bash (Bourne-again shell) shell futtató platformokon jogosultság, bejelentkezés, vagy jelszó nélkül is távolról futtatható tetszőleges kód az érintett számítógépeken anélkül, hogy erről a rendszer használója tudomást szerezne. A [saját érintettségünket például a Lifehacker oldalon megjelent](#) kis script segítségével tudjuk tesztelni:

```
"env x='()' { :; }; echo vulnerable' bash -c 'echo hello'"
```



A fentiek eredményeként rögtön látszik is, kiket érint, kell-e rögtön tenni valamit. Az első megközelítésben erre a kérdésre ugyan valóban az a szabatos válasz, hogy minden olyan *nix operációs rendszer érintett, amely az említett Bash shell szolgáltatást futtatja, ám sokaknak

ekkor csak az asztali vagy kiszolgálókon futó Unix, Linux, BSD, OSX jut az eszébe.

Ám ahogy a bevezetőben is említettük, a szerverek és munkaállomások csak egy részét jelentik a problémának, hiszen a hálózati eszközök tekintetében számtalan router, tűzfal, okostelefon tartalmazza ezt a sérülékenységet, de emellett rengeteg ipari (közlekedés, vezérlés, erőművek, stb.) rendszer is érintett lehet a Unix alapú technológia miatt. Emiatt pedig a Heartbleed mellett egy újabb, hosszan elhúzódó javítási folyamat veszi most kezdetét.



A Windowst használók most egy kicsit fellélegezhetnek, ám azt fontos megjegyezni, hogy ha olyan weboldalt látogatnak meg, ahol a Unixos webszerver tartalmazza a Shellshock hibát, fennáll a lehetősége hogy azt rosszindulatú kód terjesztésére, fertőzésére használják ki. Így itt mindössze annyi lehet a tanács, hogy tartsuk naprakészen a vírusvédelmi eszközeinket.

A Mac felhasználók élete már kicsit bonyolultabb, a hiba jelenlétét a fenti teszt segítségével elvégezhetik, amiből kiderül, kell-e aggódniuk. Sajnos az Apple javítása még nem jelent meg, így ezt kell türelmesen kivárni, vagy törölni a Bash-t vagy pedig az [appleblog](#) oldalon is közölt Xcode-os okossággal is lehet esetleg addig is próbálkozni.

A Linux rendszerek esetén - ami a szabványos és elterjedt disztribúciókat illeti - már szinte mindenhol megjelent a szükséges javítás, így Redhat, Debian és Ubuntu alatt biztosan, de [emellett folyamatosan mindenhova jönnek a javítófoltok](#). Bár már elcsépett szófordulat, de most tényleg érdemes azonnal mindenkinek frissíteni.

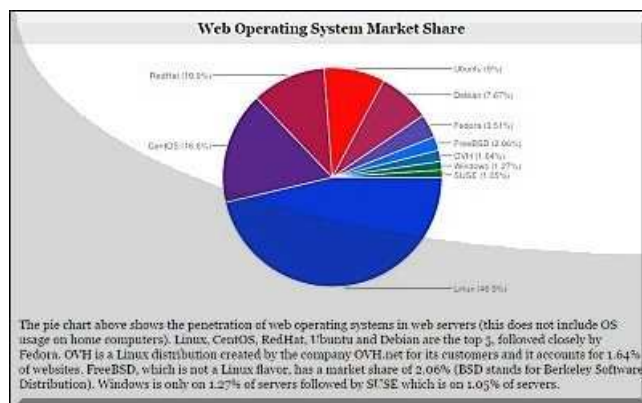


Az otthoni felhasználóknak érdemes lesz figyelemmel kísérnie az általuk használt hálózati eszközök - router, NAS, stb. - gyártóinak, fejlesztőinek weboldalát, blogját, ha van technikai fórumát és naprakészen tájékozódni az esetleges frissítésekkel kapcsolatosan. Meg lehet őket keresni levélben vagy telefonon is, és kikérni a tanácsokat, bár naprakész lista még nincs a sebezhető eszközökkel kapcsolatban. Itt is sztenderd eljárás, hogy tartsuk naprakészen a vírusvédelmi eszközeinket.

Hasonló jó tanácsok mondhatók el a SOHO és SMB ügyfeleknek is, vagyis az operációs rendszerek mellett az egyéb hálózati eszközök esetleg érintettségét is tisztázni kell, és kétség vagy szükség esetén kapcsolatba kell lépni a gyártókkal.

A vállalati IT részlegek elsődleges feladata felderíteni a rendszerben szereplő összes olyan felhasználót, akik a sebezhető Bash szolgáltatást futtatják és gondoskodni a megfelelő helyreállítás, frissítési folyamatokról.

Akik bármiféle weboldallal rendelkeznek, ellenőrizték le vagy lépjenek kapcsolatban a webhosting cégükkel, és tájékozódjanak a support oldalukon az aktuális frissítésekről, különösen Apache és CGI esetében. Ugyanez tanácsolható azoknak is, akik virtuális privát szervert használnak, vagyis forduljanak a szolgáltatójukhoz és kérjék ki a szakembereik tanácsát.



Közben sajnos megérkeztek az első komolyabb Shellshock sérülékenységet kihasználó támadások is, így például a Debianon futó

wopbot nevű botnet aktivitásáról már olvashattunk beszámolót, melyek szerint az Egyesült Államok Védelmi Minisztériumában is találkoztak már vele. A kártevők végigszkenneli az IP cím tartományokat, sebezhető gépeket keresve, illetve brute force segítségével a gyenge hálózati jelszavak ellen is támadást próbál intézni. [Olasz kutatók szerint a támadóknak ezzel a módszerrel már több, mint 200 ezer szervert sikerült megfertőzniük.](#)

 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[LastPass a pácban](#)

[Szőnyegjavítás: jobb későn, mint soha](#)

[Új funkcióval bővült a Netcraft Toolbar](#)

[A Facebook és a Microsoft együtt keresik a hibákat](#)

[Hogyan tudnék élni nélküled?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6740793>

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> **2014.09.30. 14:23:17**

apple javítás: support.apple.com/kb/DL1769 a fent linkelt oldalról

megcsináltam a bash tesztet, de egy harmadik eredmény jött ki :O csak 'hello' és elvileg volt security bash update-em
Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu>
2014.09.30. 16:03:39

A legtöbb Linux disztribútor hamar kiadta már a javítást, most végre az Apple is jelentkezett a Shellshock biztonsági csomagjával OS X-re, érdemes tehát mihamarabb frissíteni.

appleblog.blog.hu/2014/09/30/az_apple_kiadta_a_shellshock_biztonsagi_csomagot_os_x-re

Válasz erre

gizmo266 **2014.09.30. 18:39:30**

Na ugye hogy a windows jó kis operációs rendszer.

Bár most sem értem miért foglal 2 Giga helyet a memóriából, és miért akadozik, ha még 2 Giga üres hely van benne.

Válasz erre

Ször Péter díjjal jutalmazták az ESET kutatóit

2014.10.02. 09:39 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [award péter 2014 ször operation virusbulletin welivesecurity.com windigo](#)

A 24. Virus Bulletin Nemzetközi Konferencián (Seattle, USA) első ízben adták át a Ször Péterről elnevezett díjat (Péter Ször Award), amelyet idén az ESET kanadai kutatócsoportja vehetett át [az Operation Windigo elnevezésű világméretű támadássorozatról](#) írt részletes elemzésükért.



A tavaly tragikus hirtelenséggel elhunyt, magyar Ször Péter informatikus, számítógépes biztonsági szakértő, és víruskutató volt, aki a területen kimagasló érdemeket szerzett. [Ször Péter \(1971-2013\) eredetileg Balatonfüreden született, a Veszprémi Egyetemen tanult informatikát. Pasteur nevű víruskeresője ismertté tette a nevét 1995-ben, többek között ezt használta egy időben még az OTP is. 1996-ban Finnországba ment dolgozni az F-Secure elődjéhez a Data Fellows-hoz, ahol víruskereső szoftverek fejlesztésével foglalkozott.](#)

1997-ben bekerült a számítógépes vírusok kutatásával foglalkozó CARO (Computer AntiVirus Researcher's Organization) szervezetbe is, ahol a szakma olyan akkori nagyjaival dolgozhatott együtt, mint John McAfee, Mikko Hyppönen vagy Eugene Kaspersky. Tíz éven át a Symantec vezető mérnöke volt, rendszeresen publikált szakújságokban és magazinokban is, emellett pedig 40 amerikai és nemzetközi szabadalom is fűződik a nevéhez. 2009-től haláláig a McAfee cégnél dolgozott egy új fejlesztésű vírusvédelmi megoldáson.



2010. májusában jelent meg [a később magyarra is lefordított műve, a "The art of Computer Virus Research and Defense"](#), ami egy átfogó könyv, amely a vírusok, férgek, kártevők felismerésével kapcsolatosan [minden technikai részletbe belemerg, megmutatja, elmagyarázza](#). Ez a könyv olyannyira alapszövegnek számít, hogy minden víruslabor könyvespolcán megtalálható, sok helyen pedig tankönyvként is használják, és többek között cseh, kínai és lengyel nyelvre is lefordították. A magyarországi megjelenést a Sicontact Kft. támogatta, a könyv a "Vírusvédelem művészete" címmel látott napvilágot a Szak Kiadó gondozásában.



"Az ESET kanadai kutatócsoportja igazán kiérdemelte a [Ször Péter emlékére létrehozott kitüntetést](#). Az Operation Windigo részletes és alapos feltárása, [az elemzés során használt úttörő technikák alkalmazása és a különböző más szervezetekkel és kutatókkal való együttműködés](#), mind Ször Péter vitathatatlan szakmai érdemeinek szellemében történt. Reméljük a díj további kiváló minőségű kutatásokra sarkallja az ESET és más szervezetek kutatóit." – mondta John Hawes, a Virus Bulletin Operation elnöke.



Az idén először megítélt Ször Péter Award a tavaly novemberben elhunyt kutató életművének és vitathatatlan érdemeinek állít emléket. A díjat azzal a céllal hozták létre, hogy [hagyományteremtő módon, minden évben átadják a legjobb biztonsági kutatási munkaért](#). Az idei esztendőhöz hasonlóan a jelölések közül a kuratórium által összeállított shortlist alapján az évente megrendezésre kerülő Virus Bulletin konferencián választják ki a nyertest.



Ezen az archiv, még [2010-ben készült videófelvételen arról mesélt, mi indította el a pályán](#), hogyan kezdett érdeklődni a vírusok iránt, mely kártevőket találta munkája során különösen érdekesnek.

 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Elhunyt Szőr Péter](#)

[Villáminterjú Szőr Péterrel](#)

[A vírusvédelem művészete magyarul](#)

[Víruselemző kurzus az egyetemen](#)

[Napi 160 ezer Facebook account esik el](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6752215>

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 az, ami tízszer annyit ér, mint a bankkártya adat?

2014.10.03. 10:45 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [kórház adatok](#) [csalás](#) [egészségügyi személyiséglopás](#) [védtelen](#) [welivesecurity.com](#)

A klasszikus hitelkártya-adatok mellett/helyett a bűnözők egyre inkább célba veszik az értékes egészségügyi információkat. Ehhez sajnos az is hozzájárul, hogy sok esetben elavult (frissítetlen XP) és gyengén védett számítógépes rendszerekről van szó, ahol ráadásul az adatok való hozzáférés is könnyebben elvégezhető, sok helyen például nem is titkosítják azokat.

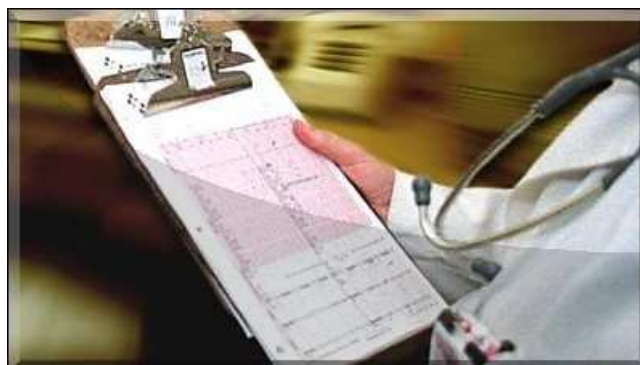


A biztonsági cégek beszámolói szerint virágzó feketepiac van az egészségügyi adatoknak, a címben emlegetett szorzó abszolút nem túlzás. Ha az okokat és a miérteket keresgéljük, hamar érthetővé válik mindez. [A gyengébben védett rendszerekből kinyerhető betegadatokkal ugyanis sok mindent lehet kezdeni.](#)

Ezek terhére igénybe lehet venni extra kezeléseket, többlet mennyiséget, illetve drágább vagy például kábítószer helyettesítő gyógyszereket is lehet vele vásárolni. Emiatt egyre több bűnöző vesz számítógépes feltöréssel szerzett egészségügyi adatokat nagy tételben, ehhez a "gáláns" eladók még egészségbiztosítónként rendezett csomagokat is kínálnak.

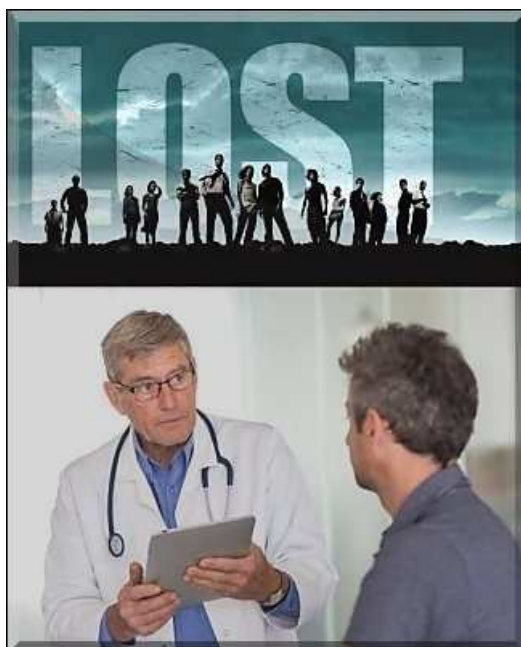


Tavaly például olvashattunk egy beszámolót arról, hogy valaki külön számlát kapott arról, hogy állítólag szívátültetésen esett át, pedig az illetőnek nem is volt semmilyen szívproblémája, és műtétje sem. Emellett az illető nevére ismeretlenek több mozgássérülteknek való robogót, illetve egyéb drága orvosi berendezést is vásároltak [az ellopott adatok segítségével, a végösszeg több tíz ezer dollárt is elérte.](#)



Don Jackson, a PhishLabs igazgatója szerint a lopott egészségügyi adatok akár 10 vagy 20-szorosát is érheti az amerikai hitelkártya információknak. A számítógépes bűnözők alvilági chatszobákban, saját szabályok szerinti tőzsdén kínálják fel ezeket.

A Daily Mail cikke szerint emiatt [az elmúlt hónapban az FBI külön is figyelmeztette az egészségügyi szolgáltatókat](#), hogy kiemelten figyeljenek az ilyen számítógépes támadásokra.



Mi is beszámoltunk korábban olyan csalásokról, ahol a szokásosnak mondható banki accountok mellett egyéb területeket is sikeresen kószoltak a támadók. Például [már 2007-ben iparszerű Second Life online játék azonosító lopások](#) történtek. **De emlékeztetnem lehet az is, amikor az áldozatok nevében hamis adó-visszatérítéseket nyújtottak be a csalók, és ezzel kaszáltak nagy összegeket.** Sajnos az egészségügyi adatok lopásával kapcsolatos tendencia azt mutatja, ezek száma folyamatosan és egyre növekszik.

A Ponemon Intézet jelentése szerint az egy évvel korábbi mértékhez képest 40 százalékkal emelkedett az egészségügyi adatok megszerzésére irányuló kibertámadások száma, míg a 2010-es adatokhoz képest viszont már 100%-kal. Így amikor majd az év végén [az antivírus cégek megejtik a szokásos, következő esztendőre tippelt jóslataikat](#), nem lesz meglepetés, ha azok között ott is találkozunk majd ezzel kapcsolatos előrejelzésekkel.

 **Tetszik** Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

   **Tweet**  **Pin it**  **+1**

Ajánlott bejegyzések:

[Egészségügyi adatokat loptak az USA-ban](#)
[Valentin nap: Szerelem helyett átverés érkezik](#)
[Túlélőkészlet webáruházi adatlopások ellen](#)
[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Az autószerelés veszélyei :-\)](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6755205>

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.

Amikor a marketing üzenet már kevés

2014.10.06. 12:47 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [apple](#) [macintosh](#) [osx](#) [reddit](#) [zombi](#) [trójai](#) [search](#) [botnet](#) [query](#) [reddit.com](#)

Egyik korábbi [posztunkban már elméltünk arról](#), vajon mennyi egyesnek és nullának kellett lefolynia a kártékony kódok folyamán ahhoz, hogy a kezdeti "Itt nincsenek vírusok, mint a Windows alapú gépeken" helyett "A rendszert úgy alakították ki, hogy az biztonságos legyen" válasz legyen olvasható 2012-től az Apple weboldalán a "Miért fogjuk szeretni a Mac-ünket?" kérdésre.



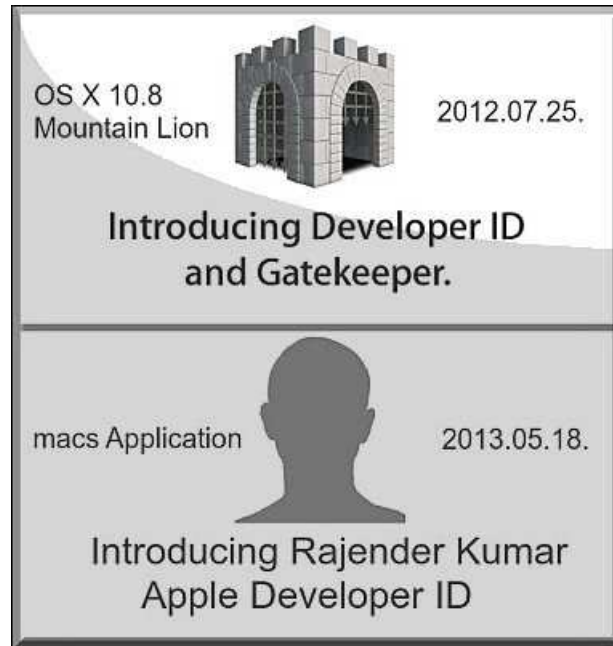
Még ha [a 2010-ben felvetett "Kell-e antivírus a Macre?" kérdésre](#) akkor még sokan feleltek is nem-mel, azt azért észre kell venni, hogy néha azért kifejezetten hasznos lehet, hiszen azóta sok minden megváltozott, másrészt eleve támadhatatlan és 100%-osan biztonságos platform gyakorlatilag nem létezik. Volt ugye például az a nagyon emlékezetes [2012-es Flashback botnet, ami 600 ezer Mac gépet tudott megfertőzni](#). A még 2011-ben kezdődött incidensnél a magát Flash frissítésnek álcázó kártevő a Java egyik biztonsági részét használta ki. Terjeszkedése érdekében pedig több módon is képes volt csatlakozni a C&C szerverhez, például domain neveket generált és adott Twitter hashtagekre is rákeresett.

És még mielőtt bárki ördögtől valónak kiáltaná ki a Java jelenlétét egy OSX számítógépen, számos banki felület pl. CIB bank, CITI bank, de az Adobe Creative Suite, a CrashPlan PRO online secure backup, vagy a talán legelterjedtebb ingyenes LibreOffice is igényli, telepíti, használja azt.



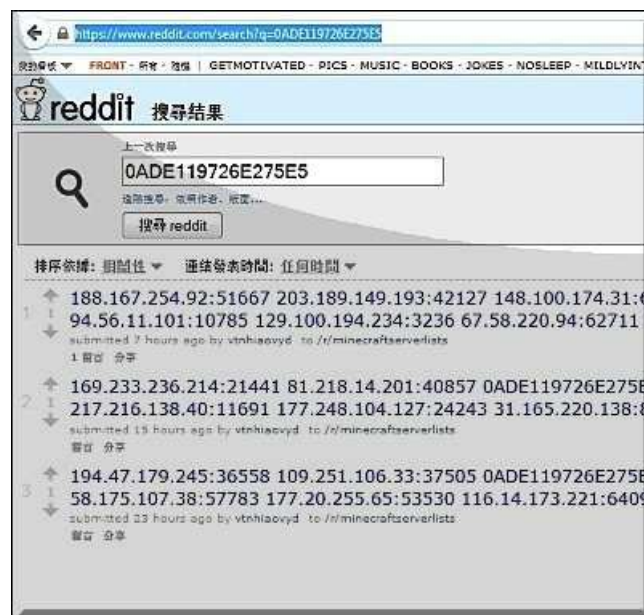
Aztán arra is emlékeztetünk, amikor az Apple a 10.8 verzióval kezdődően igyekezett fokozott hangsúlyt fektetni a biztonságra, és így kedvenc hegyi oroszlanos operációs rendszerünk (Mountain Lion) [titkosított kapcsolaton keresztül végre már automatikusan kap napi biztonsági frissítéseket](#). De ennél a verzióval debütált az Apple Gatekeeper Execution Prevention technológia is, amely a kártékony kódok kiszűrésére lett kitalálva. Sajnálatos módon alig háromnegyed évvel később máris sikerült látványosan kijátszani ezt a rendszert is.

□ **kár** kaptunk hírt arról a valódi, érvényes Apple Developer ID-vel rendelkező trójairól, amely kémkedett az áldozatok OS X alapú gépein. [Az OSX/Kitm.A trójaként aposztrofált kártevő a fertőzött Macintosh számítógépeken titokban képernyőfotókat készített, és ezeket orosz e-mailcímről regisztrált távoli C&C vezérlőszerverekre kísérelte meg feltölteni.](#) Emellett nyitott egy reverse shell-t is, melynek segítségével hátsó ajtót nyitva távoli parancsokat tudott végrehajtani a fertőzött gépeken.



És itt érdemes megemlíteni még egy fontos dolgot. **Bár az Apple rövid időn belül visszavonta ezt a bizonyos Rajender Kumar névre szóló Developer ID-t, ez a már megfertőződött áldozatoknak vajmi keveset segített.** Ugyanis ha egy kártevő már sikeresen átjutott a Gatekeeperen, akkor később már nem történik további újraellenőrzés, vagy ismételt lekérdezés, [így a korábban használt azonosító aláírással rendelkező programok továbbra is szabadon futhatnak a gépeken.](#)

Mindössze annyit lehet tenni, hogy a legszigorúbb, azaz csak a Mac App Store-ból származó programok futását engedélyező opciót választjuk ki. És/vagy a kártékony kódok folyamatos szűrését egy külső naprakész vírusvédelmi programra bizzuk. Ezt [az OSX/Kitm.A trójait a vírusirtók nagy része hamar felismerte,](#) a későbbiekben megjelent újabb módosított verziókkal együtt.



Most pedig [itt a legújabb reddit botnet, amely a biztonsági szakemberek szerint legalább 17 ezer Macintosh rendszert fertőzhetett meg,](#) és nyitott hátsó ajtót a rendszeren. A kártevő egyik érdekessége, hogy annak készítői a Reddit rendszert is felhasználták ahhoz, hogy a botnet sereg zombigép tagjait az elérhető C&C szerverek aktuális helyéről tájékoztassák. [Ehhez a reddit.com kereső szolgáltatását vették igénybe,](#) ahol a keresési lekérdezés eredménye adja ki a C&C szervereknek címét és a szükséges port számát. A keresésnél az első 8 bájtban hexában megadják az aktuális dátum MD5 hashét, az elérhető aktuális szerverek címét pedig a keresési eredmények között található kommentek tartalmazzák.

Az eset egyik tanulsága akár az is lehetne, hogy mivel a támadók folyamatosan és furmányosan ellenünk dolgoznak, mi csak akkor mondhatjuk azt, hogy valóban biztonságban vagyunk, ha egy kapuőr (biztonsági program) áll az ajtóban, ami folyamatosan figyel és ellenőrzi a rendszerünket.

Tetszik Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A Tibeti Macintosh kártevő nem adja fel](#)

[Angry Birds alkalmazásnak álcázott Mac malware](#)
[Több változata is van az aláírt Mac-es trójainak](#)
[Séta a Macintosh kártevők kertjében](#)
[Újabb részletek a Flashback trójairól](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6763719>

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](#).

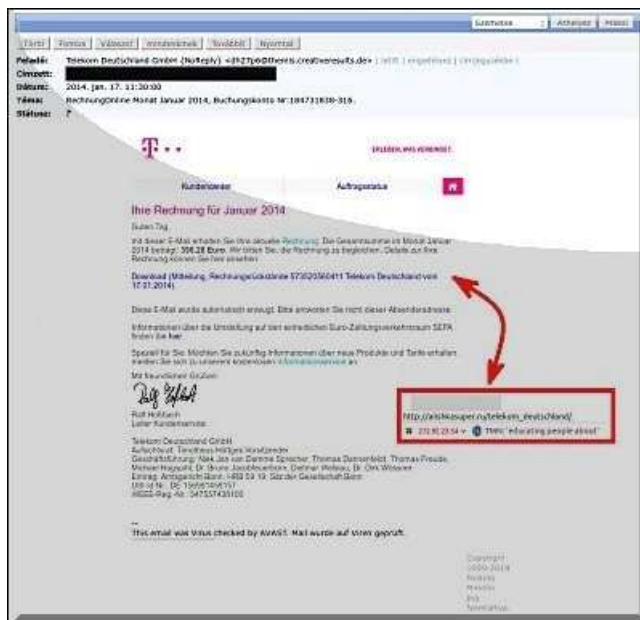
Nincsenek hozzászólások.

A számlalevelek meg egyre csak jönnek

2014.10.08. 12:56 | [Csizmazia Darab István \[Rambo\]](#) | [4 komment](#)

Címkék: [spam csalás](#) [hamis számla](#) [botnet phishing](#) [tartozás](#) [adathalászat](#) [arj zbot](#)

Számlának látszó spamek sajnos voltak, vannak és lesznek is. Ha csak kapásból kellene felsorolni, mi is irtunk már olyan fizetési megbízásról, [amelyik látszólag PayPal-tól](#) jött, vagy volt a [másik állítólagos villanyszámla](#), melyben közlik velünk, hogy a 2013-es évi villamos energia fogyasztásunk elérte a limitet. De a "szerencsésebbek" kaphattak már egy jelentősebb összegről szóló [hamis Telekom számlát](#) is.

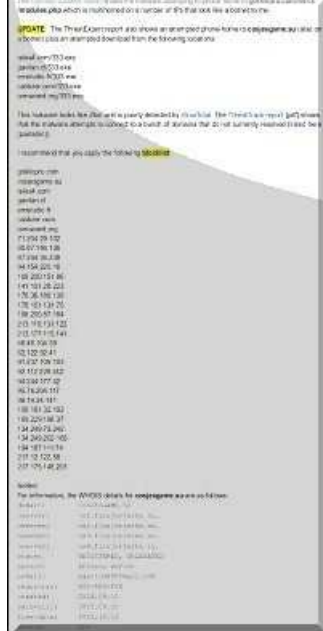


A lánc sajnos azóta sem szakadt meg, sőt itt egy újabb versenyző, amely [megint valamilyen esedékes, sőt lejárt, állítólag be nem fizetett számla ügyében](#) reklamál Mauro Reddin nevében.

A levél melléklete egy .ARJ kiterjesztésű tömörített archívum, amelyben aztán a fertőző EXE is megtalálható, ezt jelenleg [Win32/Injector.BLWX](#) variánsként észlelik az ESET programjai. Az ARJ archiválót egyébként annak idején (boldog DOS-os idők) mi is nagyon szerettük, gyors volt és hatékony, de aztán valahogy eltűnt a süllyesztőben.



Hogy mi történik akkor, ha valaki mégis kattint a mellékletre, arról bővebben egy blogbejegyzésben olvashatunk. Talán senkinek nem meglepő, hogy [egy botnetes kártevővel kapcsolatos, ahol a fertőzés után a gép csatlakozni próbál távoli vezérlőszerverekhez](#). Ebből [egy egész rakatot felsorolnak itt](#) és a [Pastebin oldalain itt](#), a nevek jól láthatóan valamilyen automatikusan generált zaggya karakteres címek.



Mit tehetünk az ilyen kamuszámlás próbálkozások ellen? Mostantól ne fizessünk számlákat ;-). Komolyra fordítva a szót, szokásos támadás ellen szokásos a védekezés is, igazából már csak ismételjük ezeket a tudnivalókat. **Ha kéréstől olyan számláról értesítenek bennünket, amiről nem is tudunk, érdemes óvatosságnak lenni. Ha az üzenet semmitmondó, és arra hivatkozik, hogy majd a mellékletből derül csak ki az érdemi információ, számunkra az is egy intő jel lehet arra, hogy hagyjuk az egészet figyelmen kívül.**

Igaz, ezen persze az sem segítene sokat, ha EXE, ZIP vagy ARJ helyett egyenesen PDF formátumban érkezne, hiszen manapság a beágyazott rosszindulatú Javascriptes kódok miatt az is egy népszerű fertőzőési módszer. Emiatt a biztonságtudatos hozzáállásunk és a hibajavító foltokkal frissen tartott rendszerünk mellett a naprakész vírusvédelmünk alkotta hármas pillérre támaszkodhatunk leginkább.

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Be nem fizetett számla. Vagy mégsem?](#)
[Adathalászat a Google nevében](#)
[Tíz dolog, amit a bankból sosem kérnek](#)
[iTunes számla vagy mégsem II. rész](#)
[Közös fellépés a support csalások ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6770053>

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](#).



[opati666 2014.10.09. 12:21:57](#)

Amíg lesznek lúzer-júzerek, addig lesznek csalók is...
Válasz erre



[maxval a bircaman • http://maxval.co.nr 2014.10.09. 12:38:41](#)

Én az ilyeneket mindig kitöltöm: valódi emialt megadva, de hamis adatokkal. Volt, hogy visszaírtak: nem jók az adataim.
Válasz erre

szib 2014.10.09. 14:29:24

☐n minden számlát a neten (gáz, víz, villany, stb.) fizetek, de magát a számlás sohasem e-mailben kapom. A szolgáltató küld egy értesítést, hogy a számla elkészült, aztán a levélben lévő linkre kattintva elérem vagy a szolgáltató saját, vagy a díjfizető oldalát, és ott fizetek. A címben benne van a szolgáltató neve, vagy annak rövidítése, felismerem, még mielőtt magát a levelet kinyitnám. Vagy egyszerűen elmentem a könyvjelzők közé, és onnan indítom. Más számlát ki sem nyitnék, de szerencsére még nem is kaptam ilyet.

Válasz erre



Robiekin ☐ <http://megfizethetetlenegeszseg.blogspot.hu/>
2014.10.09. 14:49:02

Én a lottónyereményeknél (SPAM) szoktam visszaküldeni a számlaszámom, még nem jött semmi :)

Válasz erre

Snapchat-es átverőrdi

2014.10.13. 13:31 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [képek](#) [privát](#) [incidens](#) [security](#) [cyber](#) [awareness](#) [month](#) [biztonságtudatosság](#) [snapchat](#)

Továbbra sem csendesedik [a tavaly kezdődött adatszivárgási, feltörési hullám](#), melyeknek gyakorta neves cégek is áldozatul esnek, mint az Adobe, a Target áruházlánc, a Snapchat, a LinkedIn, [vagy most éppen a JP Morgan](#). Ráadásul a Snapchat esetében az is módfelett elkésztő, hogy ennyi cikk után még 2014-ben is mennyien vannak, akik tényleg elhiszik ezt a 10 másodperces minden eltűnik maszlagot.

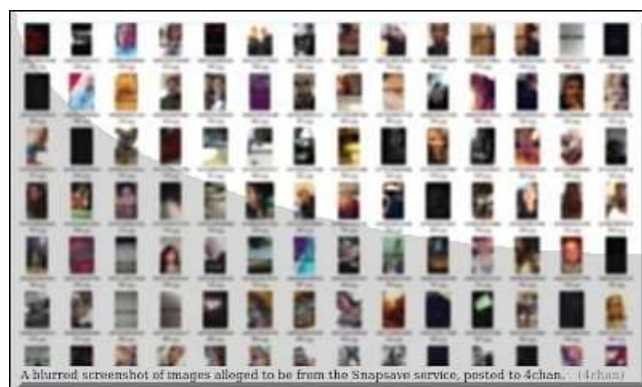


Az "ami egyszer felkerült a netre, azt onnan többet nem lehet letörölni" esetre talán az egyik legtanulságosabb példa, [ha megörökítik azt, amikor elfelejtjük a Himnusz szövegét](#). De mi is foglalkoztunk már azzal, hogy egyrészt az elküldött - az Impossible Mission klasszikus szabályai szerint elvileg önmegsemmisítő - üzenetet technikailag mégis le lehet menteni, le lehet screenshotolni, le lehet fotózni, stb.

Másfelől pedig többszörösen bebizonyosodott az is már, hogy [a szerintünk állítólag sikeresen letörölt képek sajnos a valóságban fizikailag nem tűnnek el, hanem még akár évekig is elérhetőek maradnak](#). Ugyanezt a játékot persze [akár a levelezésre is érdemes lehet végiggondolni](#).

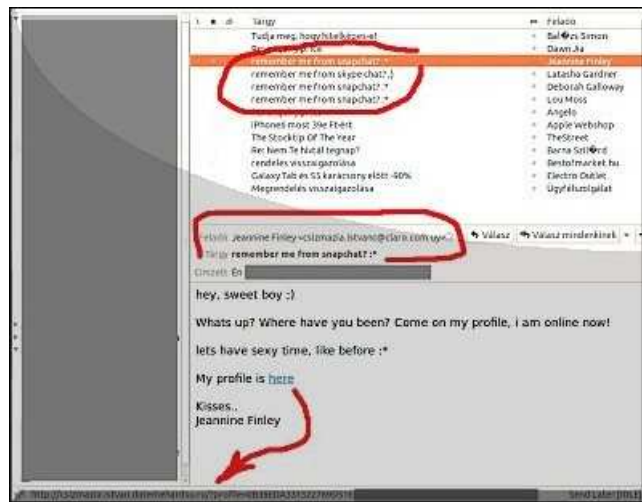


Persze a megfelelő hozzáállást jól minősíti, és roppant vicces is, amikor az iCloud esetenél először bejelentik, nem felelősek érte, majd utána a korábban érthetetlen módon hiányzó brute force elleni védelmet végre gyorsan bevezetik a Find My iPhone esetében is. És persze ott a pont azoknál is, akik az ilyen fotók és videók készítését, tárolását, feltöltését és ráadásképpen a belépési account vérprimitív jelszóval való védelmét a felhasználók kapitális hibájának tartja.



De maradjunk mi most az újabb keletű Snapchates történetnél, amelyben például [a korábbi kiszivárgott meztelen képek közül is több ezret](#) átküldtek Snapchat üzenet rendszerén, amelyek szintén nem tűntek el nyomtalanul. Itt meg lehet említeni [például a Snapsave Android alkalmazást](#) és a hasonlókat, melyek segítségével a tíz másodperces korlátozást megkerülve gyakorlatilag le lehet menteni bármit. A piacereken elvileg zajlik az ilyen appok kiszűrése, kérdés hogy milyen gyorsasággal és hatékonysággal történik mindez. (illetve ez nem is kérdés, mert biztos hogy késve)

Meg nem erősített utalások szerint lehetséges, hogy a snapsaved.com weboldal feltörésével került ki [ezúttal 13 GB!!! mennyiségű](#) [privát fotó](#), melyek közül sok állítólag kiskorúakat ábrázol.



Mellékszálként megfigyelhető, hogy a spamek között is emelkedett a Snapchates témák száma, jó csali ez mostanában. Van ahol, a fappening-nek nevezett jelenség kapcsán keletkezett képeket ajánlgatják, [vagy próbálják pénzért is kínálni](#).

De a családós férfiak is heves magyarázkodásra szorulhatnak életük párja előtt, ha éppen olyan "Remember me from Snapchat?" tárgyú e-mail landol a postafiókjukban, amelyben egy állítólagos Jeannine, Deborah vagy Lou édesnek szólítja őket, jelzi hogy megint online van, és sok csókkal "visszavár" bennünket a profiljába, ahol szerintem korábban már számos kellemes szexi órát eltöltöttünk vele. Természetesen a levél közönséges átverős spam, amely különféle orosz "randioldalakra" próbálja csábítani a gyanútlan és/vagy dühös címzetteket, esetenként pedig kártevőt tartalmazó oldalakra is el irányítja őket.



Visszatérve a Snapchat rendszerre, legalább azt elmondhatjuk, hogy a "felhasználói élmény" biztosan rendben lesz, ugyanis [mostantól már reklámokat is lehet majd "élvezni"](#) :-). A "királyfi, te még hiszel a mesékben" vicc mintájára mindenesetre érdemes lenne időről időre mindenkinek végiggondolnia, milyen szolgáltatásokban bízott meg eddig, és ezek közül melyik érdemes arra, hogy továbbra is használja.

Illetve a felhasználói szokásainkat is újra ellenőrizhetjük az aktuális incidensek fényében, például megszámolni hány darab Snapchat incidens kell még ahhoz, hogy kételkedjünk a tuti biztonságos és maximálisan privát 10 másodpercben. De itt lehet az ideje végre megváltoztatni az "abc123" jelszavunkat is "password"-ra :-). Mert hogy szavunk ne felejtünk, [egész októberben a biztonságtudatosság áll ismét a figyelem középpontjában, hiszen megint Cyber Security Awareness Hónap van](#).

Tetszik Egy személy kedveli ezt. [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

- [Beváltak-e a 2014-es jóslatok?](#)
- [Munkavállalói adatok szivárogtak az Nvidia-tól](#)
- [Séta a Macintosh kártevők kertjében](#)
- [Uber hack - 50 ezer sofőr adata bánta](#)
- [Top 10 IT biztonsági bejegyzés 2014-ben](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6786889>

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.](#)

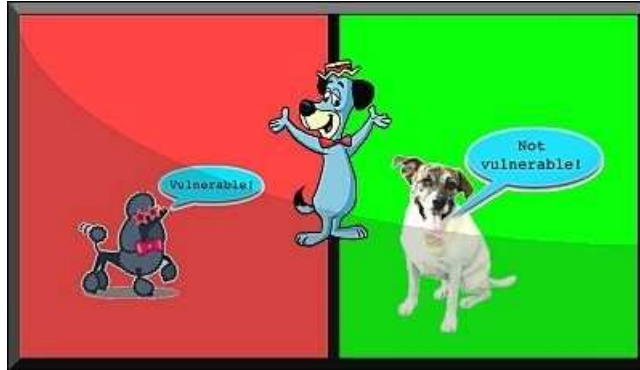
Nincsenek hozzászólások.

Tesztábrával egy jobb, biztonságosabb világot

2014.10.15. 15:23 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [teszt](#) [weboldal](#) [ssl](#) [dns changer](#) [dnscchanger](#) [terrier](#) [conficker](#) [poodle](#) [eyechart](#)

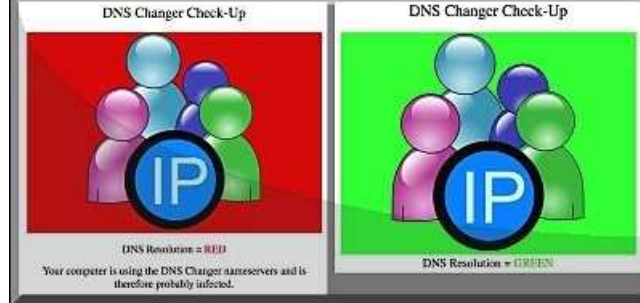
A poszt apropóját az adja, hogy [egy újabb SSL \(Secure Sockets Layer\) sebezhetőség kapcsán](#) megjelent egy olyan teszt weboldal, amelyre belépve ha egy pudlit látunk, akkor sebezhető a böngészőnk, míg ha terriert, akkor biztonságban vagyunk. Ejtünk pár szót erről az aktuális SSL 3.0 hibáról, és áttekintjük, milyen tesztoldalas kampányok segítettek már korábban is a vírusvédelmi megelőzésben.



A napokban újabb hibát fedeztek fel az SSL 3.0-val kapcsolatban. Ez némelyek szerint elsősorban a böngésző kliensek régebbi verzióit érintheti, ám kipróbálva láthatólag az újabb böngészők között is rengeteg a sérülékeny. Bár a sebezhetőség súlyosságát sokan sokféleképp értékelik, fogalmazzunk úgy, hogy semmiképpen nem vágyik arra az ember, hogy egy ilyen man-in-the-middle típusú sikeres támadás során a titkosított üzeneteink tartalmát illetéktelenül ellophassák és a session cookie-jainkat megszerezhessék.

A frissítések megérkezésig az áthidaló workaround megoldást a böngészőkben a SSL 3.0 kikapcsolása jelentheti.





Ez elsősorban a Windows, de emellett részben az OS X klienseket is érintette, hiszen ezekre az operációs rendszerekre gyártották az említett trójai kártevőket.



Később aztán végső határidőt is - 2012. március 8. - szabtak arra, hogy az ilyen fertőzött gépek a manipulált DNS szervereknek a leállítása miatt ne érhessék el a netet. Ennél az incidensnél is teszt ábra segített a gyors tájékozódást, illet [a DNS Changer Working Group \(DCWG\)](#) mellett az [FBI szervezete](#) és német nyelven a [Deutsche Telekom is](#) létrehozott.

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

- [A kilences szám hatalma - DNSChanger GYIK](#)
- [A Facebook is besegít a DNSChanger ellen](#)
- [Ideje ellenőriznünk a DNS beállításainkat?](#)
- [A jelszó ötven árnyalata](#)
- [Az antivírus nem egy lift II.](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6795299>

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 Darab István [Rambo] • <http://antivirus.blog.hu>

2014.10.16. 08:54:34

Itt egy részletes útmutató (angol nyelvű), amely minden egyes programot, böngészőt végigvesz, hogy melyikben pontosan hogyan lehet kikapcsolni az SSL 3-0-t:

scotthelme.co.uk/sslv3-goes-to-the-dogs-poodle-kills-off-protocol/

Válasz erre

Csaláselhárítás fordított képkereséssel

2014.10.17. 11:43 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [spam plugin](#) [képkeresés](#) [fogyókúra](#) [csalás](#) [átverés](#) [hamisítás](#) [search image](#) [reverse](#) [zöldkáv](#) [tineye](#)

Úgy tűnik a csodás fogyókúra témakörben terjedő átverések sosem tűnnek el, sőt egyre gyakrabban jelennek meg a korábbi spamek mellett a közösségi oldalakon, például a Facebookon. Az úgynevezett "reverse image search" segítségével azonban könnyen leleplezhetők a csalások, átverések, hamis beszámolók. Megmutatjuk hogyan lett Roberta Saumból Hertelendy Ildikó, vagy Sheile Kibe miként változott át egy csapásra Némethiné Nagy Tímeává - a módszert látva [Lohengrin csak lehajtott fejjel szégyenkezhet :-\)](#)



Ráhangelődő idézetnek jöjjön egy halhatatlan mondat az Egy bolond száz bajt csinál című könyvből: "Egy magándetektív költözött a mellettem lévő szobába, és hülyének tette magát. De ahogy kinéz, azt hiszem felesleges szimulálnia." Először is érdemes azt tisztázni, hogy a kifinomult [social engineering technikák](#) manapság óriási szerepet játszanak nem csak az áldozatok pénztárcájának megkönnyítésében, de sokszor [a bizalmas adatok ellopásában, és a vírusok terjesztésében](#) is.

Egy csillogó-villó honlap még nem garancia semmire, és ahogy azt már az [1000 dolláros Victoria Secret's ajándék kuponos átverésnél](#) is megírtuk, hogy a gyanakvás és gondolkodás lehet a segítségünk az ilyenek leleplezésében. Ami túl szép ahhoz, hogy igaz legyen, az általában nem is igaz. Ahogy ezt [nagyjából egy éve a zöld kávék spamek esetén](#) is körbejártuk.



Jöjjön akkor a mostani eset, amibe a Facebook oldalain lehet belefutni, amely pár ezer forintért az "extra titkos zsírrejtés" varázslatos receptjét ígéri a hiszékeny balekoknak. A módszer hatékonyságát a hirdető azzal igyekezik bizonyítani, hogy állítólagos konkrét hazai vásárlók kedvező tapasztalatait is feltüntetik a weblapjukon.



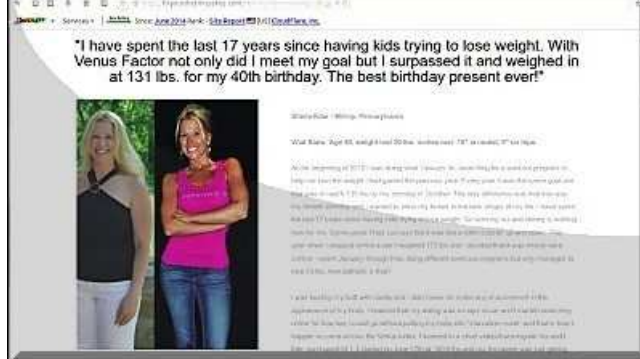
Ám az "internet nem felejt" szabályt ők viszont szemmel láthatóan elfelejtették, ennek bizonyítására [mindössze a TinEye nevezetű böngészőkiegészítőre](#) lesz csak szükségünk. A böngésző plugin nem csak Mozilla Firefox, hanem Google Chrome, Safari, Internet Explorer és Opera alá is elérhető. Nézzük akkor mit mutat például Némethiné Nagy Tímea esetében, ha a jobb egér gombbal elindítjuk a keresést a fényképére kattintva!



Hoppácska, ezek vagy egyetűjű ikrek lehetnek, vagy pedig a világtörténelem legnagyobb rejtélyébe botlottunk, hiszen a debreceni illetőségű Némethiné Nagy Tímea és a pennsylvaniai Sheile Kibe úgy hasonlít egymásra mint két tojás :-O.

Egyébként a képek számítógépes ellenőrzési technikája az évek folyamán komoly fejlődésen esett át, elég csak arra gondolni, hogy az árverési portálokra feltöltött katalógus képekre szinte azonnal, percek alatt megkapjuk az üzemeltetőktől a figyelmeztető e-mailt, hogy csak saját készítésű fotót használjunk, ha netes keresésből származó fotóval próbálkozunk.





Ha már itt vagyunk, nézzük meg, Hertelendy Ildikó kecskeméti lakos fényképe mennyire híres, hátha szerepel ez a fotó is az internet valamelyik zugában. No nézd csak, hát itt még Czeizel Endre is beajulna, mert ennyi egypetéjű iker egy rakáson - ez már feszegeti a statisztikai hibahatárt ;-)

De az is lehet, hogy csak magyarosította a nevét, mert kaliforniai lévén esetleg nem tetszett neki a korábbi Roberta Saum. Érdekes módon ott is egy fogyókúrás terméket népszerűsít, de hát ez is biztos csak merő fatális véletlen ;-)



Összegezve a látottakat, [érdeemes picit elgondolkodni a ránk zúduló kéretlen híreken](#), ajánlatokon, spameken, és a józan eszünket is használni, mielőtt valaki csak egyetlen fillért is áldoz az ilyen "hiteles beszámolóknak" és "valódi eredmények" olvasása után varázsszerekre. Ebben a biztonságtudatos gondolkodás mellett egy jobb egérgombos fénykép ellenőrzés is egyszerűen segíthet, érdemes lehet élni a lehetőséggel.

A spamek, hoaxok, miszerint [Bill Gates elajándékozza](#) a vagyonát, de az [e-mail lottó nyeremény](#) is vagy akár [az afrikai milliomos ingyen nekünk adja a pénzt](#) történetek fényében nem túlzás, ha azt írjuk le záró tanulságnak: "Az vagy, amit elhiszel..."

[Tetszik](#) Regisztrárl, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [+1](#)

• [1 trackback](#)

Ajánlott bejegyzések:

[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Ismét nyertünk 450.000 eurót :-\)](#)
[Vajon vannak-e hihető reklámok?](#)
[Itt a foci VB, jönnek az átverések is](#)
[Már ilyen is van - ugandai 419-es átverés](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6801939>

Trackbackek, pingbackek:

[Trackback: Kamu független igazságügyi szakértői trükkkel is lop a Tigáz](#) 2014.10.18. 08:05:05

Hasonló csalássorozat zajlik a gázszolgáltatóknál is, mint a hazai bankoknál az úgynevezett devizahitelezésnél. Hibás termék a gázóra is és a gázszolgáltatók által megrendelt és fizetett igazságügyi szakértői vizsgálatok úgyszintén hibásak. Az álta...

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 2014.10.20. 19:30:24](#)

Ennél már csak az ilyen oldalak alján található kamu Facebook hozzászólási lehetőség a jobb.

Amelyek előre megírtak, de azt az illúziót keltik, hogy bárki hozzászólhat. Az egyik ilyen oldal például IP cím alapján tárolta el a hozzászólásunkat, így akármelyik böngészőből megnyitva úgy látszott, mintha mi is hozzászóltunk volna. Pedig nem, bármely más címről csak a kamu hozzászólások voltak láthatóak.

Válasz erre

Végre kiesett a Conficker féreg

2014.10.20. 10:56 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [radar](#) [adatok](#) [szeptember](#) [nod32](#) [havi report](#) [threat](#) [vírusstatisztika](#) [2014](#).

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. szeptemberében a következő 10 károkozó terjedt a legnagyobb számban.



Az előző havi eredményekhez képest talán a legnagyobb szenzáció, hogy végre kiesett a Conficker féreg. Ez egy olyan hálózati féreg, amely a Microsoft Windows MS08-067 biztonsági bulletinben tárgyalt hibát kihasználó exploit kóddal terjedt, és igazából már 2008 óta létezett rá javítás. Sajnos azonban a frissítést valószínűleg sokan nem végezték el azóta sem, így emiatt az eltűnés helyett már nyolcadik éve szerepelt a toplistánkon.



A másik "időutazó" egyébként a szintén jó régi Autorun vírus, amely cserélhető adathordozókon keresztül terjed, és az első ilyen jellegű kártevő még 2007. júniusában bukkant fel. Naprakész vírusvédelemmel, illetve kikapcsolt Autorun funkciókkal már eddig is biztonságban lehetünk, később pedig szerencsére a Microsoft is letiltotta az automatikus indulási kényelmi lehetőséget egy 2011. februárjában megjelent biztonsági frissítésben. Remélhetőleg ez a nyolc éves kártevő is hamarosan lekerülhet a toplistáról, ebben a hónapban azonban egyelőre még őrzi a 10-ik helyet.

Nézzük akkor az újoncokat, a HTML/Refresh ezúttal egyből listavezetőként bukkant fel. Ez egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található. Második helyre csúszott vissza ezúttal a mentéseket törölő Win32/Bundpil féreg. Ennek kapcsán rendszeresen kihangsúlyozzuk a saját munkáink külső adathordozóra történő rendszeres mentésének fontosságát, hiszen a legjobb stratégia mindig a megelőzés.



Kilencedik helyen találjuk a másik új szereplőnket, a Win32/Danger.DoubleExtension trójait. Ez az összevont gyűjtőneve azoknak a kártevőknek, amelyek kettős vagy többes fájlkiterjesztéssel rendelkeznek, például "AnnaKournikova.jpg.vbs". Jellemzően az első álcázó kiterjesztés valamilyen közismert dokumentum formátumé - például *.DOC, *.JPG, *.PDF - míg a tényleges fájlkiterjesztés pedig valamilyen futtatható - például EXE. Emiatt ha be van kapcsolva a Windows alatt az "Ismert fájltypusok elrejtése" opció (sajnos ez az alapértelmezett állás), akkor az óvatlan kattintással az áldozatok sajnos egyből le is futtatják az eredetileg képnek vagy más dokumentumnak gondolt kártevőt.

A hatékony védekezéshez a naprakész vírusirtó mellett [javasolt az "Ismert fájltypusok elrejtése" beállítási lehetőséget is kikapcsolni.](#)

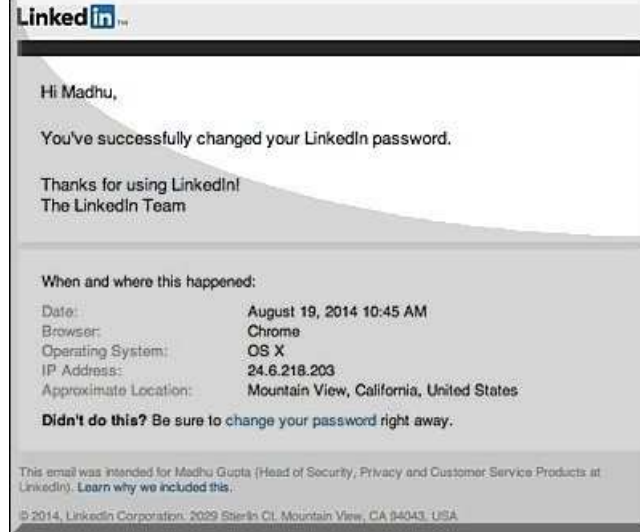


Az ESET Radar Report e havi kiadásában ezúttal az úgynevezett support csalásokról esett szó, és nem is először, hiszen az ilyen típusú támadások sajnos már évek óta zajlanak világszerte. A módszer lényege, hogy elsősorban az angol nyelvterületen élő gyanútlan áldozat kap egy kéretlen e-mailt vagy telefonhívást, melyben nem létező technikai hibára figyelmeztetik - néha arcátlanul akár a Microsoft nevében jelentkeznek - majd borsos számlát nyújtanak be a "segítségért", illetve emellett kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg elirányítani a naiv felhasználókat.

A védekezés itt természetesen az, hogy **nem hisszük el az ilyen mondvacsinált hibajelzéseket, sosem adunk ki ismeretleneknek információkat, és semmiképpen nem kattintunk általuk javasolt ismeretlen linkekre.**

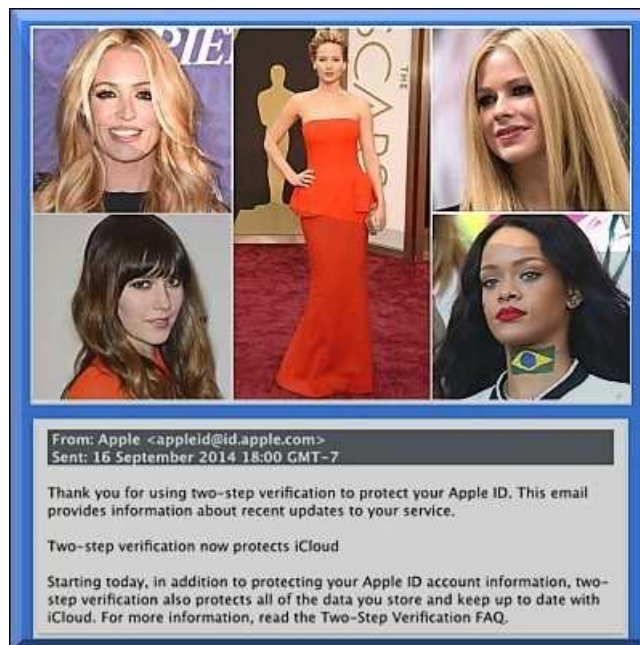


Szeptemberi fontosabb blogposztjaink között beszámoltunk arról, hogy [a CryptoLocker és a CryptoWall zsaroló kártevők tavalyi megjelenésük óta ezidáig már több, mint 1 millió dollár védelmi pénzt kasszíroztak](#) be az áldozatoktól. Érdemes tehát a szívünkön viselni a külső adathordozóra és gyakran végzett rendszeres mentéseket, mert itt valóban a megelőzés a legfontosabb teendő.



Szóba került a **LinkedIn biztonsága is, annak kapcsán, hogy a korábbi incidensek miatt [most három új elemet is bevezettek a felhasználók nagyobb biztonsága érdekében](#)**. Megjelent a bejelentkezéssel kapcsolatos kontroll, ami mostantól könnyen ellenőrizhető, ha a settings beállítások közül a "click on See where you are logged in" menüpontra kattintunk.

Emellett a **jelszóváltatásról külön e-mailes emlékeztető értesítést lehet kérni**, továbbá lehetőségünk lett a saját LinkedIn adataink mentésére is.



Az Apple iCloud incidens kapcsán eltűnődtünk, **[miért nem működött a brute force elleni védelem a Find My iPhone esetében is](#)**. A hírességek kiszivárgó meztelen fényképei miatt ugyan az Apple úgy nyilatkozott, nem felelősek a történetekért, utólag azonban végre bekapcsolták ezt.

Emellett kétlépcsős azonosítást kaptak az iCloud backupok is, valamint e-mail értesítést is bevezettek, melyben a felhasználóknak azonnal jelzik, ha valaki megpróbálja megváltoztatni az Apple ID jelszavukat, vagy valaki vissza akarja állítani az iCloud adataikat.

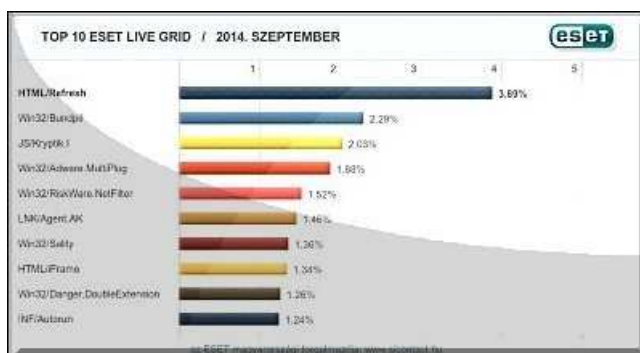


Emellett készítettünk **[egy olyan összefoglalót is, amelyben azokat a teendőket vesszük sorba, hogy mit tehetünk, ha egy éppen feltört webáruház, vagy valamilyen szolgáltatás felhasználói voltunk](#)**, ahol a támadók megszerezték a rendszerből a személyes és pénzügyi adatokat.



Végül arról is posztoltunk, hogy fény derült a [széles körben előforduló ShellShock hibára, amely a Bash parancsnnyelvel kapcsolatos](#).
 ■ **tmutatónkban részletesen leírjuk, hogy milyen teendőnk lehet, ha Windowsos, Mac-es vagy éppen Linuxos rendszert használunk.**

Összegyűjtöttük ezzel kapcsolatosan minden olyan konkrét információt, amelyek egy hétköznapi felhasználót érinthetnek, érdekelhetnek.



Vírustoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2014. szeptemberében 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.



01. HTML/Refresh trójai

Elterjedtsége a szeptemberi fertőzések között: 3.89%

Működés: A HTML/Refresh egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.



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

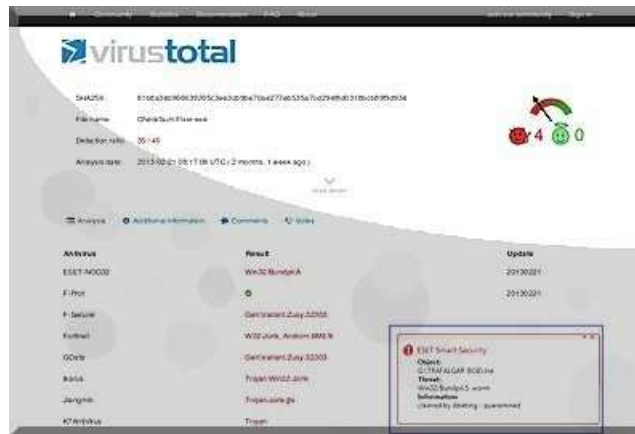


02. Win32/Bundpil féreg

Elterjedtsége a szeptemberi fertőzések között: 2.29%

Működés: A Win32/Bundpil féreg hordozható külső adathordozókon terjed. Futása során különféle átmeneti állományokat hoz létre a

megfertőzött számítógépen, majd egy láthatatlan kártevő elindított. Valódi károkozásra is képes, a meghajtóimról az *.exe, *.vbs, *.pif, *.cmd kiterjesztésű és a Backup állományokat törölheti. Ezenkívül egy külső URL címről megkísérel további kártevő komponenseket is letölteni a HTTP protokoll segítségével, majd ezeket lefuttatja.



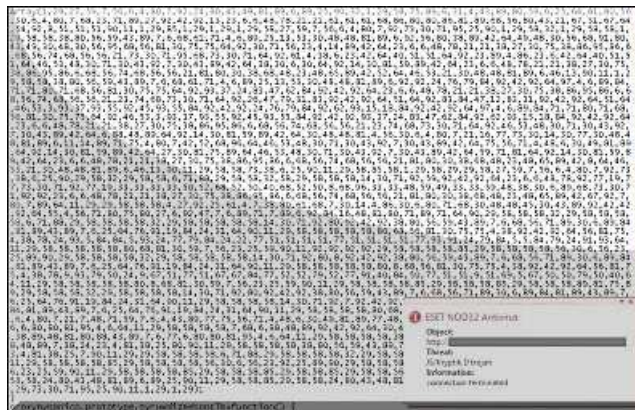
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



03. JS/Kryptik trójai

Elterjedtsége a szeptemberi fertőzések között: 2.03%

Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártevő és olvashatatlan összezárt JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártevő weboldalakra irányítja át a felhasználó böngészőprogramját.



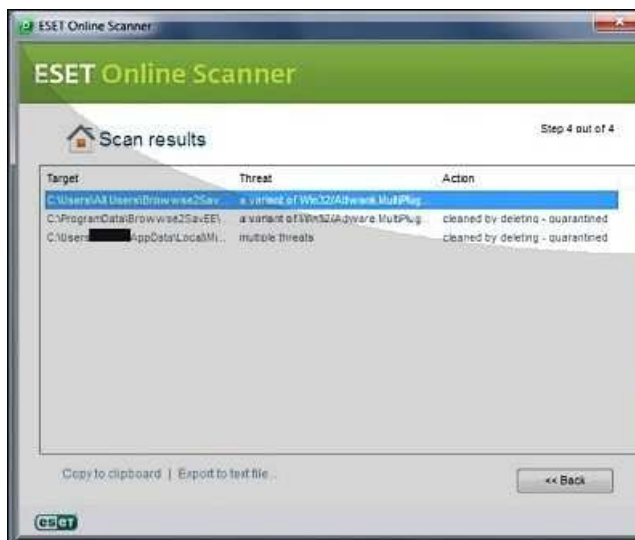
Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail



04. Win32/Adware.MultiPlug adware

Elterjedtsége a szeptemberi fertőzések között: 1.88%

Működés: A Win32/Adware.MultiPlug egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kényszerű reklámokat jelenít meg az internetes böngészés közben.



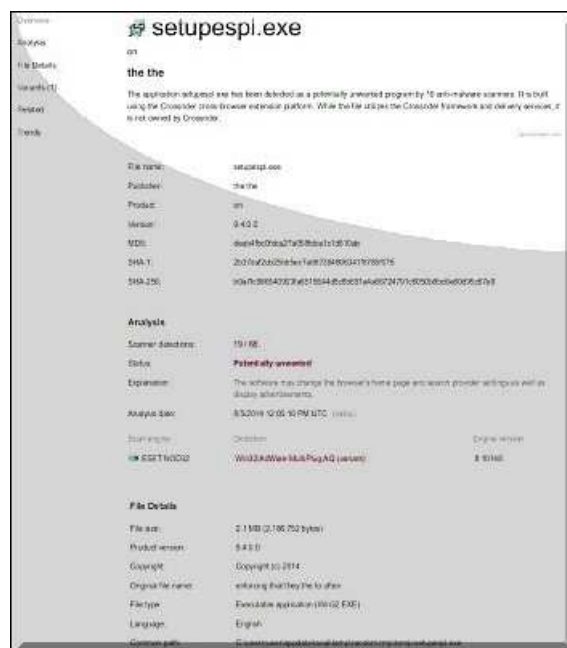
Bővebb információ: http://www.virusradar.com/en/Win32_Adware.MultiPlug.H/description



05. Win32/RiskWare.NetFilter riskware

Elterjedtsége a szeptemberi fertőzések között: 1.52%

Működés: A Win32/RiskWare.NetFilter egy olyan alkalmazás, amely magában hordoz olyan rosszindulatú kódokat, amelyek segítségével megfertőzhetik a számítógépünket, illetve a kompromittált rendszert később távolról is irányíthatóvá teszik. A távoli támadás során tipikusan adatokat lopnak el így a megfertőzött gépről, illetve távoli utasítások segítségével további kártékony kódokat telepítenek fel rá.



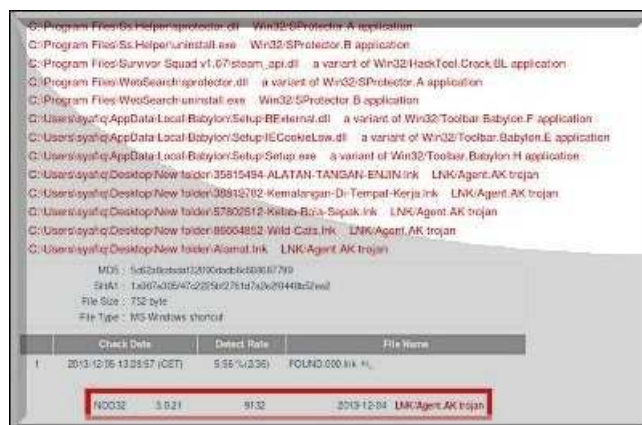
Bővebb információ: http://www.virusradar.com/en/Win32_RiskWare.NetFilter.A/description



06. LNK/Agent trójai

Elterjedtsége a szeptemberi fertőzések között: 1.46%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatot 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. Vírusselemezők 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



07. Win32/Sality vírus

Elterjedtsége a szeptemberi fertőzések között: 1.36%

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



08. HTML/Iframe vírus

Elterjedtsége a szeptemberi fertőzések között: 1.34%

Működés: A HTML/Iframe egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak Iframe tagjeibe ágyazódva egy megadott kártékony 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



09. Win32/Danger.DoubleExtension trójai

Elterjedtsége a szeptemberi fertőzések között: 1.26%

Működés: Win32/Danger.DoubleExtension az összevont gyűjtőneve azoknak a kártevőknek, amelyek kettős vagy többes fájlkiterjesztéssel rendelkeznek, például "AnnaKournikova.jpg.vbs". Jellemzően az első álcázó kiterjesztés valamilyen közismert dokumentum formátumé - például *.DOC, *.JPG, *.PDF - míg a tényleges fájlkiterjesztés pedig valamilyen futtatható - például *.EXE. Emiatt ha be van kapcsolva a Windows alatt az "Ismeret fájl típusok elrejtése" opció (sajnos ez az alapértelmezett állás), akkor az óvatlan kattintással az áldozatok sajnos egyből le is futtatják az eredetileg képnek vagy más dokumentumnak gondolt kártevőt.

Latest virus information: Win32 / Danger.DoubleExtension		September 26, 2014: Published Date
The risk for this virus: ■ ■ ■ ■ ■		
Definition name	Win32 / Danger.DoubleExtension	
If it was result of the signature check	Win32 / Danger.DoubleExtension	
Type	Trojan horse	
If it was result of the advanced heuristic inspection	If a new species of using the Troy of this original, subspecies has been detected, a warning is issued under the name "subspecies Trojan Win32 / Danger.DoubleExtension" or "NewHeur_PE".	
Corresponding period	Version 10209 (20140805) and later	
Affected platforms	Microsoft Windows	
Summary	Win32 / Danger.DoubleExtension is a generic detection name of the file that you pretend to image file or document file using the extension of two or more file names. File format is actually a PE32. Extension that represents the executable format is also attached to the tail end.	

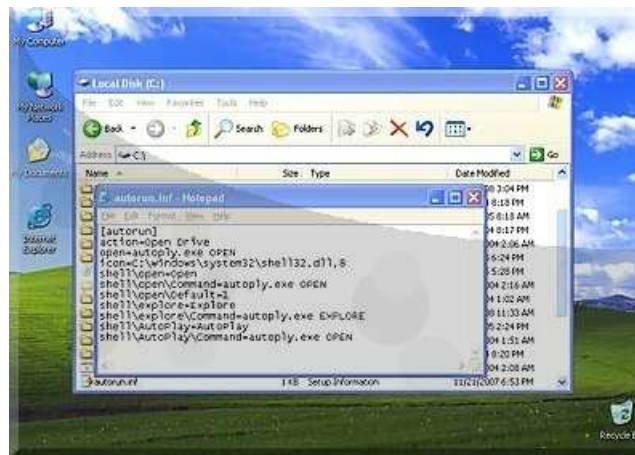
Bővebb információ: http://www.virusradar.com/en/Win32_Danger.DoubleExtension/detail



10. INF/Autorun vírus

Elterjedtsége a szeptemberi fertőzések között: 1.24%

Működés: Az INF/Autorun gyűjtőnéve az autorun.inf automatikus programfuttató fájlt használó károsítóknak. 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>

 Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[A HTML trójaiak riogattak minket októberben](#)

[Vírstoplista 2014. augusztus hónap](#)

[Júliusi vírustoplista](#)

[Júniusi vírustoplista](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6809963>

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 hamis antivírus halott és élvezi

2014.10.22. 12:01 | [Csizmazia Darab István \[Rambo\]](#) | [6 komment](#)

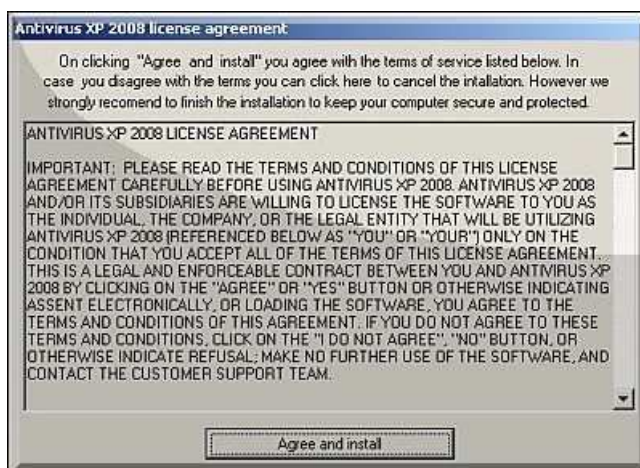
Címkék: [telefon](#) [adware](#) [csalás](#) [hamis support](#) [antivirus](#) [scareware](#)

Szóval a hamis antivírus fenyegetések valójában mégsem haltak ki, azóta sem szűntek meg létezni, inkább úgy lehetne leírni a helyzetet, hogy jó evolúciós alanyként szépen alkalmazkodnak a körülményekhez, és időnként képesek egy-egy újabb hatékony csavart belehelyezni a történetbe.



A hamis antivírusok eredetileg úgy nagyjából 2008 táján érkeztek, kezdetben még XP Antivirus 2008, 2009, és [hasonló neveken értek el brutális bevételeket](#).

A nem létező vírusokkal való ijesztgetésen túlmenően egy idő után mindig hozzáadtak valami újdonságot is a készítőik, amiket mi itt a [jó oldalon nehezítésnek éltünk meg](#). Például szándékosan nem volt uninstall, és sok esetben szembesültünk azzal, hogy a program törlése utáni gépindításnál mégis visszakerült valahogyan.



Volt aztán olyan „vicces” és kilométer hosszú, apró betűs licencszerződés, amelyen nem a szokásos „elfogad” és „elutasít” gombok szerepeltek, hanem csak egyetlen opció volt: az elfogadni gomb, pluszban az ablak felső sarkából még az X, azaz bezár funkció is hiányzott.

Valódi alkalmazás nevekre hasonlító programnév és folyamatnév, a Feladatkezelő letiltása, és reggelig sorolhatnánk a trükköket. Akit a zsaroló programok története részletesebben is érdekel, annak [érdeemes lehet elolvasni az ezzel foglalkozó korábbi összefoglalónkat](#).



Rátérve az újabb eseményekre, itt is hasonló felugró ablakok bukkannak elő, amelyek azt próbálják elhitetni velünk, hogy a rendszer fertőzött, és az eltávolításhoz szakértőre van szükség, aki segíthet ebben. Az ilyen böngészés közben megjelenő reklám ablakok sokféleképpen kerülhetnek a képernyőnkre: lehet a rosszindulatú hirdetés egy általunk telepített ártalmatlannak tűnő böngésző kiterjesztésben, valamilyen ingyenes programban, sok olyan játék, de még felhasználói segédprogram - rendszer optimalizáló, fájlkonverter, stb. - is tartalmazhat ilyet.

Persze a hatásosabb fenyegetés érdekében az ilyen üzenetekben nem mulasztják el megemlíteni azt sem, hogy [az állítólagos fertőzés miatt veszélyben lehetnek a személyes és pénzügyi adataink is](#).



És itt jön a plusz csavar, mivel a feltüntetett "segítő szakértő", aki ugye mondanunk sem kell, hogy 24/7 rendszerben várja a hívásunkat, **máris hozzáteszi a hamis support komponenst** a történethez. Magyarán már nem ők telefonálnak hideg hívással a Microsoft nevében ismeretleneknek, mint régebben, hanem nyugodtan várják az átvert felhasználók hívásait.

A végeredmény pedig [a hamis support csalásokból már jól ismert forgatókönyv alapján folytatódik](#): vagy csillagászati összeget kérnek az úgynevezett "segítségért", vagy a telefonban olyan rosszindulatú webhelyre irányítanak minket, ahonnan backdoort telepítenek a gépünkre, de az is lehet, hogy mind a kettőt együtt.

 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

- [Telefonos support vagy mégsem](#)
- [Újabb trükkök a hamis antivírusoktól](#)
- [Hamis antivírus örökön örökre](#)
- [Közös fellépés a support csalások ellen](#)
- [Nincs hamis AV banki szemhunyas nélkül](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6816677>

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](#).

szigetipotyautas •

**<http://kommentanemkommentalhatora.blog.hu> 2014.10.22.
16:42:46**

Mondd, az androidos alkalmazásokban rendszeresen megjelenő "Potenciális veszély észlelése! Telefon szkennelése" típusú hirdetésekről tudsz valami közelebbit?

Csak aljas reklámok vagy ezek is hordoznak valami fertőző kódot?

Szinte az összes ingyenes programom ilyenekkel szórakoztat, ha épp nem akkumulátor élettartamot növelő csodaszert reklámoznak.

Amennyiben valóban malware terjesztésről van szó, akkor jó lenne valahogy jelezni a google felé, de hol, hogyan? Megnyitni nem merem, nehogy valamit összeszedjen a mobilom, így meg csak annyit látok, hogy valami bosszantó szemét tolul a képembe, amikor élő netkapcsolat mellett nyitom meg mondjuk a file manager applikációm.

Válasz erre



[vanvelemenym](#) 2014.10.23. 23:15:25

Az általad észlelt figyelmeztetésekhöz nem tudok hozzászólni, de az avast! -nak is van androidos antivirus megoldása, de az android saját weboldalon is találsz.

Az akkumulátor élettartam novelo kb olyan "hatekony", mint egy vonatkerekek-pumpalo kollega.

Válasz erre



[vanvelemenym 2014.10.23. 23:17:48](#)

Bocs, elfelejtettem írni, hogy nekem a tableten is és a telefonomon is f-secure van (fizetos)

Az avast! ingyenes

Válasz erre

[szigetipotyautas •](#)

[http://kommentanemkommentalhatora.blog.hu 2014.10.24. 09:21:31](#)

@vanvelemenym: köszi, de ugye azt te is tudod, hogy ezek sem védenek 100% biztonsággal? Ezért gyanús linkekre inkább nem megyek rá. Inkább jelenteném a google felé, mivel ha nem is okoznak kárt, akkor is tisztességtelen módszer, amit használnak.

Válasz erre



[vanvelemenym 2014.10.24. 16:40:39](#)

@szigetipotyautas: Nincs 100%-as antivirus program, az ostoba juzerek ostoba cselekedetei ellen nincs 100%-os védelem. De az avast! pl. segít megvédeni, legalábbis nekem sosem volt bajom, riasztott, ha kellett, stb. De ma már az f-securet használom (ami fizetos), mert egyéb okok miatt megerte egy nagyobb csomagot venni, és így az egy eszközre jutó költség kicsit kisebb.

Amúgy örök szabály, hogy az ingyenes vagy nagyon olcsó dolgok a legdrágábbak, pl ha egy "ingyenes" app valójában phishing, és lenullazza a bankszámlád, vagy "csak" zombiként használja a géped, de ha nagyon szerencsés vagy, akkor csak az összes ismerosod kap egy csomó spamet, stb.

Szerintem a guglit nem nagyon érdekli, hogy a jüzer milyen programokat tölt le, és az appok ártalmasságát nem a "tisztességtelen" fokozattal keresik. Linkekre pedig akkor sem szabad kattintani, ha nem gyanús, és a legjobb barátod küldte, hogy jaj de cuki csajok, és, ha a banktól kapsz levelet, akkor se kattints, hanem kezzel potyogd be a bankod linkjét, sose a levelben kapott linkrol indulj stb.

Válasz erre

[szigetipotyautas •](#)

[http://kommentanemkommentalhatora.blog.hu 2014.10.24. 17:25:38](#)

@vanvelemenym: víruskeresőm van, de annyira nem bízom benne, hogy ilyen reklámokat ellenőrizzek.

A Google meg, ha ártalmas linket jelzel feléjük, azért utána szokott nézni, csak az a gáz, hogy ezek applikációból nyílnának, nem tudom kimásolni belőle a linket. Ezért érdekel, hogy tud-e róla valaki közelebbit.

Válasz erre

Twitter bejelentkezés másképpen

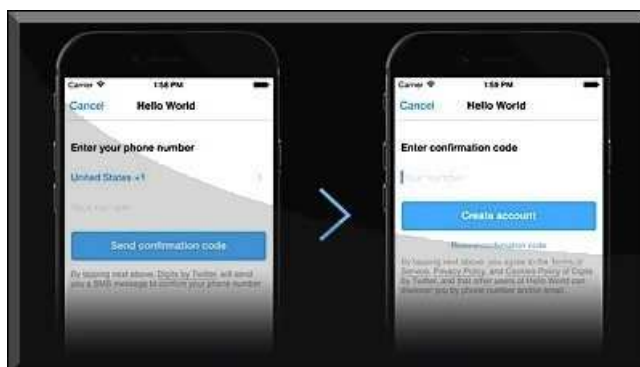
2014.10.27. 12:44 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [biztonság](#) [jelszó](#) [twitter](#) [telefonszám](#) [mikroblog](#) [welivesecurity.com](#) [kétfaktor](#)

Egy újszerű belépési módot kínál a Twitter a felhasználók számára. Az elgondolás lényege, hogy nem muszáj ragaszkodni a **hagyományos jelszavak begépeléséhez**, hanem mostantól arra is mód nyílik, hogy a **telefonszám azonosítja a felhasználót a bejelentkezéskor**.



Az eredeti elgondolás, illetve ennek kommunikálása arra alapoz, hogy sokan egyes fejlődő országokban - Brazília, India és Indonézia -, [ha Twitterezni akarnak, állítólag nehézséget jelenthet nekik egy ehhez szükséges e-mail cím regisztrálása](#). Erre született meg válaszul az a megoldás, hogy a **belépéshez egy olyan szolgáltatást használnak fel, amely bekéri a felhasználó telefonszámát, és oda küld egy bejelentkezéshez szükséges kódot**, amit minden egyes alkalommal be kell gépelni.



Ez a banki SMS aláíráshoz hasonlóan igyekszik két faktoros azonosítás lenni, **bár ez ha magán a telefon jelentkezünk be, akkor már csak másfél faktor**, hiszen akkor a klasszikus fizikailag két különböző készülékes modell helyett itt ugyanarra az egy eszközre kapjuk a kódot. Ennek a konstrukciónál a gyengeségét jól jellemzi, hogy erre [már 2011-ben is létezett például olyan, Zeus Mitmo nevű trójai kártevő, amely a fertőzött telefonon sikeresen elfogta a bankból érkező SMS aláírási üzenetet](#).



Természetesen érdemes megemlíteni a lehetséges ellenérveket is. Sokan úgy gondolják, **ez addig jó, amíg nem lesz kötelező, hanem csak egy választható opció**. Emellett felmerülhet egy olyan aggály is, hogy ha az üzemeltetők később eladják az adatbázist, akkor onnantól mindenkit elboríthat majd az SMS spam, meg a kéretlen reklám hívások áradata. Ami például a [MoPub tavalyi 350 millió dolláros felvásárlása után](#) lehet, hogy nem is annyira utópisztikus félelem.



A [The Verge cikkében emellett arra is kitér](#), hogy igaz ugyan, hogy nem könnyen, de a telefonszámok klónozása is megoldható. A legtöbb ember számára mégis megfelelő megoldást jelenthet a fenti módszer, illetve **a pusztán csak jelszavas belépéshez képest két készülék használatával azért biztonságosabb**. A technológia mostanra már 28 nyelven és 216 országban elérhető, iOS, Android platformon, valamint a hagyományos webes elérésnél, beleértve ebbe a magyar nyelvű lehetőséget is.

 **Tetszik** Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Amikor mások baltázzák el - part II.](#)
[Napi 160 ezer Facebook account esik el](#)
[Kormányzati e-mailek kontra biztonság](#)
[Lopott Minecraft jelszavak szivárogtak ki](#)
[Biztonsági konferencia - nyitott wifi honeypot-tal](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6836967>

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.

Hogyan védekezzünk botnetek ellen?

2014.10.29. 10:00 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

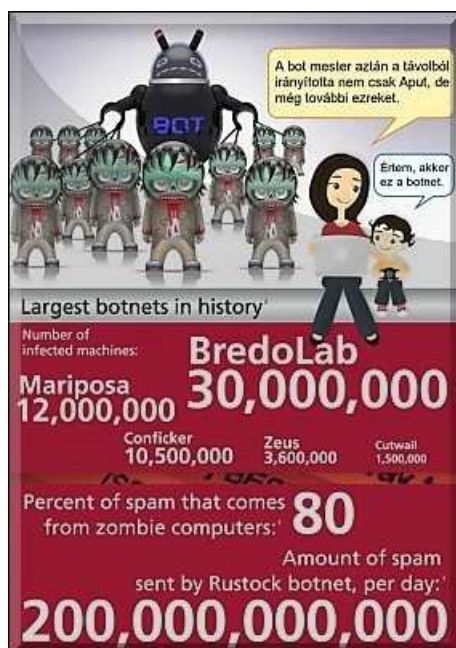
Címkék: [security](#) [smart védelem](#) [zombi](#) [8 botnet](#) [nod32](#) [eset](#) [techológia](#)

Ha végignézünk néhány nagy és hírhedt botnetes támadást, akkor azt láthatjuk, hogy ezek az **automatizált kártékony programok, amelyek megtámadják a javítatlan biztonsági résekkel rendelkező számítógépeket, óriási károkat képesek okozni.** Mivel a támadók egyszerre nagyszámú számítógép felett veszik át az uralmat, az így kialakult zombihadsereg nem csak szolgáltatásmegtagadásos (DDoS) támadásokban, spam levelek terjesztésében vehet részt, hanem **ma már jellemzően a botnetek segítségével terjesztik tovább a kártevőket, és fertőznek meg újabb számítógépeket.**



Ha a botnet jelen van a számítógépen, akkor a korábban felsorolt veszélyek mellett - **DDoS támadásokban való részvétel, spam levélszemét üzenetek terjesztése - sajnos az is jellemző, hogy a fertőzött gépekről egyúttal eltulajdonítják az összes személyes és bizalmas adatot is,** így áldozatul eshetnek a banki hitelesítő adataink, belépési jelszavaink vagy a hitelkártyaszámaink.

Milyen jelek segíthetnek még felfedezni - természetesen a víruskereső jelzésén kívül - hogy esetleg egy zombihálózat tagjai vagyunk?



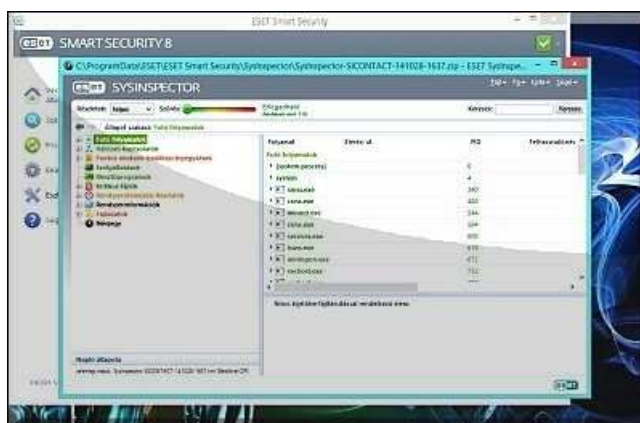
Ilyen jellegzetes szimptóma lehet például, hogy túlságosan sokszor pörögnek fel ok nélkül a hűtőventilátorok jelezve azt, hogy erősen dolgozik a gép, akkor is, amikor éppen nem is dolgozunk rajta. **Vagy túlságosan sok ideig tart, amíg a gép kikapcsol (shutdown), sőt esetleg ez nem is sikerül neki.**

A barátok, családtagok, vagy ismerősök azt jelzik, furcsa leveleket, esetleg csak egy szöveg nélküli, de linket tartalmazó üzeneteket kaptak tőlünk, pedig mi nem is küldtünk nekik semmit.



De az is intő jel lehet, ha a programjaink igen lassan futnak, vagy **a rendszer nem engedi letölteni a legfrissebb Microsoft frissítéseket, a legfrissebb vírusadatbázist**, illetve egyes vírusvédelmi weboldalak nem is jönnek be a böngészőben.

Sokféle gyanús momentum fordulhat elő, attól kezdve, hogy **rövidebb-hosszabb ideig az internet sebessége drámaian lelassul** egészen addig, hogy hirtelen popup ablakok kezdenek el megnyílni, reklámok jelennek meg vagy pedig **a Windows Feladatkezelőjében furcsa nevű programok, folyamatok tűnnek fel**.



A most debütált az ESET Smart Security 8 legújabb kiadásában többek közt már olyan új funkciókat is láthatunk, mint a **Botnet elleni technológia**. Mire jó ez nekünk? A védelem kiegészítő pilléreként segíti a kártékony programok felfedezését azáltal, hogy elemzi azok hálózati kommunikációs mintáit és protokolljait.

A botnet elleni védelem gyakran változik a hálózati protokollokkal szemben, amelyek az elmúlt években változatlanok maradtak. Az ESET ennek az új technológiának a segítségével nyújt **védelmet azok ellen a kártévők ellen, amelyek az észlelés megkerülését megkísérelve megpróbálják a számítógépet a botnet hálózatához csatlakoztatni**.



2013-ban is már számos nagy horderejű botnet támadás tanúi lehettünk, ilyen volt például **az ESET kutatói által feltárt Operation Windigo is tavasszal**. Ennek leleplezésében is szerepet játszott, hogy sikerült felfedni a botnetek normál hálózati kommunikációs mintáktól eltérő forgalmát. **Ennél az incidensnél a 25 000 megfertőzött szerver több mint két éven keresztül naponta félmillió webes látogatót irányított rosszindulatú oldalakra**.

Mindent egybe vetve, a támadóknak sikerült naponta több mint 35 millió spam üzenetet küldeniük a botnet segítségével. A Verizon Data Breach 2014-es jelentéséből szintén az derül ki, hogy **a botnet tevékenység volt a kártékony programok legjelentősebb kategóriája (86%) az utóbbi időszakban**.

Megosztom [tumblr](#) [Tweet](#) [PinIt](#) [+1](#)

Ajánlott bejegyzések:

[Védekezés exploitok ellen](#)

[Zombi-e vagy?](#)

[Itt a lopásvédelemmel ellátott Smart Security 6](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6841339>

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.



Samsung lock Oleg Pliss nyomdokain

2014.10.31. 08:26 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

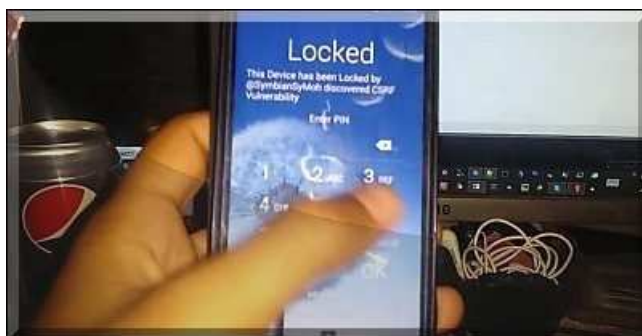
Címkék: [samsung mobile hálózati my biztonsági lock rés távoli find elérés](#)

A korábbi incidensnél, ahol ausztrál iPhone és iPad felhasználókat zártak ki készülékeikből, többek közt azt a tanulságot szűrhetjük le, hogy felettebb fontos dolog a mindenhol egyedi jelszó. Mert [mindig is lesznek olyanok, akik nem lesznek restek, és a máshonnan kiszivárgó accountokat mindenhol](#), például az Apple Find My iPhone szolgáltatáson is végigpróbálgatják.

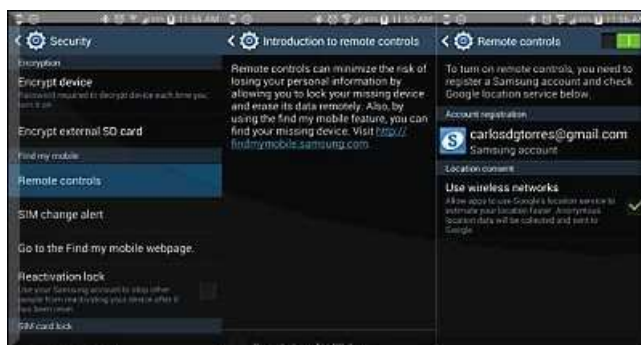


Ugye a korábbi történet lényege az volt, hogy a lezárt telefonhoz való hozzáférést csak 50 USD váltságdíj fizetése ellenében kaphatták volna vissza az áldozatok. Nos ehhez a zsaroláshoz kísértetiesen hasonló veszélyre figyelmeztetnek most a Samsung okostelefonok esetében.

Ha a "Find My Mobile" engedélyezve van a készüléken, úgy a támadóknak lehetőségük nyílik távolról lezárni azt és közben megváltoztatni a feloldó kódot - kizárva ezzel a tulajdonost. Vagyis az eredendően jó célokat szolgáló hasznos funkció - amely lehetővé teszi, hogy a készülék elvesztése vagy ellopása esetén a távolról zárolhassuk azt - sajnos [ártó szándékkal is kihasználható](#).



A rést felfedező [egyiptomi kutató videóban is bemutatta](#), hogy egy Samsung Galaxy SIII esetében mindez hogyan néz ki. Emellett ugyancsak aggodalomra adhat okot még az a tény is, hogy ha egy felhasználónak már létezik Samsung fiókja, és alapértelmezetten nem aktív nála a hálózaton keresztüli távoli hozzáférés, [sajnos tudta és beleegyezése nélkül akkor is be lehet ezt kapcsolni](#).



A sérülékenységgel kapcsolatban a Mashable kérdésére a Samsung azt válaszolta, komolyan veszik a biztonsággal kapcsolatos bejelentéseket, és jelenleg már vizsgálják ezt az esetet is. A National Vulnerability Database bejegyzése szerint a Samsung készülékek egyáltalán nem ellenőrzik azt, hogy milyen forrásból kapják a lezáró kódot, így [a sebezhetőség besorolása 7.8, azaz magas kockázatú lett](#).



[f Tetszik](#) Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Sebezhető-e vagy?](#)
[Károkozási ki mit tud](#)
[Mit tegyek, ha ellopják az androidos telefonomat?](#)
[Célkeresztben a telefontolvajok](#)
[IDC Biztonsági Konferencia 2014.](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6850195>

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](#).

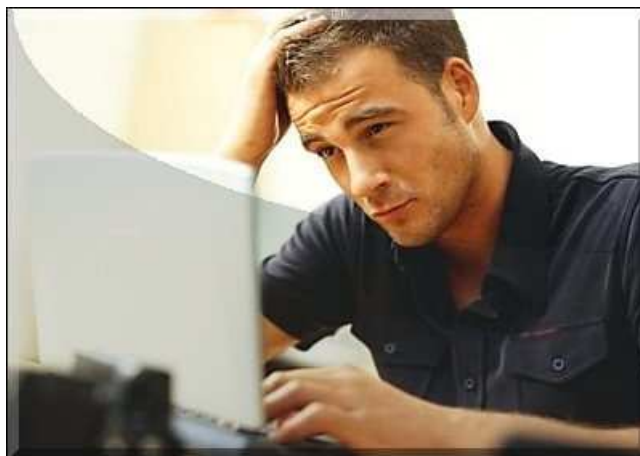
Nincsenek hozzászólások.

Gépeinket is támadják a zombik

2014.11.04. 09:05 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [spam halloween](#) [fertőzés](#) [sample átverés](#) [zombi botnet](#)

Az ESET kutatói Halloween alkalmával **védelmi tippeket** adtak az ilyenkor fokozódó veszélyek miatt, és emellett **összegyűjtötték az eddigi öt legfélelmetesebb zombi botnetet** is.



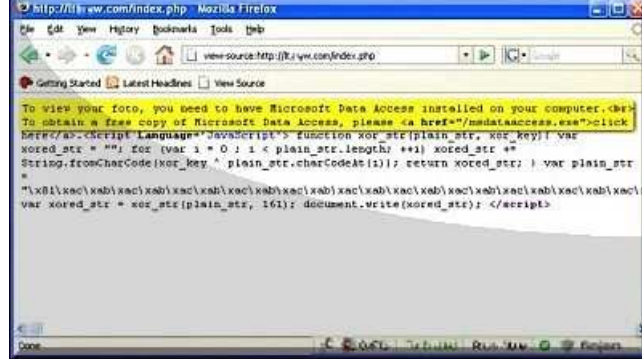
Ha az online veszélyektől szeretnénk megóvni magunkat, úgy először is legyünk óvatosak a Halloween tárgyú e-mailekkel. **Halloween, mint minden más ünnep, külön figyelmet kap.** A támadók ilyenkor a social engineering (pszichológiai manipuláció) használatával próbálják meggyőzni áldozatukat az általuk küldött fertőzött levél ártatlanságáról. Ha nem várunk hasonló tárgyú leveleket, akkor inkább egyszerűen ne nyissuk meg ezeket az e-maileket, mert könnyen áldozatokká válhatunk.

Frissítsük az antivirus megoldásokat a számítógépünkön és a mobil eszközeinken. Ha még nem rendelkezünk ilyennel, akkor telepítsünk egyet. Mára már egyáltalán nem menő a "Tudom mit csinálok az interneten, nekem nincs szükségem védelemre!" és az "Én biztonságos platformot használlok." kifogások. A mai kártevők már kihasználják a böngészőben található biztonsági réseket, így amint meglátogatjuk a fertőzött oldalt, már kattintás nélkül elkezdik megfertőzni a számítógépünk. **Korábbi megfigyelések alapján Halloweenkor az ilyen típusú támadások száma növekszik.**

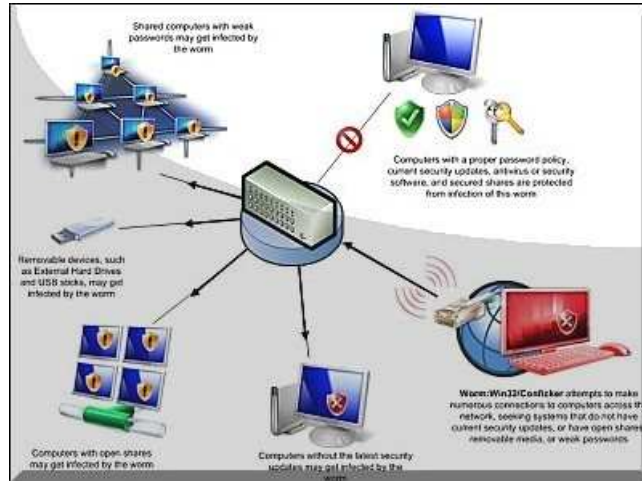


Állítsuk be a frissítések rendszerességét és automatikus indítását. Túl sok programot használunk már ahhoz, hogy egyesével manuálisan frissítsük őket a számítógépünkön. Ne feledjük, hogy minden szoftvert frissíteni kell, nem csak az operációs rendszert, a böngészőket és az antivirus programokat. Fontos, hogy a PDF olvasó, a Java, az Office programok és a videó lejátszó is mindig naprakész legyen, így minimalizálhatjuk rendszerünk sérülékenységének veszélyét.

Figyeljünk, miközben a neten keresgélünk: Halloween ideje alatt a Google, Bing vagy Yahoo felületeken a fertőzött oldalak jobb elérést igyekeznek elérni etikátlan, nem engedélyezett keresőoptimalizálási módszerek (BlackHat SEO) segítségével, így könnyebben katinthatunk veszélyes oldalakra. Ebben az időszakban még jobban figyeljünk a kattintásainkra és védjük számítógépünk és mobil eszközeinket antivirus programokkal, amelyek segítenek felismerni az ilyen típusú veszélyeket is. Most pedig következzen az ESET szerinti öt legfélelmetesebb zombi hálózat listája:



Storm – A legrégebbi malware a listán, az egyik legkorábbi botnet, amely olyan technikákat kezdett alkalmazni, amely a későbbi kártevők alapja lett. A gyorsan és nagymértékben terjedő kártevő tíz millió Windows rendszerű gépet fertőzött meg. Ez volt az első olyan nagyobb botnet is, amely anyagi jövedelmet hozott a tulajdonosainak.



Conficker – Fénykorában több millió Windows gépet fertőzött meg: egyes számok szerint több mint 15 milliót. A filmekben is, ha egy, az életünket kockáztató, elsőprő erejű katasztrófa közeleg, akkor egy szakértői csoport kialakítása a legkézenfekvőbb mód a védekezés elkezdésére. Itt sem volt ez másképpen: olyan nagymértékben terjedt a fertőzés, hogy megalakították a Conficker Working Group nevű csoportot, mely aztán felvette a harcot a károkozóval. Hat évvel az első felfedezése óta, még a mai napig léteznek megfertőzött számítógépek szerte a világban.

Zeus – Ez a malware nem egyszerűen csak egy sikeres botnet, hanem egy olyan kártevő is, amely online banki kódokat lopott különféle fertőzött mobil eszközökről (Symbian, Windows Mobile, Android és Blackberry). 2012-ben az US Marshals technikai csapata győzte le a botnetet. A kártevőt létrehozók nem télenkedtek: az eredeti botnetből elraktározva egy darabot újraleszítették Gameover Zeus néven, amelyet csak idén nyáron sikerült az FBI és partnereinek hatástalanítania. De még ez sem volt elég ennek a "ragadozónak": még egyszer feltámasztották a zombi hálózatukat. A tavalyi év Cryptolocker nevű vírusát is a Zeus különböző variánsai terjesztették.

Mit lopott el a Flashback?

CVE-2011-3544
CVE-2012-0507
CVE-2012-0507

UUID & Mac címek
Egyedi azonosító szám a Mac OS X operációs rendszert futtató számítógépekhez.

OS verzió
A Mac operációs rendszer verziója

Személyes adatok
Látogatott weboldalak, keresési kifejezések, és más adatok

Flashback – Azoknak az embereknek, akik abban a hitben éltek, hogy a Macintosh gépeket nem lehet vírussal fertőzni, ez a kártevő kisebb-nagyobb sokkot jelentett. Bebizonyosodott, hogy a Mac gépek is ugyanúgy "kaphatnak" vírust, sőt a megfertőzött gépek hatalmas botnetek részévé is válhatnak. Az Apple gépek nagy része, mintegy 600 000 számítógép fertőződött meg ebben a nagy erejű támadásban világszerte. Ez a botnet most éppen nem aktív, de bármikor azzá válhat.



Windigo – Látszólag ez a botnet is ugyanolyan, mint a többi: fertőzött gépekről lop el adatokat, vagy kéretlen leveleket küld szét a világba. Akár még kedvelhetnénk is ezt a zombit, mivel a többihez képest "csak" néhány tízezer gépet fertőzött meg. Viszont úgy néz ki, hogy a botnet alkotói szépen lassan építik fel zombi hadseregüket, így egy időre mindig láthatatlanná válhatnak és megbújhatnak. A több tízezer Windigo által megfertőzött Linux alapú számítógép illetve szerver pedig addig is több millió emberhez juttatja el a vírust.

 **Tetszik** Egy személy kedveli ezt. [Regisztráld](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Tíz gyanús jel, hogy zombi-e vagy](#)
[Ami a csövön kifér](#)
[A LinkedIn support üzent nekünk. Vagy mégsem?](#)
[Közelgő Karácsony, szaporodó adathalászat](#)
[Átverés a Google spam](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6861391>

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.

Gyorshajtási bírsággal is terjed a CryptoLocker

2014.11.06. 08:32 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [social autó büntetés gyorsajtás bírság váltságdíj engineering zsaroló cryptolocker](#)

Az eléggé figyelemfelkeltőre sikeredett cím igazából arra utal, hogy a lelemény milyen sok mindenre nem képes. Az **ausztráliai Új-Dél-Walesben figyeltek fel ugyanis arra trükkre, hogy az e-mailben terjedő üzenetekben hamis linkek segítségével egy állami hivatal nevével visszaélve** igyekeztek a gyanútlan és talán gyorsan is hajtó felhasználók gépeire kártevőt letölteni.



A felhasználók ebben az esetben látszólag "helybe mennek a pofonért", ugyanis a **hamis State Debt Recovery Office (SDRO) weboldalán meg kell adniuk egy Captcha kódot, aminek hibamentes begépelése után éppen saját maguk töltik le az offence_id_37984264.zip névre hallgató kártevőt.**

Azon túlmenően, hogy a levélben kapott állítólagos bírságot azonosító kód és a letöltési ID nem is egyezik, illetve hogy az eredeti és a hamis állami adósságbehajtó iroda weblapjának kinézete sem teljesen egyezik, a ZIP archívum egy hasonló nevű [futtatható offence_id_37984264.exe rejt magában, amit lefuttatva aztán beindul](#) a már jól ismert forgatókönyv.



Az összes felcsatolt hálózati, betűjeles felhőtarhely és csatlakoztatott helyi adattároló eszköz állományait meglövi a titkosító váltságdíjszedő kártevő egy 2048 bites RSA kulccsal. Erről pedig azt kell tudni, hogy a mentés, helyreállítás sokszor nehézkes, vagy időnként akár lehetetlen, emiatt [az lehet a legfontosabb, hogy a nagyobb hangsúlyt mindig a megelőzésre, és a mentések készítésére tegyük.](#)

Azt sem árt tudni, vagy inkább megismételni, hogy **semmilyen garancia nincs** arra, hogy az esetleges váltságdíj fizetés után valóban hozzáférünk az adatainkhoz: ez vagy így lesz, vagy nem.



[A CryptoLocker állomány titkosító kártevő eredetileg meg 2013-ban indult](#) el világhódító útjára. 2014-ben az Egyesült Királyságban már a számítógépek 3%-át meg is támadta, az áldozatok közül pedig a váltságdíjat fizetők aránya 40% volt.

A kezdeti 300 dolláros ár azonban időközben szépen megemelkedett, most éppen 500 dollárnak megfelelő Bitcoint kérnek, ám késedelmes fizetés, vagyis 5 nap leteltével ez már megduplázódik, és egészen 1000 USD-re nő.



Említsük még meg, hogy a social engineering minden lehetőségre lecsapó e módszere nem teljesen előzmény nélkül való, ugyanis egy ehhez hasonló ötletet már 2009-ben is kitaláltak, akkor az autók szélvédőjére kaptak csali értesítő levelet az áldozatok azzal az ürüggyel, hogy állítólag lefotózták és megbüntették autóikat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetik az inkriminált képeket. A büntetécédulák persze hamisak voltak, [a weboldal pedig kártékony szoftvereket próbált telepíteni](#) az áldozatok számítógépére.

Megosztom [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Véddij a CryptoLocker terjesztőjének fejére](#)
[Újra itt a CryptoWall zsaroló kártevő](#)
[Magyarországra is megérkezett a CTB-Locker](#)
[Bitcoinos zsaroló járja be Európát](#)
[Újabb adathalász kísérlet a Yahoo! ellen](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6869149>

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.

Védekezés exploitok ellen

2014.11.10. 09:00 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [java](#) [security](#) [smart védelem](#) [8](#) [nod32](#) [eset](#) [exploit](#) [techológia](#)

A világ már csak ilyen, logikus szabályokra épül, ahol minden egyes szereplőnek megvan a maga érdeke. A szoftverfejlesztők az, hogy a javításkor húzzák az időt, és kijelentsék, hogy nincs tudomásuk az adott sérülékenységet konkrétan kihasználó esetről. A támadóknak pedig az, hogy egy-egy javítással még nem rendelkező hibát minél hamarabb és minél intenzívebben kihasználjanak, de persze eközben nem dobják sutba a régebbieket sem, hiszen nagyon sokan különböző okokból hosszú időn át egyáltalán nem frissítenek.



A nulladik napi kihasználható kódokra erős vásárlói igény jelentkezik a piacon, [több féle árverési portál is létezik hozzájuk](#). Ezek segítségével könnyen támadhatók célzottan vagy tömegesen a rendszerek, néhány esetben pedig egész stratégiát is építenek köré a támadók.

Emlékeztet lehet például, hogy [a 2014-es április Windows XP technikai támogatás kezdetéig bespájzoltak a zero dayekből](#) a kártevőterjesztők, és türelmesen kivárták azt az időszakot, amikor már nem jelennek meg többet javítófoltok.



Hogy mit tehetünk a már ismert sebezhetőségek esetén, arról már sokat beszéltünk. Használjuk a naprakész vírusvédelmi rendszerünket, és persze emellett ugyanilyen fontos, hogy mind az operációs rendszert, mind az összes alkalmazói programunkat rendszeresen és gyors reakcióidővel frissítsük. Az automatizált patch management elvégzésére több hasznos kiegészítő eszköz is létezik, az egyik ilyen például a Secunia Personal Software Inspector (PSI).



Szerencsére azonban az új sérülékenységek ellen is léteznek bizonyos lehetőségek [az ESET Smart Security programban](#), elsőként

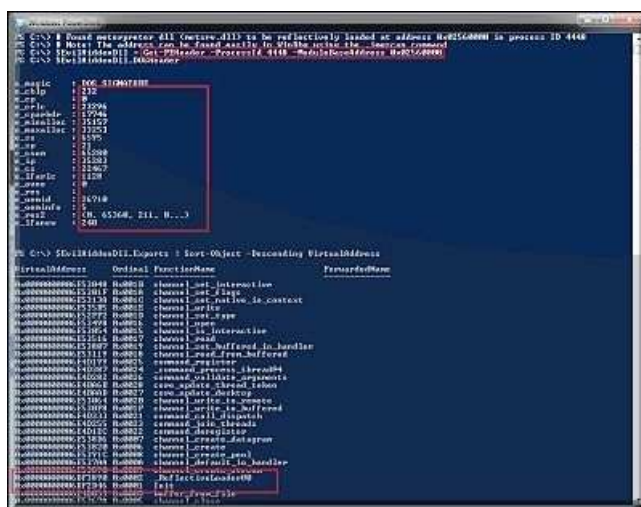
például említhetjük az úgynevezett Exploit blokkoló modul. Ez a támadásoknak gyakran kitett alkalmazástípusok, például webböngészők, PDF-olvasók, levelezőprogramok és MS Office-összetevők, folyamatok viselkedésének figyelésével olyan gyanús tevékenységeket keres, amelyek biztonsági résekre utalhatnak.

Amikor az Exploit blokkoló gyanús folyamatot talál, képes azonnal leállítani azt és rögzíteni a kártevőre vonatkozó adatokat, amelyeket elküld a ESET Live Grid felhőrendszernek.



Létezik emellett egy **Java Exploit blokkoló bővítmény is**, amely pedig a Java rendszert figyelve abban segíthet, hogy biztonsági rések kiaknázására utaló viselkedéseket keres.

Ennek folyamán a modul által blokkolt minták jelenthetők a kártékony programokra szakosodott elemzőknek, akik további elemzést végeznek a gyanús kódon, és szükség esetén vírusdefiníciók létrehozásával blokkolhatják őket a különböző rétegeken (például URL-blokkolás, fájlletöltés stb.)



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.

Amikor még hackelni sem kell a kukkoláshoz

2014.11.12. 13:24 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [admin](#) [biztonság](#) [webkamera](#) [kamera](#) [password](#) [default](#) [webkamerás](#) [kukkolók](#) [welivesecurity.com](#) [insecam.com](#)

A korábbi frappáns alcímű írásunk, miszerint "[Éljen és virágozzék az alapértelmezett jelszó](#)" úgy tűnik, sanos nem vezetett el arra az eredményre, hogy azóta mindenkinek a legelső dolga legyen az azonnali jelszó csere. Az [Insecam.com](#) nevű júniusban regisztrált weboldal azzal igyekszik sokkolni, illetve figyelmeztetni a webkamerás felhasználókat, hogy több, mint 73 ezer szabad préda biztonsági kamera képét gyűjtötték csokorba a világ minden tájáról, ami ékes bizonyítéka annak, hogy mennyire hamis a "lustaság fél egészség" típusú hozzáállás.



Ébresztő, ideje lenne mindenkinek felébredni, mert ezeket a kamerákat az égvilágon nem hackelte meg senki sem. **Amiért ide mégis bekerültek, annak az az oka, hogy a tulajdonosa semennyire sem törődött a biztonsággal, és a dobozból kivéve semmilyen egyéni beállítást nem eszközöltek ezeken, így gyakran a szokásos admin-admin segítségével bárki hozzáférhet.**

Van kamera választás gyártónkénti, modellenkénti bontásban, de országok alapján történő szűrés is rendelkezésre áll, így a magyar felhozatal is nézegethető, ez a ma reggeli adatok alapján éppen 300 darab webkamerát jelent. Az egyes kamerák kiválasztása után még Google térképet is kapunk, amely megmutatja az eszköz hozzávetőleges földrajzi pozícióját.



A [Webkamerás kukkolók sorozatban](#) már párszor körbejártuk ezt a témát, és igyekeztük praktikus tanácsokkal is szolgálni. Például [csak a letakart webkamera a jó webkamera](#), de persze idetartozik a mai téma is, amely az alapértelmezett, vagyis a gyári kicsomagolás után minden fajta setup beállítás változtatás nélküli használatának veszélyeit ismerteti.

Mindenestre erős "falra hányt borsó" feelingje van a dolognak, és ami még aggasztóbb lehet, hogy sok eszköz emiatt illetéktelenek számára nem csak nézegethető, de akár vezérelhető is.



Minden egyes hálózatképes eszköznél - legyen az router, webkamera, okostv, bármi - érdemes a setup beállításokat használatbavételkor azonnal megváltoztatni. Természetesen wifi használat esetén magának a vezeték nélküli hozzáférésnek is ajánlatos az erős jelszó és a WPA2 protokoll alkalmazása.

A CNET észrevétele szerint a listán szereplő kamerák közül több, mint 11 ezer található az USA-ban, míg az Egyesült Királyság is kiveszi belőle a részét a maga 2500 védetlen eszközével, de **igazából szinte kivétel nélkül minden egyes régióból lehet találni itt ilyeneket.**



Rendszeresen ostromozzák a felhasználói fantáziátlanságot azzal, hogy [minden esztendőben megjelentetik a Worst Password típusú összefoglalókat](#), ahol elképedhetünk az ottani rangsorban olvasható harmatgyenge jelszavaktól.

Ám legalább ugyanekkora bakinak, felelőtlenségnek számít az is, ha valaki semmit nem változtat a gyári beállításokon. **Érdemes lenne tehát erre jobban odafigyelni, hiszen a megoldás is pofonegyszerű lenne: új erős egyedi jelszó beállítása.**

Tetszik 4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Webkamerás kukkolók](#)
[Webkamerás kukkolók IV. - 100 férfi ér egy nőt](#)
[Webkamerás kukkolók III.](#)
[Napi 160 ezer Facebook account esik el](#)
[Kormányzati e-mailek kontra biztonság](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6890477>

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 HTML trójaiak riogattak minket októberben

2014.11.14. 12:00 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

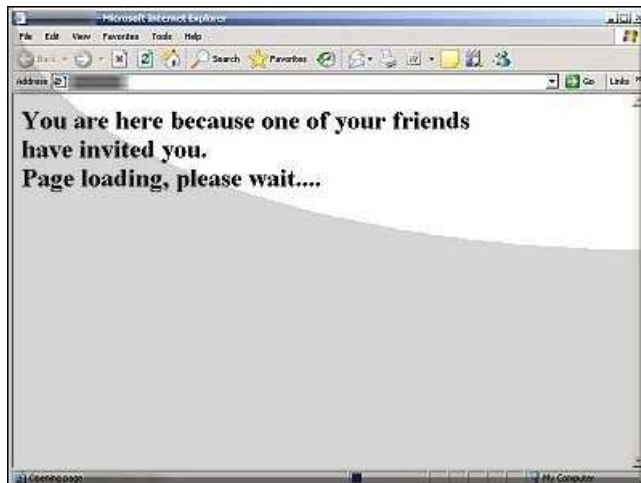
Címkék: [statisztika](#) [radar](#) [adatok](#) [nod32](#) [október](#) [havi](#) [report](#) [threat](#) [vírusstatisztika](#) [2014.](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. októberében a következő 10 károkozó terjedt a legnagyobb számban.



A múlt hónapban megjelent, és azonnal a lista élén felbukkanó **HTML/Refresh** maradt októberben is az **első helyen**. Ez egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.

Hatodik helyre költözött vissza a sokáig kiszorult **HTML/ScrInject** trójai. A visszatérő szereplőként üdvözölt trójai program egy olyan 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.



Eggyel előkelőbb pozícióba lépett viszont a Win32/RiskWare.NetFilter, az előző havi ötödik helyezést cserélte fel immár a negyedikre. A **Win32/RiskWare.NetFilter** egy olyan alkalmazás, amely magában hordoz olyan rosszindulatú kódokat, amelyek segítségével megfertőzhetik a számítógépünket, illetve a kompromittált rendszert később távolról is irányíthatóvá teszik. A távoli támadás során tipikusan adatokat lopnak el így a megfertőzött gépről, illetve távoli utasítások segítségével további kártékony kódokat telepítenek fel rá.

Az ESET Radar Report e havi kiadásában ezúttal az adó-visszatérítésekkel kapcsolatos csalásokról, adathalász támadásokról esik szó. A beszámoló szerint Írországból az ilyen típusú átverések száma minden korábbi mértéket meghaladóan növekszik. A csalási módszer arra alapoz, hogy egyrészt rengetegen utálnak beadványokat körmölni, hivatalos ügyeket intézni, másrészt ha valaki kap egy olyan felajánlást - ráadásul az adóhatóság nevében -, hogy hamar, **2-5 napon belül megkapja a visszatérített összeget, akkor annak sokan nem tudnak ellenállni.**

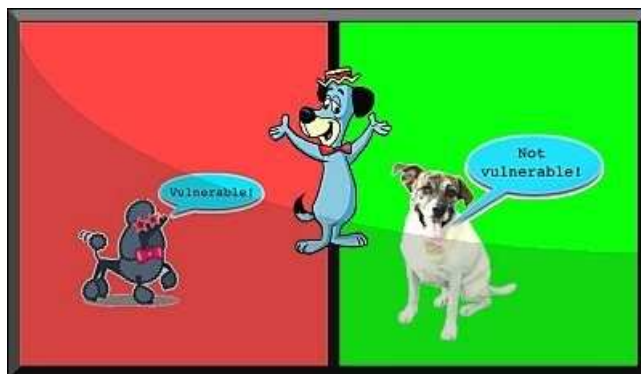
A támadók olyan űrlapok kitöltésére igyekeznek rávenni az áldozatokat, ahol **nem csak az összes személyes adatukat kell kitölteni, hanem emellett a bankkártyájuk számát is, sőt a hozzátartozó CVV kódot is bekérlik.** Mindenkinek fontos lenne józanul gondolkodni ilyenkor, és gyanakodni, ha valamilyen furcsa adatbekéréssel találkozik. Nem lehet elégszer figyelmeztetni, hogy bankok, hatóságok és hivatalok sosem kérnek be bizalmas személyes adatokat kérésre e-mail üzenetben vagy pop-up ablakban.



Októberi fontosabb blogposztjaink között beszámoltunk arról, hogy a 24. Virus Bulletin Nemzetközi Konferencián (Seattle, USA) **első ízben adták át a Szőr Péterről elnevezett díjat (Péter Szőr Award), amelyet idén az ESET kanadai kutatócsoportja vehetett át az Operation Windigo elnevezésű világméretű támadássorozatról írt részletes elemzésükért.**



Szóba került egy olyan markáns trend is, amely azt mutatja, **a klasszikus hitelkártya-adatok mellett/helyett a bűnözők egyre inkább célba veszik az értékes egészségügyi információkat.** Ehhez sajnos az is hozzájárul, hogy sok esetben elavult (frissítetlen XP) és gyengén védett számítógépes rendszerekről van szó, ahol ráadásul az adatok való hozzáférés is könnyebben elvégezhető, sok helyen például nem is titkosítják azokat.



Írtunk **a nem régen felfedezett SSL 3.0 böngésző sebezhetőség kapcsán egy olyan teszt weboldalról,** amelyre belépve **[ha egy pudlit látunk, akkor sebezhető a böngészőnk, míg ha terriert, akkor biztonságban vagyunk.](#)** Emellett áttekintettük, milyen tesztoldalas kampányok segítettek már korábban is a vírusvédelmi megelőzésben.



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



02. Win32/Bundpil féreg

Elterjedtsége az októberi fertőzések között: 2.24%

Működés: A Win32/Bundpil 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.



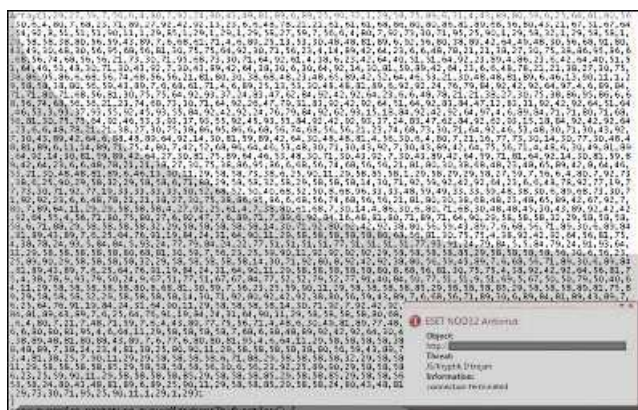
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



03. JS/Kryptik trójai

Elterjedtsége az októberi fertőzések között: 2.17%

Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlanul összezeavart JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját.



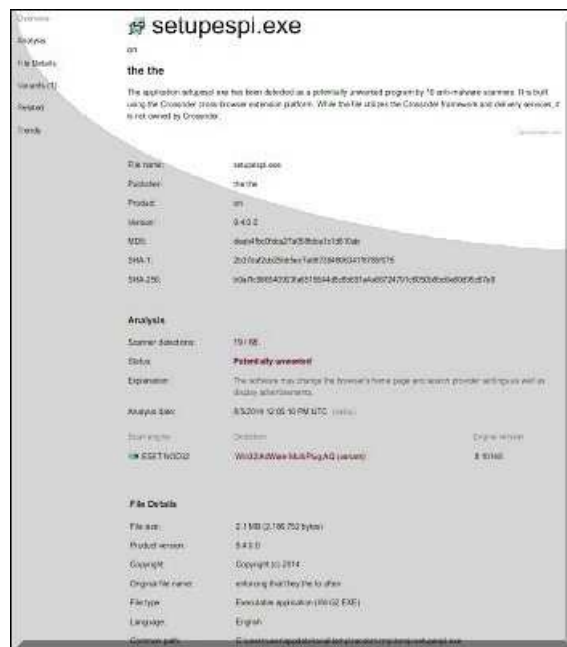
Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail



04. Win32/RiskWare.NetFilter riskware

Elterjedtsége az októberi fertőzések között: 1.49%

Működés: A Win32/RiskWare.NetFilter egy olyan alkalmazás, hordoz olyan rosszindulatú kódokat, amelyek segítségével megfertőzhetik a számítógépünket, illetve a kompromittált rendszert később távolról is irányíthatóvá teszik. A távoli támadás során tipikusan adatokat lopnak el így a megfertőzött gépről, illetve távoli utasítások segítségével további kártékony kódokat telepítenek fel rá.



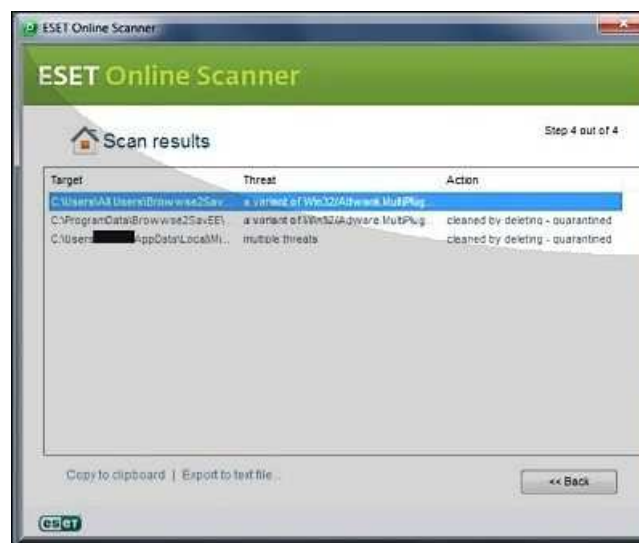
Bővebb információ: http://www.virusradar.com/en/Win32_RiskWare.NetFilter.A/description



05. Win32/Adware.MultiPlug adware

Elterjedtsége az októberi fertőzések között: 1.47%

Működés: A Win32/Adware.MultiPlug egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kényszerű reklámokat jelenít meg az internetes böngészés közben.



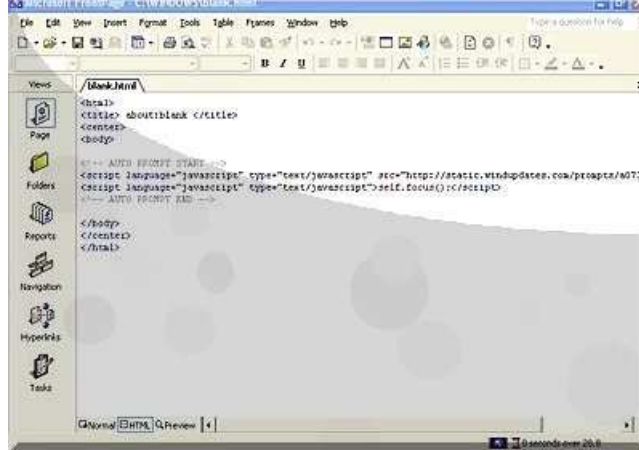
Bővebb információ: http://www.virusradar.com/en/Win32_Adware.MultiPlug.H/description



06. HTML/ScrInject trójai

Elterjedtsége az októberi fertőzések között: 1.45%

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.



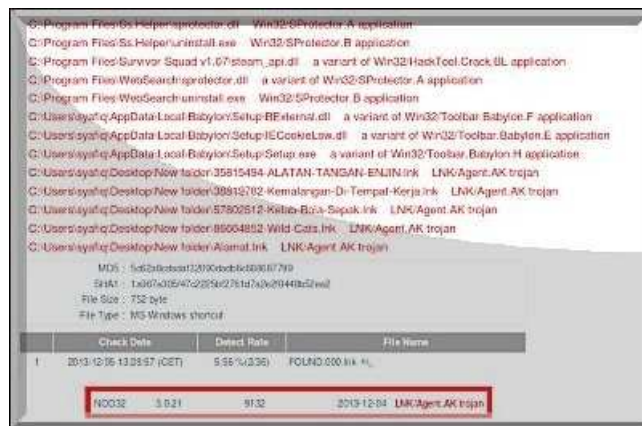
Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/scriinject-b-gen>



07. LNK/Agent trójai

Elterjedtsége az októberi fertőzések között: 1.40%

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. Vírusselemezők 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



08. Win32/Sality vírus

Elterjedtsége az októberi fertőzések között: 1.34%

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



09. HTML/IFrame vírus

Elterjedtsége az októberi fertőzések között: 1.24%

Működés: A HTML/IFrame egy gyűjtőneve az olyan vírusoknak, amelyek HTML weboldalak IFrame tagjeibe ágyazódva egy megadott kártékony URL helvre irányítják a böngészőt a felhasználó tudta és engedélve nélkül. Fertőzött weboldalakon keresztül terjed.



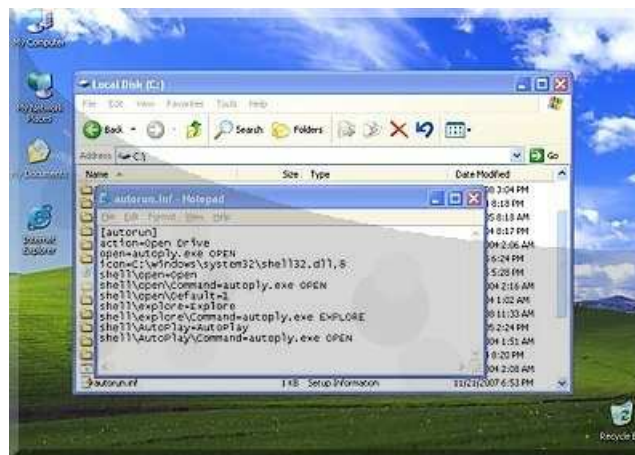
Bővebb információ: http://www.virusradar.com/HTML_Iframe.B.Gen/description



10. INF/Autorun vírus

Elterjedtsége az októberi fertőzések között: 1.22%

Működés: Az INF/Autorun gyűjtőneve az autorun.inf automatikus programfuttató fájlt használó károkozónak. 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>

Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[Végre kiesett a Conficker féreg](#)

[Vírstoplista 2014. augusztus hónap](#)

[Júliusi vírustoplista](#)

[Júliusi vírustoplista](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6895673>

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.

Célzott támadás a G20 csúcstalálkozó nevében

2014.11.17. 14:04 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

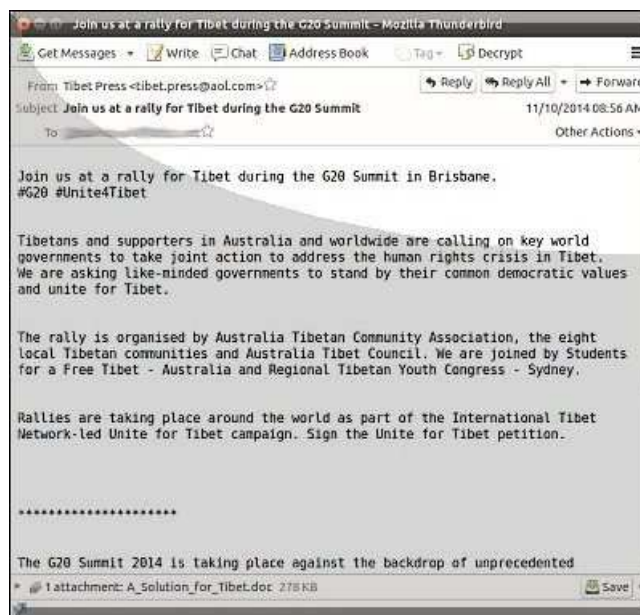
Címkék: [remote tibet tool access csúcstalálkozó rat g20 welivesecurity.com](#)

Az sajnos már régen nem újdonság, ha politikai szervezetek, vagy csoportok ellen APT támadásokat hajtanak végre. Időnként [megtörténik ez a New York Times szerkesztőségével](#) éppúgy, mint a különféle [tibeti ellenzéki csoport tagjaival](#), sőt az utóbbiak szemléletmást "kiemelt figyelmet élveznek" e tekintetben.



A hétvégén Ausztráliában tartott G20 értekezlet nevével visszaélő próbálkozást azonosítottak a minap biztonsági kutatók. A támadáshoz olyan célzott e-mail üzeneteket használtak fel, illetve küldtek szét, amelyek látszólag a Tibet Press nevében érkeztek (Tibet Press <tibet.press@aol.com>).

Ez a tibeti emberi jogokkal kapcsolatos küzdelem aktuális helyzetéről tájékoztató levél ["természetesen" tartalmazott egy "A_Solution_for_Tibet.doc" nevezetű fájl mellékletet is.](#)



A mellékelt dokumentum ezúttal egy viszonylag régebbi, [CVE-2012-0158 biztonsági rés kihasználására alkalmas kódot tartalmaz](#), amely a Gh0st Rat távoli elérést biztosító programot telepíti fel az áldozatok gépére. A Remote Access Tool futása során indiai és Kókusz szigetekre doménekhez (mailindia.imbss.in, godson355.vicp.cc) próbál meg csatlakozni.

A támadók kilétéről általában ritkán lehet biztos információkat megtudni, sejtteni azonban rendre Kínát szokták az ilyen jellegű akciók hátterében.



Itt azt lehet érdemes kihangsúlyozni, hogy az ismeretlen feladóktól kéretlenül érkező üzenetekben szereplő mellékletek vagy linkek jelentik manapság a legnagyobb, és egyúttal a leggyakoribb APT kockázatot, fertőzési veszélyforrást.

Ez természetesen mindenkire ugyanúgy egyformán vonatkozik, vagyis vigyázni mindenkinek kellene, de persze az sem lehet meglepetés, hogy a politikai, közéleti szereplőknek, illetve különféle kiemelt cégeknek, civil szervezeteknek mindez kiemelten is fontos.

[Tetszik](#) Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Ez itt a Microsoft távoli hozzáférés, vagy mégsem?](#)

[Napi 160 ezer Facebook account esik el](#)

[Kormányzati e-mailek kontra biztonság](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6909843>

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](#).

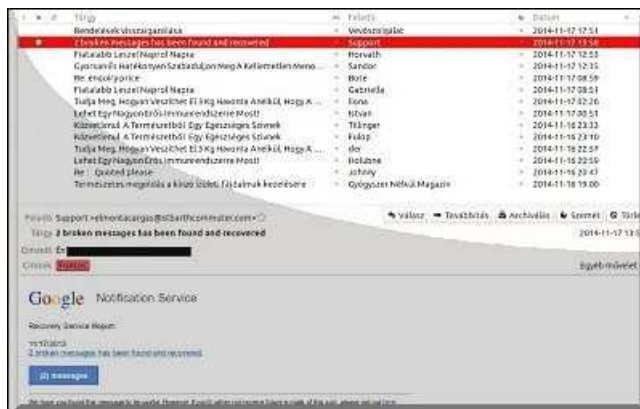
Nincsenek hozzászólások.

Átverés a Google spam

2014.11.19. 09:51 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [google spam](#) [kanadai átverés](#) [hamis gyógyszerész](#)

"Önnek két sérült üzenete volt, amiket észleltünk és sikeresen visszaállítottunk" - ezzel a tárgysorral érkezik a **legújabb spam látszólag a Gmail-t üzemeltető Google nevében**. A próbálkozás viszont a szép színes Google logó ellenére több szempontból is elég halványra sikeredett, remélhetőleg ezúttal valóban a nullához konvergál azoknak a száma, akik mégis rákattintottak.



Sokszor és [sokat foglalkoztunk már a kéretlen levelek témakörével](#), amit úgy kell elképzelni, mint egy [hatalmas neverending story-t](#), ami [mindig volt, van és lesz is](#). Emellett pedig szintén számtalanszor felsoroltuk azokat a fogódzókat, amikkel az esetek döntő többségében egyszerűen felismerhetőek az ilyen primitív próbálkozások.



Esetünkben rögtön két hatalmas lóláb is kilóg, **az egyik mindjárt a feladó személye**. Ugye azt senki nem gondolja komolyan, hogy egy hivatalosnak feltüntetett üzenet feladója a Google helyett "Support <elmontacargas@stbarthcommuter.com>" cím lenne? Többeknél itt már meg is bukott a dolog remélhetőleg, bár sokan sajnos nem is nézik meg a feladót.



A másik javasolt trükk a mouseover, vagyis **vigyük az egérkurzort az ajánlott, javasolt link fölé kattintás nélkül, és akkor előtűnik, mire is akarnak bepalizni bennünket**. Önmagában már az is mókás, hogy az úgynevezett "Leiratkozás" is ugyanarra a kamu weboldalra mutat.

Ez most "http://weightlossarchive.com/helene.php" linket jelenti, amely fájl egy kis JavaScript kód segítségével megkeveri még egy kicsit a weblapátírányítást, és egészen máshova továbbítja a gyanútlan látogatót.



A végállomás helyszíne [ezúttal is egy "kanadai gyógyszerész"](#) weboldal, a [Hongkongban hosztolt](#) angol nyelvű [firstmedicaremarket.ru](#). Van itt persze mindenféle pirula dögivel, "kitűnő" minőség, és olcsó az ára.



Az akció kétségkívül legviccesebb eleme a gyógyszerész webáruház "Contact Us", azaz kapcsolat menüben található "Report spam: Click here." opció, amely egy ilyen kéretlen levél után legalább őszinte mosolyt fakaszt bennünk, "made my day".

[Tetszik](#) Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

[Megosztom](#) [tumblr.](#) [Tweet](#) [Pin it](#) [g+](#)

Ajánlott bejegyzések:

[A Facebook nevében](#)

[A LinkedIn support üzent nekünk. Vagy mégsem?](#)

[Közelgő Karácsony, szaporodó adathalászat](#)

[Instagram üzenet. Vagy mégsem?](#)

[Új Picasa képek az albumunkban. Vagy mégsem?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6914447>

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 brit cégek fele alkalmazna korábbi hackereket

2014.11.21. 15:54 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [it brit felmérés cég hacker védelem vállalat welivesecurity.com tudásanyag](#)

Egy friss, 2014 októberi kutatásban arra keresték a választ, vajon a vállalatok, nagyvállalkozások IT részlegein mennyire van meg a megfelelő naprakész szakértelem ahhoz, hogy hatékonyan felvehessék a küzdelmet a számítógépes bűnözőkkel.



A svájci KPMG International felmérésében **háromszáz** olyan IT és HR vezetőt kérdeztek meg, akik **500 és 10,000 főt alkalmazó nagyvállalatoknál dolgoznak**. Az eredmények között számos meglepő és kevésbé meglepő adat kerül a felszínre.

Először is **a többség őszintén elismerte, nem rendelkeznek elegendő készséggel** ahhoz, hogy hatékony megvédjék az IT infrastruktúrájukat, **a válaszadók 60% szerint nincs elegendő felkészült szakemberük ehhez a feladathoz**.



57%-a a megkérdezetteknek úgy vélekedett, hogy [az utóbbi két esztendőben ez a speciális feladat kétségtelenül minden eddigénél nehezebb feladatot ró a szakemberekre](#), míg **52% látja úgy, hogy ezen a területen agresszív fejedárással hapolják el a cégek egymástól az ütőképes specialistákat**.



Abban szinte egységes az álláspont - **74%** - hogy vállalati környezetben vadonat új ismeretek, skillsek szükségesek az újonnan megjelenő támadási formák elleni hatékony fellépéshez.

A felmérésben szereplő vállalatok 70%-a azonban jelenleg nem rendelkezett megfelelő színvonalú adatvédelmi stratégiával és a privát szférát hatékonyan védelmező megoldásokkal.



Érdekes, hogy **a megkérdezett brit cégek több, mint fele nyilatkozott úgy, hogy emiatt erősen fontolgatja korábbi hackerek alkalmazását, sőt ezt akár annak ellenére is fontolóra vennék, ha az illető korábban már volt büntetve.**

Az mindenesetre a felmérés kapcsán elmondható, hogy **a szakmai tudásanyag elavulása soha nem látott mértékben felgyorsult**, és a IT biztonsági szakembereknek folyamatosan kell képezniük magukat, hiszen szinte naponta egészül ki ez a terület új ismeretekkel.

 **Tetszik** Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A brit felnőttek hatoda volt már kiberáldozat](#)
[Lebecsüljük a BYOD kockázatokat](#)
[Amikor a suszter cipője lyukas](#)
[Ki miben bízik?](#)
[Mennyi? 420 ezer. Mi 420 ezer? Miért mi mennyi?](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6921571>

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.

Megfertőzheti-e számítógépünket az e-cigaretta?

2014.11.24. 11:01 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [usb töltő](#) [malware fertőzés](#) [kártevő backdoor](#) [hátsóajtó e-cigaretta](#) [welivesecurity.com](#)

Nem csak a tüdőre lehet káros az e-cigaretta, derült ki a **Guardian** egyik cikkéből. Azt még az Autorun vírus hosszú pályafutása idején megtanulhattuk, ha valami külső adathordozókon terjed, az lehetővé teszi, hogy a legváratlanabb helyeken bukkanjon fel. Így nem csak a klasszikus USB kulcs, memóriakártya, vagy külső merevlemez játszik ilyenkor, hanem például fényképezőgép, MP3 lejátszó, okosóra, [digitális képerlet](#) vagy éppen nyilvános fotófeldolgozó automata is könnyen jöhet szóba, mint potenciális kártevő hordozó. **Ebbe az egyébként is széles malware forrás táborba most az e-cigaretta is bejelentkezett.**



Számos e-cigaretta készülék tölthető USB porton keresztül is, amit természetesen a szokásos konnektorba dugható töltő egységen kívül a PC számítógépre is lehet csatlakoztatni, így [előfordulhat, hogy az ártalmatlannak gondolt e-cigi is lehet a vírusfertőzések forrása](#), és különösen érdekes lehet mindez az adatbiztonság szempontjából egy vállalati környezetben.

A Redditen olvasható történet szerint az derült ki ugyanis egy [Kínában gyártott e-cigaretta egységről, hogy az abban szereplő kártékony kód "hazatelefonált"](#), azaz ha rá volt dugva a számítógép USB portjára, akkor kapcsolatba lépett egy távoli szerverrel és megfertőzte a rendszert.

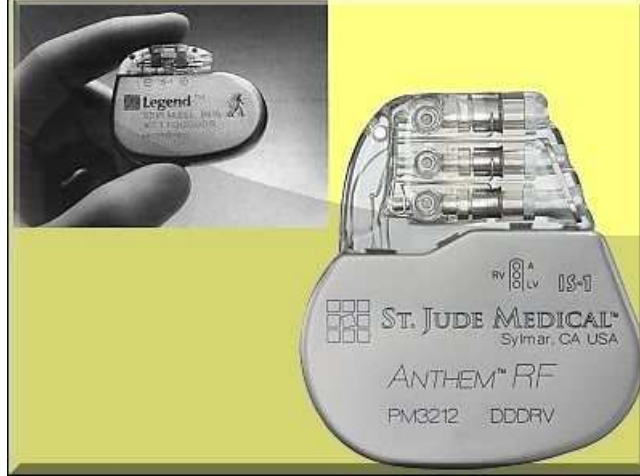


A fenti incidenssel kapcsolatban **Rik Ferguson**, a Trend Micro biztonsági tanácsadója úgy nyilatkozott, hogy a történet teljesen **hihető**. Ehhez lehet jó adalék Kovács Zsombor Hactivitys előadás, melyben egy **Kínában gyártott Androidos telefonon elemezte az arra előtelepített alkalmazásokat, és például a gyárilag installált és módosított Opera böngésző tartalmazott egy olyan hátsó ajtót**, melynek révén vígan hozzáférhetett például az SMS és egyéb telefonfunkciókhoz.

A töltésekkel egyébként sem árt vigyázni, ehhez két korábbi példát is érdemes megemlíteni. Az egyik eset az volt, amikor az **Energizer Duo akkutöltő szoftverében trójai programot találtak, amely az elemek állapotának ellenőrzése helyett (vagy mellett) hátsó ajtót nyitott**, azaz távoli hozzáférést biztosított az így kompromittált számítógéphez.



A másik érdekesség a tavalyi BlackHat egyik előadásában szerepelt, ahol **egy módosított preparált töltő segítségével lehetett olyan kártékony alkalmazásokat telepíteni a gyanútlan áldozat iOS eszközére**, mely appok az AppStore-ba soha nem kerülhettek volna be, és mindezt módosítás, azaz jailbreak mentes készülékeknél.



A dolgok internete és a BYOD káosz miatt a korábban sem egyszerűen menedzselhető biztonság **amúgy is egyre összetettebb probléma, hiszen naponta dob a felszínre új, addig sosem látott kockázatokat.** Van ezek közt olyan, amire sokan számítanak - gondoljunk csak [David Jacoby Hacktivitys előadására az okos otthonok](#) kapcsán.

De akad köztük váratlan és meglepő dolog is, például amikor tavaly októberében a korábbi amerikai alelnök, [Dick Cheney pacemakerében az orvosok amiatt tiltották le a vezetékek nélküli képességeket](#), hogy ezzel **kiküszöböljék egy esetleges gyilkossági kísérlet veszélyét.**

 **Tetszik** 16 személy kedveli ezt [Regisztrájl](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Hátsóajtó az Energizer elemtöltő szoftverében](#)
[Amikor a botnet vízumot igényel](#)
[Célzott támadás Ukrajnában és Lengyelországban](#)
[A váltásdíjas titkosító kártevő visszatér](#)
[Nincs nyoma backdoornak a TrueCryptben](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6928237>

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 brit felnőttek hatoda volt már kiberáldozat

2014.11.26. 19:31 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [brit](#) [felmérés](#) [adathalászat](#) [kibertámadás](#) [welivesecurity.com](#)

Egy friss felmérés eredménye szerint a briteknél a felnőtt lakosságból **minden hatodik felhasználó szenvedett már el valamilyen kibertámadást.** Az incidensek közül az adathalászat, a személyes adatok eltulajdonítása illetve banki adatok kifürkészése, manipulálása a leggyakoribb.



Az ITV beszámolójából többek közt az is kiderül, hogy bár valóban **16% az áldozatok aránya, mégis sok esetben egyáltalán nem is védik az eszközeiket biztonsági alkalmazásokkal.** Jellemzően az iPad és az okostelefon az, [amire sokan úgy gondolják, nem szükséges védelmi eszközt telepíteniük rá.](#)

A megkérdezettek 60%-a nyilatkozott úgy, hogy okostelefonján semmilyen védelem nem fut, és az iPad tulajdonosok 48%-a is hasonlóképpen válaszolt erre a kérdésre.



Ezzel együtt azonban a felhasználók majdnem fele bankol hordozható okoseszközéről, egy harmaduk pedig rendszeren elektronikusan vásárol is a segítségével, pedig a mobiltelefonos adathalászat mértéke 80 százalékkal emelkedett az előző évekhez képest.

Összességében 83%-ukat csapták már be valamilyen módon asztali PC vagy laptop használat közben, [egy ötödük \(21%\) szenvedett el valamilyen támadást az okostelefonján,](#) míg 17 százalék volt azoknak az aránya, akik a tablethasználat közben futottak bele ilyenbe.

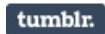


A tudatlanság talán az egyik legnagyobb probléma, amire a felmérés is rámutat, hiszen a felhasználók 59%-a tévesen úgy vélekedik, hogy szemben a klasszikus számítógéppel okostelefonon vagy tableten semmilyen vírus vagy biztonsági fenyegetés nem érheti.

Ha viszont ezzel szembe állítjuk a korábban emlegetett 80%-os emelkedést a mobileszközös adathalászatban, akkor jól látható, hogy tények

egyáltalán nem támasztják alá az átlag vélekedést, amit az internetes bűnözők igencsak alaposan ki is használnak.

 Tetszik Regisztrálg, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A brit cégek fele alkalmazna korábbi hackereket](#)

[Így költjük a pénzt az online vásárlásoknál](#)

[Lebecsüljük a BYOD kockázatokat](#)

[Phishing - így halásztak ők 2013 első félévében](#)

[Majdnem mindenki átverhető adathalászattal](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6935663>

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.

Kell-e aggódjunk a Regin kémprogram miatt?

2014.12.01. 10:51 | [Csizmazia Darab István \[Rambo\]](#) | [3 komment](#)

Címkék: [biztonság](#) [tippek](#) [állami kémprogram](#) [védekezés](#) [regin](#)

Egy a napokban megjelent cikk szerint [Edward Snowden a legjobb IT biztonsági pedagógus](#), ténykedése és kiszivároztatásai nagyobb hatást értek el a biztonságtudatossági iparban, mint korábban bármilyen szlogen vagy kampány. Természetesen nem tőle hallottunk először állami kémprogramokról - volt már sokkal korábban Magic Lantern, Echelon és társai - ám az újonnan felfedezett Regin kártevő kapcsán ismét felmerülhet a kérdés, kell-e félni a hétköznapi átlagfelhasználóknak?



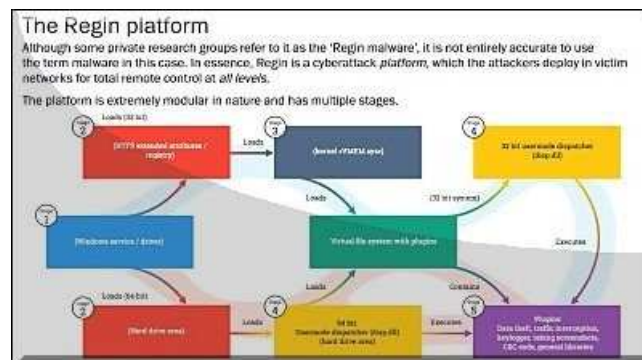
Aki követte az eseményeket állami kémprogram fronton, emlékezhet, hogy 2010. júniusában a Stuxnet [célzottan az iráni Busehri atomerőmű uránium dúsító berendezéseinek sabotálására](#) lett kifejlesztve és el is érte célját, hiszen 2010. novemberében Irán kénytelen volt leállítani az urándúsítóit, mert a centrifugák 20%-a megsemmisült.

A kártevőt az USA és Izrael közösen fejleszthették ki. [Érdekes mellék és utóhatások kísérték a Stuxnet útját](#), ugyanis [röviddel az események után a SkyNews egy riportban számolt be arról, hogy máris árulják a bűnözők az interneten a Stuxnet kártevő kódját](#).



Sajnos hiába figyelmeztetnek évek óta többen is - köztük Mikko Hypponen - hogy [az állami kártevők \(Stuxnet, Flame, Duqu, Gauss, Careto, stb.\) veszélyes útra visznek](#), sajnos azóta is többet azonosítottak ilyenből. Mivel minden kártékony kód előbb-utóbb nyilvánosságra kerül, módosítják, másolják, ingyenesen terjesztik, vagy éppen eladják, nem tartható kordában.

Erre remek példa, amikor 2012-ben az egyik legnagyobb amerikai olajcég, [a Chevron beismerte, hogy a hírhedt Stuxnet vírus bejutott a hálózatukba](#).



Most mindenestre újabb egyed került elő ezekből, [a Regin a szakemberek szerint az eddigi legprofesszionálisabb kémeszköz](#), mellyel valaha találkoztak.

Segítségével [évek óta széleskörű kémtevékenységet folytattak egy sor országban](#), többek között Algériában, Afganisztánban, Belgiumban, Brazíliában, a Fidzsi-szigeteken, Németországban, Iránban, Indiában, Malajziában, Szíriában, Pakisztánban, Oroszországban, illetve Szaúd-Arábiában is jelentős aktivitást mutattak ki.



Ezek után lássuk, mit tehet egy átlag felhasználó egy olyan világban, ahol az ilyen állami csúnyaságok mellett még 200 ezer új kártevőminta is keletkezik NAPONTA. Nyilván minden ellen nincs orvosság, és ugye 100%-os védelem sem létezik, de a tőlünk telhető legnagyobb gondossággal azért igyekezhetünk magunkat megóvni.

- **rendszeres és azonnali biztonsági frissítés**, és nem csak az operációs rendszer, hanem azon felül minden felhasználói szoftvernél is (Java, Adobe, böngészőklens, stb.)

- **mentések és backup, legyen több különböző állapotról is** mentésünk, egy olyan külső adathordozón, amely nincs állandóan csatlakoztatva a géphez, a mentés legyen ellenőrzött (baj esetén legyen garantáltan visszaolvasható és kicsomagolható), emellett pedig az a legjobb, ha mindezt titkosított mentéssel végezzük

- **legyen többretegű védelmünk, a szimpla antivírusnál ugyanis sokkal hatékonyabb** egy komplex internet security csomag, amelyben tűzfal, sebezhetőség elleni védelem, exploit blokkoló, botnet és adathalászat elleni védelem, sőt egyes termékek akár a közösségi oldalak hatékony védelmét is elvégezhetik

- **egészséges gyanakvás, biztonságtudatosság - szükséges és bölcs dolog**, hogy némi egészséges paranoia lakozzon mindenkiben. A számítógépes bűnözők gyakran vonzó, vagy fenyegető dolgokkal igyekeznek rávenni bennünket a kattintásra, letöltésre, mindenesetre érdemes figyelni az intő jelekre, és ha valami látszólag szokatlan vagy gyanús, akkor érdemes azonnal megállni, gondolkodni, nem pedig reflexből kattintani.

- **kétfaktoros autentikáció használata, ahol csak lehet** - azon túlmenően persze, hogy legyen erős jelszavunk, amit rendszeresen cserélünk ha kell, ha nem; illetve mindenhol legyen ez egyedi, és ha már ennyi helyen ilyen gálánsan elkészítették nekünk a kétfaktoros azonosítást - Google, PayPal, Yahoo, Twitter, Facebook, stb. és persze az Apple ID is - akkor érdemes is igénybe venni mindenkinek.

 **Tetszik** 4 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[12 tipp a biztonságos karácsonyi vásárláshoz](#)
[Android kémprogram persze csak a mi érdekünkben](#)
["Szösölmédia" és nyaralás](#)
[Nyári tanácsok utazáshoz](#)
[A jó, a rossz és a kormányzati](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6947825>

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](#).

lőfüle elemér 2014.12.02. 07:06:48

Egyszerű újságírókám. A címben feltett kérdésre ismét nem válaszoltál. Érthető a hazug cím, hiszen kell a kattintás, de belegendolt már a kétfüles agyad abba, hogy ha folyamatosan hazug, félrevezető címekkel manipuláltok, akkor biza előbb-utóbb mindenki szarik az írásaitokra, és nem lesz olvasótok.

Válasz erre



Csizmazia Darab István [Rambo] • <http://antivirus.blog.hu>
2014.12.02. 07:32:24

"Ezek után lássuk, mit tehet egy átlag felhasználó egy olyan világban, ahol az ilyen állami csúnyaságok mellett még 200 ezer új kártevőminta is keletkezik _NAPONTA_. Nyilván minden ellen nincs orvosság, és ugye 100%-os védelem sem létezik, de a tőlünk telhető legnagyobb gondossággal azért igyekezzhetünk magunkat megóvni."

Válasz erre

[antyg 2014.12.02. 10:56:01](#)

[@lófüle elemér](#): Kedves értelmezni képtelen hozzászóló!

Mielőtt megszólalsz jó lenne, ha végig is olvasnád, és próbálnád értelmezni a szöveg teljes egészét!

Válasz erre

Közelgő Karácsony, szaporodó adathalászat

2014.12.03. 13:21 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

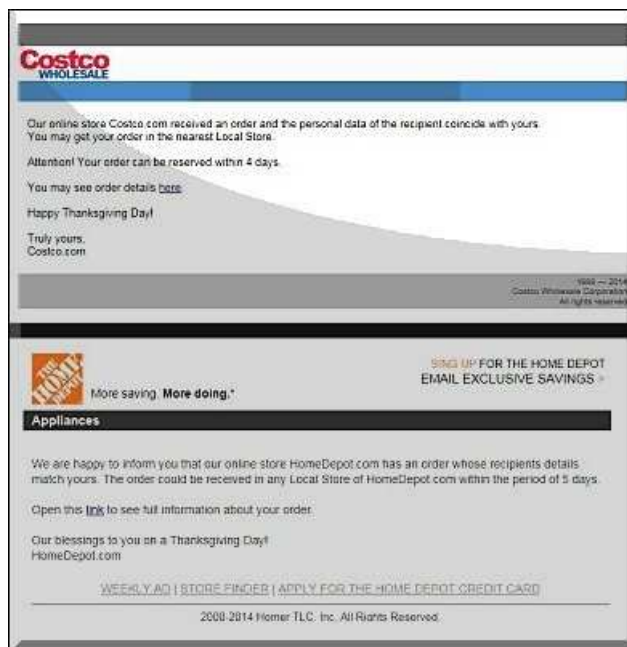
Címkék: [spam vásárlás online karácsony xmas átverés hamis welivesecurity.com](#)

Ahogy egyre közelednek a karácsonyi ünnepek, és az ehhez kapcsolódó felfokozott online bevásárlások időszaka, úgy szaporodik az adathalász kísérletek mennyisége is. **A jó hír viszont az, hogy ezek még mindig eléggé egy kaptafára készülnek**, ezért aztán ha valaki csak egy kicsit figyelmes, akkor biztosan nem sétál bele a csapdába.



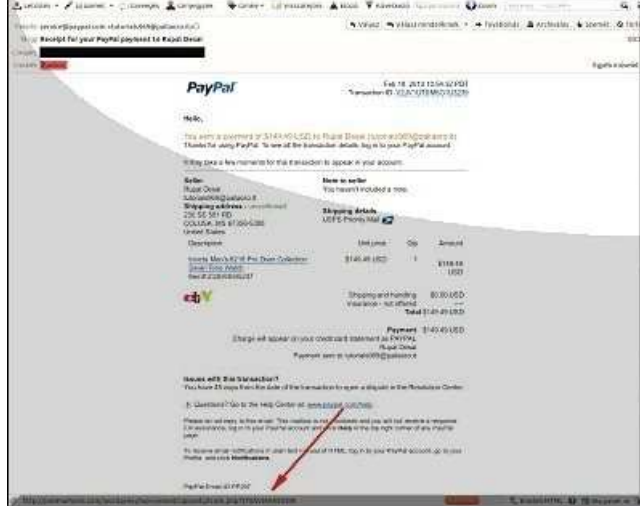
Volt már [több korábbi olyan számlának, illetve vásárlási visszaigazolásnak látszó spamről szó](#), ahol vagy célzottan vagy akár csak próbaszerencse alapon óriási mennyiségben kiszórva azt próbálják meg elhitetni az áldozatokkal, hogy a nevükben már elindult egy vásárlás. **Ha ettől megijednek, akkor a kéréstlen levélben mellékelt linke rákattinthatnak a visszavonás vagy a tétel ellenőrzése miatt.**

Természetesen nem csak az ilyen - webshopokból, fizetesközvetítőktől, bankoktól származó - üzenetek hamisak, hanem a mellékelt linkek is vagy kártevőt terjesztenek, vagy egyéb más burkolt trükkös tevékenységnél használják fel: űrlap kitöltögetés, reklám oldalakra való továbbítás fejpénzért, személyes adatok begyűjtése, stb.



A december elején tipikusnak mondható spamek arról tájékoztatnak, hogy köszönik szépen, megérkezett az állítólagos rendelésünk, ami napon belül ki is szállítanak majd az áruházba. **A rendeléssel kapcsolatos részletesen információ természetesen nem szerepel a levél testben, ahhoz kattintani "kell", hogy megláthassuk, mi is az valójában.** [Bár a bemutatott példákban a Home Depot és a Costco WholeSales szerepeltek](#), tulajdonképpen bármilyen céget, áruházat, bankot, iTunes és hasonló zene és app boltot, vagy fizetesközvetítőt a helyükbe lehet és kell is képzelni.

Azon túlmenően, hogy a link fölé vitt egér szépen megmutatja, hova is mutat igazából az adott URL hivatkozás azt is érdemes megjegyezni, hogy ha a levél szöveges részében a rendelésünkkel kapcsolatban semmilyen konkrét információ nem található, akkor ez számunkra gyanúra kell, hogy okot adjon.



Akik a karácsonyi online vásárlással kapcsolatos korábbi tanácsainkat szeretnék elolvasni, vagy az ezzel kapcsolatos biztonsági óvintézkedéseket felfrissíteni, azok [elolvashatják a biztonságos online vásárlással kapcsolatos legfontosabb tudnivalóinkat ezen a linken](#).

 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Így költjük a pénzt az online vásárlásoknál](#)
[Átverés a Google spam](#)
[Megtalálták az eltűnt maláj repülőt! Ismét :-\)](#)
[Itt a foci VB, jönnek az átverések is](#)
[12 tipp a biztonságos karácsonyi vásárláshoz](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6954275>

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](#).

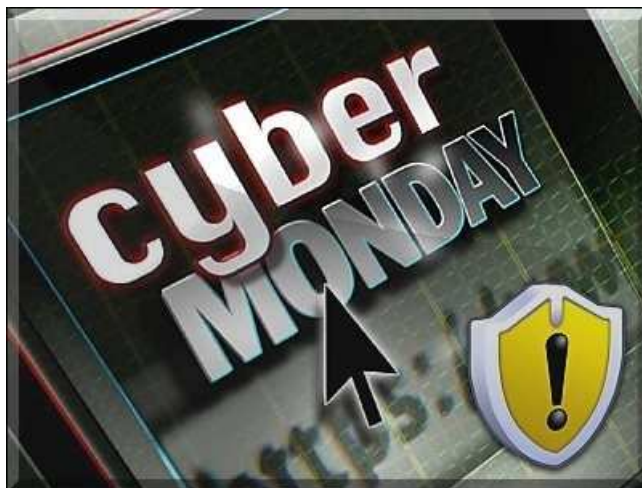
Nincsenek hozzászólások.

Így költjük a pénzt az online vásárlásoknál

2014.12.08. 17:24 | [Csizmazia Darab István \[Rambo\]](#) | [1 komment](#)

Címkék: [statisztika](#) [vásárlás](#) [biztonság](#) [online](#) [black](#) [cyber](#) [eset](#) [friday](#) [karácsonyi](#) [monday](#) [infografika](#) [welivesecurity.com](#) [goexplore.net](#)

Mostani infografikánk azt próbálja meg összefoglalni, milyen tendenciákat lehet megfigyelni az online vásárlásokkal kapcsolatosan. Az úgynevezett "Cyber Monday" esetében például - a hagyományos Black Friday-hoz hasonlóan - évről évre emelkedő tendencia figyelhető meg. A "kik vásárolnak leginkább online" kérdésre pedig elsősorban a magasabb keresetű, és egyetemi végzettséggel rendelkező középkorú nők vezetnek a statisztikát.



Idén december 1-ére esett [a 2005-ben kitalált "Cyber Monday"-nak nevezett akciós hétfő](#), amikor mélyen leszállított akciós árakkal várják az online áruházak a megrendelések áradatát. Aki megnézte a [Black Friday-ról szóló beszámolókat](#), annak valószínűleg kellően elmehetett a kedve a verekedésig fajúló árucikkekért folytatott fizikai közelharctól.

Ám lehet ezt kényelmesen fotelből otthonról is intézni, tumultuózus jelenetek mellőzésével. Nézzük először is néhány statisztikai adatot arról, hogy főleg kik azok, akik nem félnek online vásárolni.



Ahogy azt a bevezetőben is láthattuk, a dolog egyre népszerűbb, és nagyjából minden évben 10%-kal emelkedik az ilyenkor elköltött összeg. Elképesztő számok látnak napvilágot, például hogy a kiber hétfőn csak este 8 és 9 között 150 millió dollárt - hozzávetőlegesen 37 milliárd jó magyar forint - hagynak az online kasszában a vásárlók.

Ami még érdekes lehet, hogy [a tavalyi adatok szerint a beérkező rendelések nagyjából ötöde - 18 százaléka - mobil eszközökről származik](#).



Ugyancsak jól érzékelhető, hogy az online kereskedem legfőbb fogyasztói a magas iskolai végzettséggel rendelkezők, a nagyobb jövedelmet élvezők, illetve a nemek alapján a nők erre látszólag jobban rá vannak kattánva.

Nyilván valamennyire a fizetőképességgel is összefügg, hogy életkor szerint az Y (1980 és 1995 között születettek) és az X (1965-1979 születettek) generáció, valamint az Alfák (2005- utáni születésűek), illetve a középkorúak (1946-1964) vezetik az internetes online költségek statisztikáját.



Természetesen az infografikából nem hiányzik néhány alapvető biztonsági tanács sem, mikre érdemes vigyázni, hogy a vásárlás ne váljon rémálommá, vagy anyagi veszteséget is okozó bosszúsággá. Az ESET szakemberei öt pontban sorolják fel a legfontosabb tippeket, így ezek között megemlítve a biztonsági frissítések kiemelt fontosságát, a megbízható saját könyvjelző linkek használatát, az adathalász oldalak veszélyeit, és az otthoni wifi sokkal nagyobb megbízhatóságát az utcai publikus kapcsolódásokkal szemben.

Illetve emellett a bankkártyák esetében egyes országokban az is fontos különbség lehet, hogy a hitelkártyáknál - ahol nem a saját, hanem a bank pénzét költjük - sokszor zökkenőmentesebb az incidensek kivizsgálása, és az esetleges csalások miatti pénzvisszaszerzési procedura. Akik ebben a témában további biztonsági tippeket is szívesen olvasnának, [azok figyelmébe ajánljuk korábbi 12 pontos részletes összefoglalónkat](#).

 Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Közelgő Karácsony, szaporodó adathalászat](#)
[Életünk része lett az állandó támadás](#)
[12 tipp a biztonságos karácsonyi vásárláshoz](#)
[Napi 160 ezer Facebook account esik el](#)
[Kormányzati e-mailek kontra biztonság](#)

A bejegyzés **trackback** címe:

<http://antivirus.blog.hu/api/trackback/id/6967711>

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](#).



saját macskám 2014.12.08. 22:12:24

bödönbe

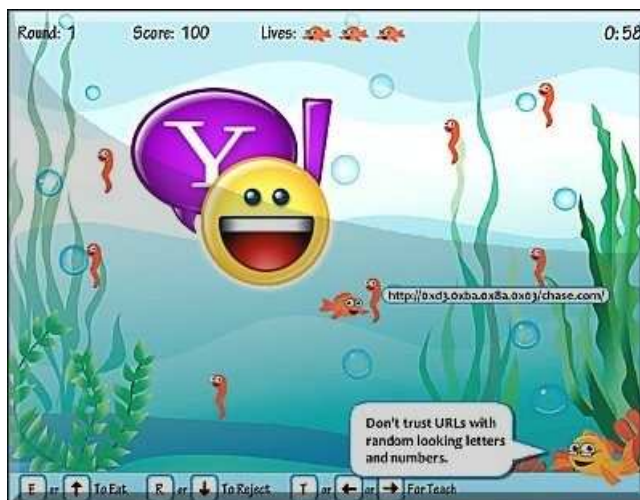
Válasz erre

Újabb adathalász kísérlet a Yahoo! ellen

2014.12.10. 15:32 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [yahoo!](#) [social átverés](#) [phishing](#) [adathalászat](#) [engineering](#)

Megszokhattuk már, hogy ezek a trükkök sosem szűnnek meg, hanem **rendre kisebb-nagyobb változtatásokkal, újabb social engineering trükkökkel felturbózza próbálkoznak** a gyanútlan felhasználóknál. Most ismét a Yahoo! felhasználóknál kopogtattak.



A legfrissebb esetben egy olyan kéretlen levelet kapott az áldozat, melyben a Yahoo! nevében arról tájékoztatták, miszerint a legutóbb küldött üzenetét nem sikerült elküldeni, mert állítólag túllépte a levelezési tárhely fizikai méretét. A sikeres elküldés feltétele a figyelmeztetés szerint az lenne, hogy kattintsunk (na persze ;-)) a mellékelt linkre, ahol az állítólagos tárhely kvóta bővítés ingyenesen elvégezhető.

Valószínűleg mindenki kitalálta már, hogy a link nem bővít semmit, hanem [egyenesen egy adathalász linkre vezet](#). Egy EMC jelentés szerint a 2013-a esztendő rekord évet mutatott a phishing támadások tekintetében, a **becsült veszteség 5.9 milliárd USD volt**. A legnépszerűbb adathalász célpontok a PayPal, eBay, a Yahoo, a Facebook és a LinkedIn mellett általában a különböző bankok szoktak lenni.



Persze **nem csak adathalász oldalon lehet a levelezéssel elvégezni, elég ehhez a gyenge jelszó emlékeztető kérdés is**. Emlékeztetes lehet például az a 2008-as eset, amelynél Sarah Palin szenátor Yahoo! alatti levelezését tudta megszerezni egy támadó.

[A módszer nem feltörés, nem jelszó találgatás volt, hanem egyszerűen új jelszó igénylése](#). A születési hely és idő megszerzése nem okoz neki semmilyen gondot, a titkos ellenőrző kérdés pedig az volt, hol ismerkedtek meg annak idején a férjével. Vicces módon ez is [Googlizható volt](#), mert Palin erről is beszélt már a nyilvánosság előtt.



Aki esetleg begépelte már a jelszavát valamilyen gyaníthatóan adathalász oldalon, vagy csak túl régóta nem változtatott már

jelszót, annak itt a remek alkalom, hogy most azonnal másik erős és egyedi jelszót válasszon. Ha a szolgáltatás támogatja, akkor érdemes bekapcsolni a fokozott biztonságot nyújtó kétfaktoros azonosítást is.

A korábbi incidensek tanulsága gyakorta úgy hangzik, hogy a túlzott naivság, a figyelmetlenség, és a hiszékenységek a fő ellenségünk. Akit pedig részletesebben is érdekel, hogy **mit tehet, ha véletlenül mégis phishing áldozatává válik, annak érdemes egy korábbi részletes összefoglalónkat fellapozni**, melyben [minden ilyenkor szükséges kárenyhítő teendőt és ezzel kapcsolatos megelőző tanácsot csokorba gyűjtöttünk](#).

[Megosztom](#) [tumblr](#) [Tweet](#) [Pin it](#) [g+1](#)

Ajánlott bejegyzések:

[Új haladócsoporthoz Android kártevő](#)
[Nyerjünk 250 ezer eurót. Vagy mégsem?](#)
[LinkedIn meghívó. Vagy mégsem?](#)
[Mai szavunk pedig: keyjacking](#)
[Zsákbamacska autó: fénykép csak kérésre](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6972561>

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.

Rejtett előfizetéssel trükköző cégek

2014.12.12. 16:34 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [mobil statisztika](#) [szolgáltatás büntetés](#) [trójai emeltdíjas kártevő](#)

Három brit vállalatot is megbüntettek nemrégiben ilyen jellegű tisztességtelen magatartás miatt. A vizsgálat szerint **különféle Androidos alkalmazásokba olyan rosszindulatú funkciót rejtettek, amelyek révén az áldozat drága emelt díjas szolgáltatásokra iratkozott fel tudtán kívül.**



A [330 ezer angol fontos bírság mértéke is mutatja](#), komoly dologról van szó. Mint arról a PhonepayPlus biztonsági csapata beszámolt, a trójai alkalmazás használata során a jóhiszemű áldozatok bárhova is kattintottak az app képernyőjén, azzal rejtve feliratkoztak felnőtt tartalmakat értékesítő szolgáltatásokra.

A kártékony alkalmazás arra is ügyelt, hogy eltüntessen a kijelzőről az ilyenkor szokásos minden figyelmeztető üzeneteket. Ezáltal a felhasználók észre sem vették mi történik, és csak a hónap végi számlájukon derült ki a jellemzően 1.5 és 4.5 angol fontnyi heti túlszámlázás, ezzel havi kb. 3-7 ezer forintnak megfelelő összegekkel károsították meg az áldozatokat.



A nyomozás eredményei alapján a Manchesteri székhelyű Circle Marketing 130,000 GBP (50 millió HUF), a Coventry illetőségű Synchronized 120,000 angol fontnyi (47 millió forint), míg [az Edinburgh-ben székelő Cloudspace 80 ezer GBP \(azaz nagyjából 31 forintnak megfelelő\) összegű büntetést volt kénytelen fizetni.](#)

Az Android platform tortaszelete a mobil eszközök piacán ma már 80 százalék feletti, és a trójai alkalmazások száma is évről évre meredeken emelkedik, így [2012-es jóslatunk, miszerint "Az Android az új Vadnyugat"](#) sajnos vastagon beigazolódni látszik.



A mobilos kártevők évről évre egyre komolyabb gondokat okoznak, és a statisztikák szerint sokan nem tartják fontosnak a kártevők elleni védelmi programok használatát. Mint ismeretes, a nemrég ismertettet brit felmérés azt mutatta, hogy [a megkérdezettek közel 60%-a okostelefonján semmilyen védelem nem fut.](#)

Ezzel együtt azonban a felhasználók majdnem fele bankol hordozható okoseszközzel, egy harmaduk pedig rendszeren elektronikusan vásárol is a segítségével, miközben tévesen úgy vélekedik, hogy szemben a klasszikus számítógéppel okostelefonon vagy tableten semmilyen vírus vagy biztonsági fenyegetés nem érheti.



Pedig a statisztika szerint viszont a mobilos kártevők számának növekedés szárnyal, ezért elmondható, hogy itt is a PC-s platformhoz hasonlóan szükség van vírusvédelmi alkalmazásra.

Bár gyártóktól függően különböznek az értékek, de a számok egyébként azt mutatják, hogy míg PC-s környezetben átlagosan 50-80 ezer kártékony kód keletkezik naponta, addig **a mobilos platformon hozzávetőlegesen körülbelül ezer darab per nap a tempó.** A mobilos kártevők mennyiségének emelkedése főként az utóbbi 2 évben gyorsult fel erőteljesen.

 **Tetszik** Regisztráld, hogy megnézd, mi tetszik az ismerőseidnek.

   **Tweet**  **Pin it**  **g+1**

Ajánlott bejegyzések:

[A váltságdíjas titkosító kártevő visszatér](#)
[Itt az első váltságdíjas titkosító kártevő Androidon](#)
[Célzott támadás Ukrajnában és Lengyelországban](#)
[A CryptoWall bevétele átlépte a milliós határt](#)
[Újra Bitcoin bányász kártevő a Google Play-en](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6978227>

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.

6 tipp személyazonosságunk megvédésére

2014.12.15. 18:54 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [tipp](#) [személyes privacy trükk](#) [privátszféra](#) [adatlopás](#) [szivárgás](#) [biztonságtudatosság](#)

A privát szféra megóvása lassan mindegyikünk a gondolkodásába beépül, hiszen mindenki tapasztalt már saját példáján vagy ismeretségi körében olyan incidenseket, lopásokat, amelyek esetleg elkerülhetőek lettek volna egy biztonság tudatosabb hozzáállással. Ennek kapcsán ismertetünk pár, könnyen megfogadható tippet, amelyek betartásával segíthetünk személyes adataink hatékonyabb védelmében.



A Microsoft 2014 végzett egy nemzetközi felmérést, melynek során tízezer embert kérdeztek meg arról, hogy érte-e őket valamilyen személyiséglopás, illetve adatlopás. Az elszenvedett károk, illetve a helyreállítás költségei évről évre már több milliárdos nagyságrendet képviselnek, míg a felmérésben megkérdezettek átlagos kára 632 dollár (156 ezer HUF) volt.

Ezen belül is a válaszadók 15%-a jelezte, hogy volt már áldozata adathalász típusú támadásnak, az itt kiszámolt átlagos veszteség 158 USD összegre, azaz nagyjából negyvenezer forintra jött ki. Ezen felül 13% számolt be arról, hogy a személyiséglopásnak valamilyen további káros következménye is történt, például szakai hírnév, hitelrontás, egyéb visszaélés. [Lássuk akkor végül a biztonsági tippeket!](#)



1. Ismerjük fel a figyelmeztető jeleket

Ha különféle intézmények, hivatalos szervek, bankok, fizetésközvetítők nevében kapunk kéréstlen üzeneteket, figyeljünk a kinézetre, helyesírásra, a linkekre. Kéretlenül kapott levél mellékelte linkjeiben, csatolt mellékleteiben gyakoriak a kártevővel fertőzött állományok. Ellenőrizzük rendszeresen a számlamozgásainkat, és ha egyenlegünkön akármilyen csekély összegű megmagyarázhatatlan terhelés tűnik fel, és teljesen biztosak vagyunk abban, hogy azt nem mi kezdeményeztünk, akkor haladéktalanul keressük fel bankunkat és kérjük, vizsgálják ki, mi történt, haladéktalanul tegyünk bejelentést.

A csalók időnként nem csak a számlát igyekeznek megcsapolni, de a részletes személyes adatok birtokában további kellemetlenségeket is okozhatnak nekünk, például adót igényelnek vissza a nevünkben, vagy ami még rosszabb, hitelt, kölcsönt vesznek fel az ellopott személyazonossággal. Emiatt mindig alaposan olvassuk el a nekünk szóló banki tájékoztatásokat, hivatalos leveleket.



2. Erzékeny, bizalmas információkat ne küldjünk e-mailben

Ha például hitelkártyát kérelmezünk, vagy más olyan ügyet intézünk, amínél tucatszori személyes információt kell megadnunk magunkról, akkor intézzük ezt lehetőleg hagyományos postai úton.

Angol nyelvterületen visszatérő családi forma például az adó-visszatérítéssel kapcsolat átverés, ahol ha valaki naivan megadja az össze személyes adatát, akkor a csalók az ő nevén igénylik azt vissza, majd eltűnnek a pénzzel. Ha privát ügyeinket intézzük, tegyük ezt otthonról saját e-mail címről, és semmiképpen ne a munkahelyi címünk segítségével a benti levelezőrendszeren keresztül.



3. Rendszeresen változtassunk banki jelszót

Ez tulajdonképpen minden fajta szolgáltatás (levelezés, közösségi oldalak, fizetés közvetítő, aukciós portál, bank) igaz kellene hogy legyen. **Ne csak akkor változtassuk meg a jelszót, ha gyanítjuk vagy biztosak vagyunk személyes adataink ellopásában, hanem rendszeres időközönként csak úgy is.** Ne felejtjük el, hogy a jelszó csak akkor ér valamit, ha erős és egyedi - azaz máshol nem használjuk ugyanazt.

Emellett ha a szolgáltató valamilyen okból (például támadás, szivárgás, belső visszaélés, stb.) jelszócserére figyelmeztet, akkor ne hagyjuk ezt figyelmen kívül, és változtassuk meg haladéktalanul.



4. Ha valaki felhív minket, az ő feladata bebizonyítani azt, hogy ki ő valójában

A support átverés esetén a gyanútlan áldozat kap egy kéretlen emailt vagy egyre gyakrabban valamilyen telefonhívást, melyben nem létező mondvacsínált technikai hibára figyelmeztetik - néha arcátlanul akár a Microsoft nevében jelentkeznek - majd végül borsos számlát nyújtanak be a semmiért, illetve kártékony kódokat, vagy távoli hozzáférést biztosító weboldalakra próbálják meg el irányítani a naiv felhasználókat.

Emellett igen gyakori a személyes adatok kikérdezése is, amikor a csaló a bank nevében tőlünk kéri a részletes személyes adataink beolvasását "megerősítésképpen". Vessük az eszünkbe, hogy a vonal végén bárki lehet, így sose adjunk ki így személyes adatokat és sürgetni se hagyjuk magunkat. Gyanú esetén bontsuk a vonalat, és nyomban tárcsázzuk a bankunkat.



5. Otthonunkban, lakásunkban is óvjuk a személyes adatokat

Aki olvasta Kevin Mitnick könyveit, az jól tudhatja, az információ szerzés egyik hatékony formája a célba vett személy szemetesének alapos vizsgálata. De a lakás azon részében sem érdemes számlákat, hivatalos iratok elől hagyni, ahol házhoz szállítók, postás, vendégek,

látogatók könnyen hozzáférhetnek.

Nem csak a készpénz és az ékszer az, aminek illik egy trezorban, vagy legalább elzárt helyen lennie, hanem a személyazonosításra alkalmas iratoknak is érdemes zárható helyet keresni. Ha pedig esetleg betörnének, akkor az iratok, igazolványok esetleges eltűnését is feltétlenül ellenőrizni kell.



6. Vigyázzunk a Facebookos kvízekkel, ingyen akciókkal

Sok esetben a személyes adatok tömeges begyűjtése a cél, a nyeremény játékok többsége pontosan erről szól. **Sokszor azt sem tudjuk pontosan, hogy az ilyenkor begyűjtött adatokat kinek adják tovább, vagy adják el marketing célokra, így érdemes egészséges gyanakvással megadni a személyes adatokat, különösen ha sok és túl részletes kérdést szegeznek nekünk látszólag indokolatlanul.**

Hasonló a helyzet az ingyen nyereményt ígérő kampányokkal, ahol később az itt megadott mobilszámra SMS spamok érkezésére is számíthatunk. Itt is igaz, hogy ami akció túl szép ahhoz, hogy igaz legyen, az többnyire valóban nem igaz, hanem átverés.



Tetszik 20 személy kedveli ezt [Regisztrálj](#), hogy megnézd, mi tetszik az ismerőseidnek.

Megosztom **tumblr** **Tweet** **Pin it** **+1**

Ajánlott bejegyzések:

[Uber hack - 50 ezer sofőr adata bánta](#)
[Védelmi tippek az iskolakezdésre](#)
[Facebook csoportot csak őstermelőtől](#)
[Így változtunk Snowden óta](#)
[Kormányzati e-mailek kontra biztonság](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6985481>

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.

Bitcoinos zsaroló járja be Európát

2014.12.18. 09:52 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

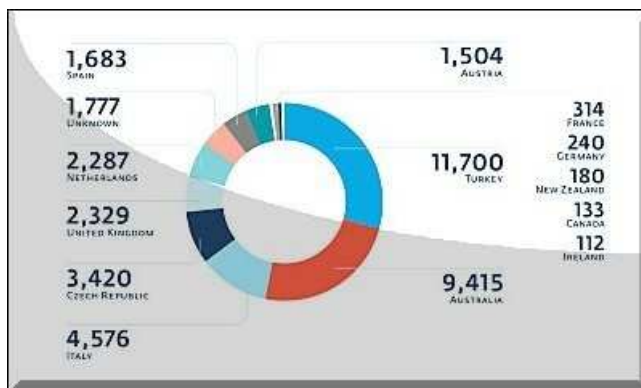
Címkék: [backup](#) [európa](#) [mentés](#) [kártévő](#) [zsaroló](#) [ransomware](#) [bitcoin](#) [cryptolocker](#) [torrentlocker](#)

Az ESET kanadai kutatói alaposan megvizsgálták az év elején megjelenő TorrentLocker nevű zsarolóprogram működését. A malware legutolsó változata legalább 40,000 rendszert fertőzött meg pár hónap alatt, és leginkább az európai országokban szedte áldozatait.



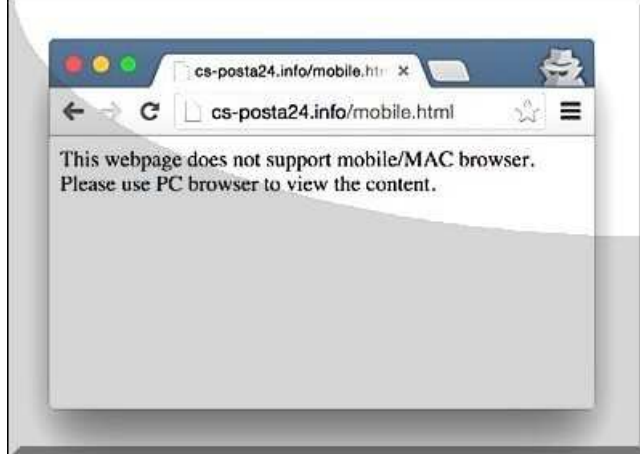
A szakemberek most elkészítették a zsarolóprogramra vonatkozó kutatásuk háttéranyagát, amely a malware viselkedésének vizsgálatát és részletes elemzését tartalmazza. Az ESET Win32/Filecoder.DI névvel azonosítja a TorrentLocker mostani verzióját. Az elnevezés a malware korai korszakából ered, hiszen a program ezt a "Bit Torrent Application" elnevezésű registry kulcs bejegyzést használta konfiguráció beállításainak tárolására.

Az összefoglaló szerint a TorrentLocker hét különböző módon terjedt és a telemetria mérésnek köszönhetően kiderült, hogy a malware első nyomai még 2014. februárjában bukkantak fel. A rosszindulatú program folyamatosan fejlődik, a kártévőcsalád legfejlettebb variánsa augusztustól szedte áldozatait.



A zsarolóprogramnak ez a változata dokumentumokat, képeket és egyéb fontos fájlokat titkosít a felhasználó eszközén és váltságdíj fejében engedélyezi csak a hozzáférést a fájlokhoz. Jellegzetessége, hogy a váltságdíjat kizárólag virtuális valutában lehet kifizetni és akár 4 bitcoint (ez nagyjából 1180 euró vagy 1500 dollár) is követelhet.

Az utolsó kampányban a TorrentLocker 40,000 számítógépet fertőzött meg és több mint 280 millió dokumentumot titkosított. A célzott országok zöme ugyan európai volt, de a fertőzés már Kanadában, Ausztráliában és Új-Zélandon is megjelent. Szerencsére "csak" 570 áldozat fizette ki a követelt váltságdíjat, de még így is összesen 585,401 bitcoin ütötte a TorrentLocker mögött álló bűnözői csoport markát.



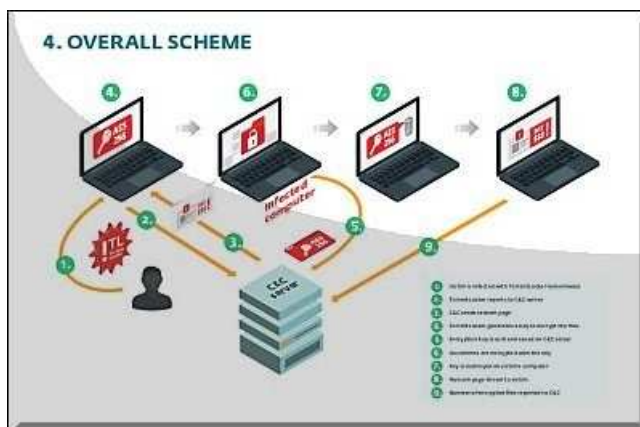
□ arc-Etienne M. Léveillé, az ESET kanadai kutatója szerint a TorrentLocker mögött álló személyek ugyanazok lehetnek, akik a Hesperbot nevű banki trójai család mögött álltak. A TorrentLocker-ben a támadók reagáltak az online biztonságtechnikai jelentésekre, hiszen megkerülik az ilyen típusú kártevők felismerésére szolgáló eljárásokat és megváltoztatták az AES (Advanced Encryption Standards) titkosítási módszerüket CTR-ről (Counter mode) CBC típusúra (Cipher block chaining mode), annak hatására, hogy ismertté vált egy módszer a kulcsfolyamuk megszerzésére.

Ennek következtében a TorrentLocker áldozatai már nem tudják visszaállítani a dokumentumaikat az elkódolt fájljaik és az egyszerű szöveges állományának kombinálásával megszerzett kulcsfolyam segítségével.



A folyamat úgy zajlik, hogy a leendő áldozat kap egy fertőzött dokumentumot tartalmazó kéréstlen e-mail. A mellékelt fájl megnyitása általában egy ki nem fizetett számlát, csomagok nyomon követését vagy kifizetetlen gyorshajtási büntetést tartalmaz. Az e-mail hitelességét erősíti, hogy az áldozat közvetlen környezetéből származó üzleti vagy kormányzati honlapokat utánoz.

Ha olyan áldozat olvasta az emailt, aki nem a célországából kattintott a linkre és kezdeményezte az oldal letöltését, akkor automatikusan a Google search oldalra irányította a kártevő. Az áldozatok becsapásának érdekében a támadók CAPTCHA képeket is illesztettek a levelekbe, így keltve hamis biztonságérzetet.



A teljes kutatás és [a malware bemutatása WeLiveSecurity.com](#) blogon érhető el, míg a [részletes elemzés \(technical white paper\)](#) pedig [ezen a linken](#) olvasható.

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

Ajánlott bejegyzések:

[Mentési tippek CryptoLocker ellen](#)
[Véddij a CryptoLocker terjesztőjének fejére](#)
[Magyarországra is megérkezett a CTB-Locker](#)
[Kisokos a Cryptolocker kártevő ellen](#)
[De elfogadunk akár Bitcoint is...](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/6994267>

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.

Képes malware történelem és novemberi toplista

2014.12.23. 10:38 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [statisztika](#) [radar](#) [november adatok](#) [nod32 report](#) [threat](#) [vírusstatisztika 2014.](#) [hvi](#)

Az ESET minden hónapban összeállítja a világszerte terjedő számítógépes vírusok toplistáját, melyből megtudhatjuk, hogy aktuálisan milyen kártevők veszélyeztetik leginkább a felhasználók számítógépeit. 2014. novemberében a következő 10 károkozó terjedt a legnagyobb számban.



Harmadik hónapja vezeti a listát a HTML/Refresh. Ez egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található. Ismét listatag lett a Win32/Ramnit, ezúttal a kilencedik helyre elegendő teljesítményével vívta ki a jelenléte.

Ez egy olyan fájlfertőző vírus, amelynek kódja minden rendszerindításkor lefutva DLL és EXE formátumú állományokat képes megfertőzni, valamint 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 fertőzött számítógépen.**



És végül, de semmiképpen nem utolsó sorban látszólag nem képes hibázni az Autorun vírus. Érdekes módon 2011. április óta nem tud lekerülni a listánkról az Autorun vírus, sőt az előző havi 10-ik helyről most a 8-ik pozícióba merészkedett vissza.

A rekord hosszúságú szereplés okairól már többször is szót ejtettünk, hiszen már évek óta rendelkezésre áll a sebezhetőséget bezáró, illetve az automatikus indulást lekapcsoló biztonsági frissítés. Ám sajnos sokan ezt azóta sem futtatták le, részint lustaságból, részint mert az érintett gépek egy része valószínűleg illegális Windows példányt futtat. Emellett pedig számos felhasználónál futhat még a régi, már nem támogatott XP verzió is.



Az ESET Radar Report e havi kiadásában ezúttal folytatódik az előző hónapban megkezdett téma, amely az úgynevezett support csalásokról szól. Az ilyen típusú támadások sajnos már évek óta zajlanak világszerte. A módszer lényege, hogy elsősorban az angol nyelvterületen élő gyanútlan áldozat kap egy telefonhívást, melyben nem létező technikai hibára figyelmeztetik. **A dolog apropója pedig az, hogy az FTC (U.S. Federal Trade Commission) azaz az amerikai fogyasztóvédelmi hatóság vizsgálatot folytat egy ilyen cég ellen. A gyanú szerint a New York-i székhelyű Pairsys Inc. cég iparszerűen üzte az ilyen jellegű csalásokat,** és a Microsoft, illetve a Facebook technikai személyzetének kiadva magukat kiterjedt telemarketing rendszert üzemeltettek az ilyen hamis hívások nagy számban történő megvalósításához.

A mondvacsinált, nem létező problémák "kijavításáért" busás munkadíjat szedtek be az áldozatoktól, ez jellemzően 149 és 249 USD közötti összeg volt - mai árfolyamon körülbelül 37-62 ezer forintnak felel meg. Az üzletszerű csalásokról Brian Krebs biztonsági szakértő is rendszeresen publikál a blogjában, és bár eredetileg az USA volt a fellekvára az ilyen átveréseknek, egyre több jel mutat arra, hogy az érdeemi "munkát" a bűnözők kiszervezik Indiába. Mi mindenesetre azt emeljük ki az ügy kapcsán, hogy érdemes óvatosnak lenni az ilyen kéretlen telefonhívások esetén, és gyanú esetén inkább egyszerűen tegyük le a kagylót, mielőtt valamilyen kémprogramra, kártevőre mutató oldalra navigálnak bennünket a hamis "segítők".

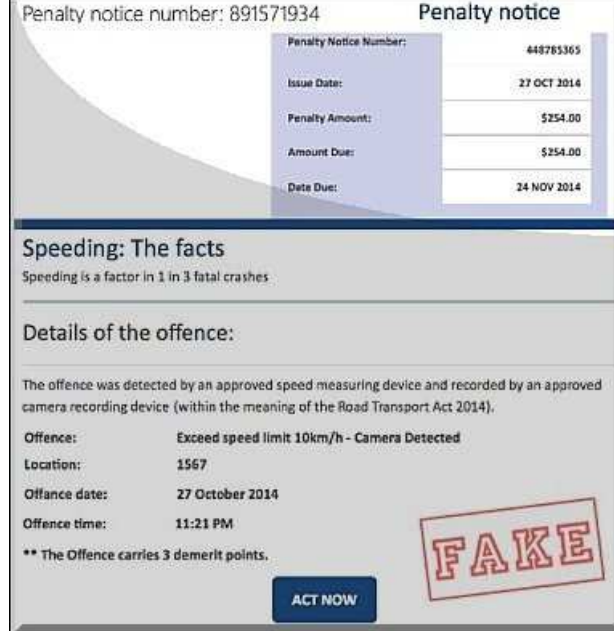


Emellett egy infografikán igyekszünk bemutatni a számítógépes kártevők történetét. Az összefoglalóból kiderül, hogy a kezdeti híres, hírhedt vírusokon, a világjárványt okozó férgek át hogyan jutottunk el a rejtett kémprogramokig, vagy napjainkban egyre gyakoribb állami kártevőkhöz.

Az infograika az 1986-ban megjelent, és a vírustörténelem „nulla kilométerkövének” tartott pakisztáni Brain vírustól egészen napjaink, 2014-es botnetes kártevőkhöz tartó időszakot mutatja be igen látványosan.



Novemberi fontosabb blogposztjaink között [Halloween alkalmával védelmi tippeketadtunk](#) az ilyenkor fokozódó veszélyek miatt, és emellett összegyűjtöttük az eddigi öt legfélelmetesebb zombi botnetet is.



Emellett szót ejtettünk arról az [újfajta social engineering trükkéről is, melyben gyorsajtási bírsággal is terjed a CryptoLocker](#). Az ausztráliai Új-Dél-Walesben figyeltek fel ugyanis arra a módszerre, hogy az e-mailben terjedő üzenetekben hamis linkek segítségével egy állami hivatal nevével visszaélve igyekeztek a gyanútlan és talán gyorsan is hajtó felhasználók gépeire kártevőt letölteni.

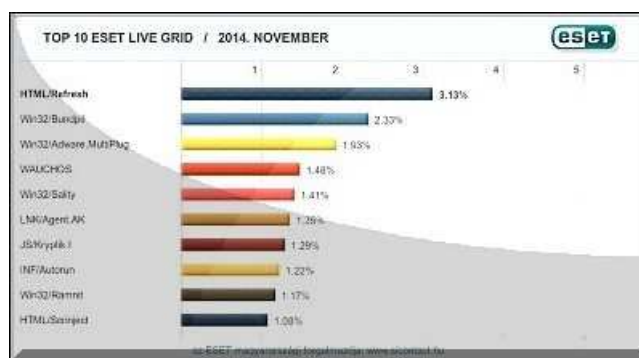


Beszámoltunk ezenkívül arról is, hogy **nem csak a tüdőre lehet káros az e-cigaretta**, ez derült ki ugyanis a Guardian egyik cikkéből. A dolog lényege, hogy az Autorun vírus nem csak a klasszikus USB kulcs, memóriakártya, vagy külső merevlemez segítségével képes fertőzni, hanem például fényképezőgép, MP3 lejátszó, okosóra, digitális képkeret vagy [akár az USB töltési lehetőséggel rendelkező e-cigaretta is jelenthet ilyen veszélyt](#).



Végül megemlítettünk egy érdekes brit felmérést is, melynek eredményeiből az látszik, hogy az ottani [felőtt lakosságból minden hatodik felhasználó szenvedett már el valamilyen kibertámadást](#). Az incidensek közül az adathalászat, a személyes adatok eltulajdonítása illetve banki adatok kifürkészése, manipulálása a leggyakoribb.

Sajnos azonban az is kiderült, hogy a felhasználók jelentős hányada egyáltalán nem is védi az eszközeit biztonsági alkalmazásokkal.



Virusstoplista

Az ESET több millió felhasználó visszajelzésein alapuló statisztikai rendszere szerint **2014. novemberében a következő 10 károkozó terjedt világszerte a legnagyobb számban**, és volt együttesen felelős az összes fertőzés 16.39%-áért. Aki pedig folyamatosan és első kézből szeretne értesülni a legújabb Facebook-os kártevőkről, a közösségi oldalt érintő mindenfajta megtevesztésről, az csatlakozhat hozzánk az ESET Magyarország www.facebook.com/biztonsag, illetve az antivirusblog.hu oldalán.



01. HTML/Refresh trójai

Elterjedtsége a novemberi fertőzések között: 3.13%

Működés: A HTML/Refresh egy olyan trójai család, amelyik észrevétlenül átirányítja a felhasználó böngészőjét különféle rosszindulatú web címekre. A kártevő jellemzően a manipulált weboldalak HTML kódjába beágyazva található.



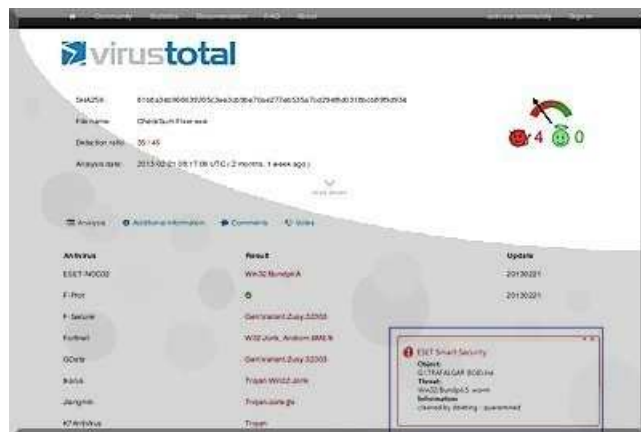
Bővebb információ: http://www.virusradar.com/en/HTML_Refresh/detail



02. Win32/Bundpil féreg

Elterjedtsége a novemberi fertőzések között: 2.33%

Működés: A Win32/Bundpil 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.



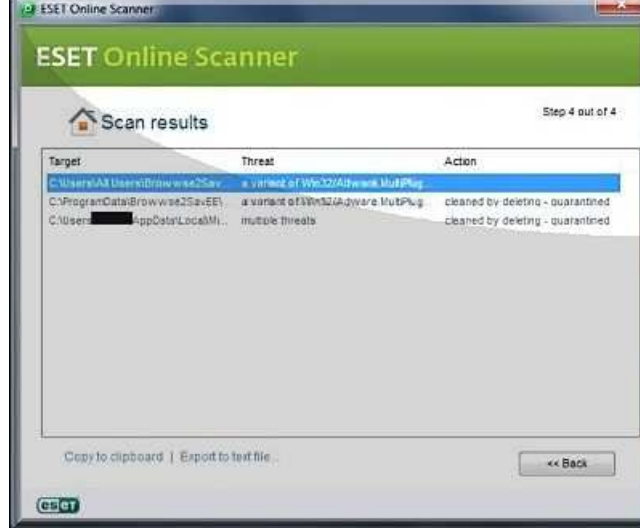
Bővebb információ: http://www.virusradar.com/en/Win32_Bundpil.A/description



03. Win32/Adware.MultiPlug adware

Elterjedtsége a novemberi fertőzések között: 1.93%

Működés: A Win32/Adware.MultiPlug egy olyan úgynevezett nemkívánatos alkalmazás (Potential Unwanted Program, PUP), amely a felhasználó rendszerébe bekerülve különféle felugró ablakokban kényszerű reklámokat jelenít meg az internetes böngészés közben.



Bővebb információ: http://www.virusradar.com/en/Win32_Adware.MultiPlug.H/description



04. Win32/TrojanDownloader.Wauchos trójai

Elterjedtsége a novemberi fertőzések között: 1.48%

Működés: A Win32/TrojanDownloader.Wauchos egy olyan trójai, amelynek fő célja további kártékony kódokat letölteni az internetről a fertőzött számítógépre. Különböző registry kulcsok létrehozásával gondoskodik arról, hogy minden rendszerindításkor lefusson a kódja. Hátsó ajtót nyit a megtámadott rendszeren, és ezen keresztül próbál meg adatokat továbbítani a gép operációs rendszeréről, beállításairól, IP címéről, illetve ezen keresztül parancsokat fogad, így a támadóknak távolról tetszőleges kód futtatására nyílik lehetőség.



Bővebb információ: http://www.virusradar.com/Win32_TrojanDownloader.Wauchos.A/description



05. Win32/Sality vírus

Elterjedtsége a novemberi fertőzések között: 1.41%

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.



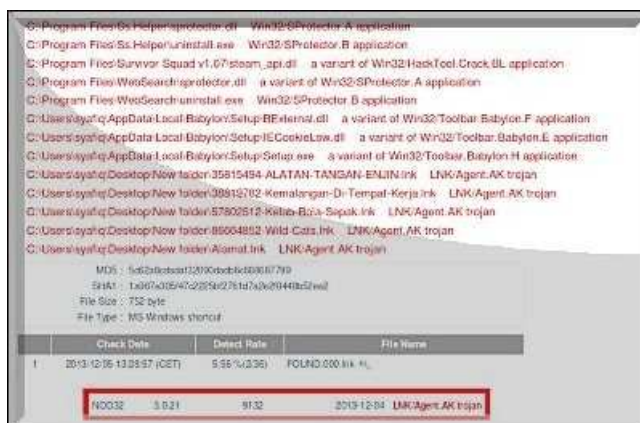
Bővebb információ: http://www.virusradar.com/Win32_Sality.NAR/description



06. LNK/Agent trójai

Elterjedtsége a novemberi fertőzések között: 1.35%

Működés: A LNK/Agent trójai fő feladata, hogy a háttérben különféle létező és legitim - alaphelyzetben egyébként ártalmatlan - Windows parancsokból kártékony célú utasítássorozatot 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. Vírusselemlők véleménye szerint ez a módszer lehet a jövő Autorun.inf szerű kártevője, ami valószínűleg szintén széles körben és hosszú ideig lehet képes terjedni.

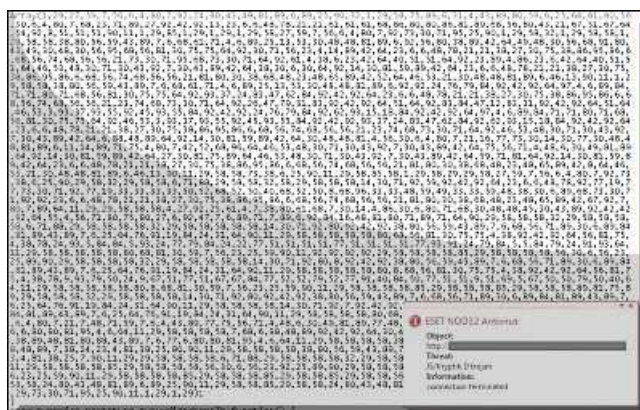


Bővebb információ: http://www.virusradar.com/en/LNK_Agent.AK/description

07. JS/Kryptik trójai

Elterjedtsége a novemberi fertőzések között: 1.29%

Működés: A JS/Kryptik egy általános összesítő elnevezése azoknak a különféle kártékony és olvashatatlan összezárt JavaScript kódoknak, amely a különféle HTML oldalakba rejtetten beágyazódva észrevétlenül sebezhetőségeket kihasználó kártékony weboldalakra irányítja át a felhasználó böngészőprogramját.

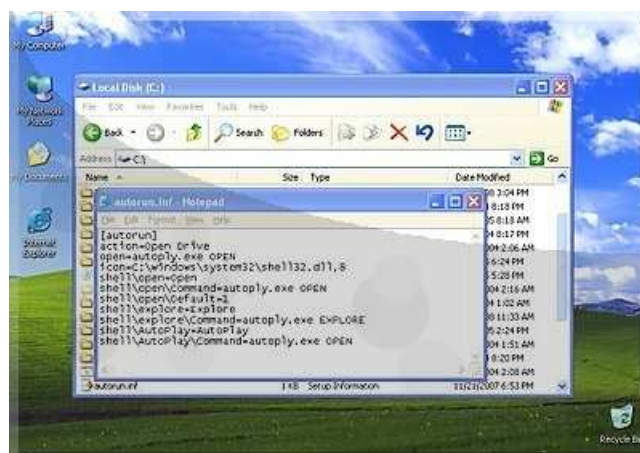


Bővebb információ: http://www.virusradar.com/en/JS_Kryptik/detail

08. INF/Autorun vírus

Elterjedtsége a novemberi fertőzések között: 1.22%

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

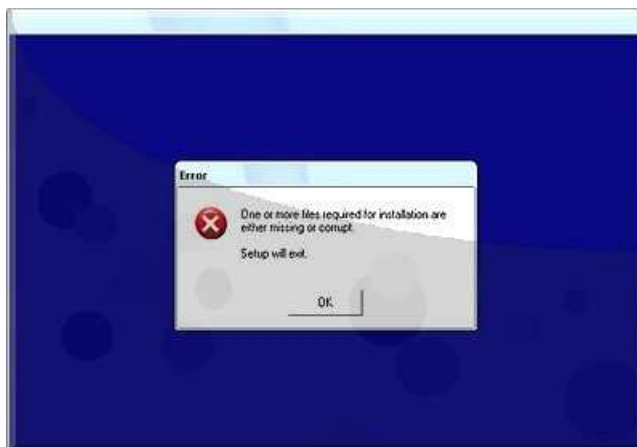


Bővebb információ: <http://www.eset.hu/tamogatas/viruslabor/virusleirasok/%21autorun>

09. Win32/Ramnit vírus

Elterjedtsége a novemberi 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.



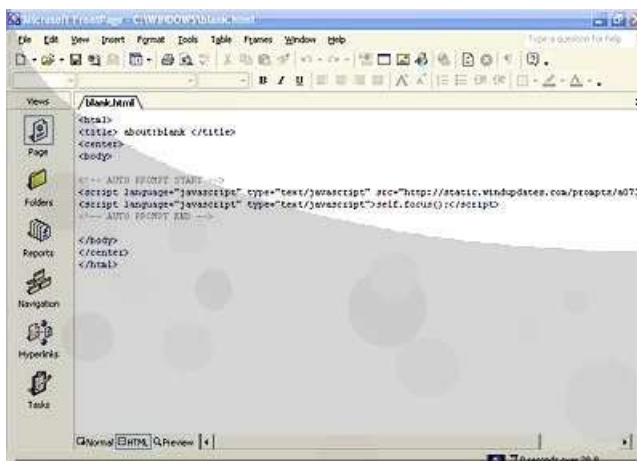
Bővebb információ: http://www.virusradar.com/Win32_Ramnit.A/description?lng=en



10. HTML/ScrInject trójai

Elterjedtsége a novemberi fertőzések között: 1.08%

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 kísér meg letölteni.



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

 Tetszik Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[A HTML trójaiak riogattak minket októberben](#)

[Végre kiesett a Conficker féreg](#)

[Vírusedzőlista 2014. augusztus hónap](#)

[Júliusi vírusedzőlista](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/7006083>

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

2014.12.24. 13:03 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [karácsony](#) [xmas](#) [hellókarácsony](#)

Boldog Karácsonyt és sikerekben gazdag Új Évet kívánunk az oldal minden látogatójának!



*"The Christmas is coming, the goose are getting fat
Please put a penny in the old man's hat
If you haven't got a penny, a ha'penny will do
If you haven't got a ha'penny, then God bless you!"*





 **Tetszik** Regisztrálj, hogy megnézd, mi tetszik az ismerőseidnek.

Ajánlott bejegyzések:

[Kellemes Karácsonyi Ünnepeket](#)

[Kellemes Karácsonyi Ünnepeket](#)

[Kellemes Karácsonyi Ünnepeket](#)

[Béták reggelire](#)

[Karácsonyi ajándékok vírusíróknak és irtóknak :-\)](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/7008543>

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](#).

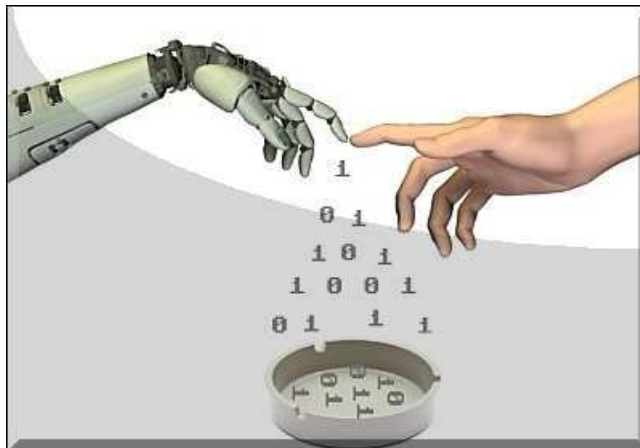
Nincsenek hozzászólások.

Top 10 IT biztonsági bejegyzés 2014-ben

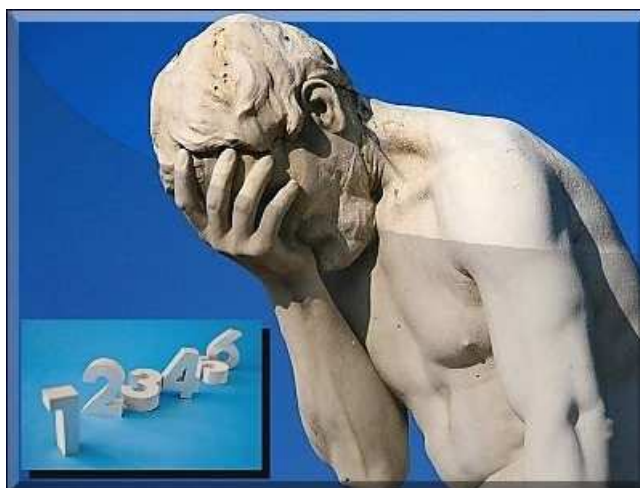
2014.12.29. 11:47 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [toplista](#) [incidens](#) [posztok](#) [antivirus.blog](#) [antivirus.blog.hu](#) [2014.](#) [legolvasottabb](#)

Nyakunkon az év vége, ez pedig egyúttal a visszatekintések ideje is. Megnéztük, mely [antivirus.blog](#) posztok tartottak számot olvasóink legnagyobb érdeklődésére ebben a hamarosan záródó 2014-es esztendőben, és ezek közül válogattuk ki a tíz legérdekesebb bejegyzésünket.



Nem csak az Android platform elterjedtsége döntött rekordokat az idei évben, de a mobil kártevők száma is exponenciális mértékben emelkedett. Valójában csak folytatódott a korábbi trend, hiszen a 2012-ről 2013-ig terjedő időszak alatt is már 63%-os emelkedést lehetett tapasztalni. [Összeállításunkban összeszedtünk mindenféle hasznos tippet ahhoz, hogy mit tegyünk a biztonságunkért, ha Androidos okostelefont](#) rejt a zsebünk vagy a retikülünk?



A jelszó választás egy elég jelentős kulcskérdés a biztonságban, elég ha csak az iCloud-ról kiszivárgott meztelen "celebfotókra" gondolunk, amiben az Apple hibáján felül a felhasználók primitív jelszóválasztási, jelszóismétlési szokásai is vastagon belejártak. [Infografikás sorozatunkban ezúttal egy ebben témában készült felmérés eredményei szerepelnek egy látványos és tanulságos ábrában.](#)

Például 16%-a a felhasználóknak sosem változtatja meg a jelszavát, és 18%-uk figyelmen kívül hagyja a jelzést, ha az általa leggyakrabban használt online vagy közösségi oldal jelszócserére figyelmeztető üzenetet küld neki.



2014 egyik legjelentősebb kártevője a CryptoLocker volt. A botnetek is nagy erővel terjesztették ezt a zsaroló programot, amely adataink elkódolásával fenyegetett bennünket.

[Összefoglaltuk, mit lehet tenni, ha egy ilyen kártevő bejut a Windowsos gépünkbe](#), és azt láttuk, a komoly károkozások miatt sajnos elég keveset, így elsősorban a megelőzésre kell tennünk a hangsúlyt.



Érdekes módon egy szimpla szolgálati közlemény is felemelkedett a legolvasottabb posztok elit csapatába. Mindenesetre akkor most itt is elismételjük, hogy [még februárban kettéválasztottuk a szerző magánemberi és az antivirus.blog Facebook oldalát](#), így február óta már a www.facebook.com/antivirusblog oldalon vagyunk elérhetőek, olvashatóak, kommentelhetők és akár lájkolhatók.



Talán a hangzatos cím és az Index címlapos megjelenés bontotta a vitorláját annak a posztoknak, amely más szavakkal a ["hogyan bukjuk el 5 perc alatt egész életünk során megtakarított nyugdíjunkat"](#) kérdésre adott egy lehetséges választ. Ez pedig esetünkben nem volt más, mint az online társkeresési csalás csapdájába való jóhiszemű besétálás.



Az Androidos kártevők folyamatos evolúciójában idővel nem csak mennyiségi, hanem minőségi fejlődés is megfigyelhető. [Ennek egy érdekes állomásaként számoltunk be olyan új malware-ről, amely az ismert támadási vektorokat egyesítve](#) ezeket párhuzamosan, egyszerre alkalmazza, így beveti nem csak a "szokásos" rejtett feliratkozást emelt díjas SMS-re és az adatlopást, hanem kiegészülve mindezeket számos más változatos büntető rutinnal, valamint közösségi oldalokról ismert social engineering terjedési módszerrel is.



Milyen lehetőségeket képes kínálni egy Androidon futó biztonsági csomagban szereplő lopásvédelem? Erre kerestük a választ az ESET Mobile Security legújabb Androidos változatának megjelenése kapcsán, [amely új funkciókkal felvértezve látott napvilágot](#).

Például üzenhetünk a beépített kamera által amúgy is lefényképezett tolvajnak vagy ha hamar észbe kapunk, bekapcsolhatunk a készüléken egy vijjogó szirénát.



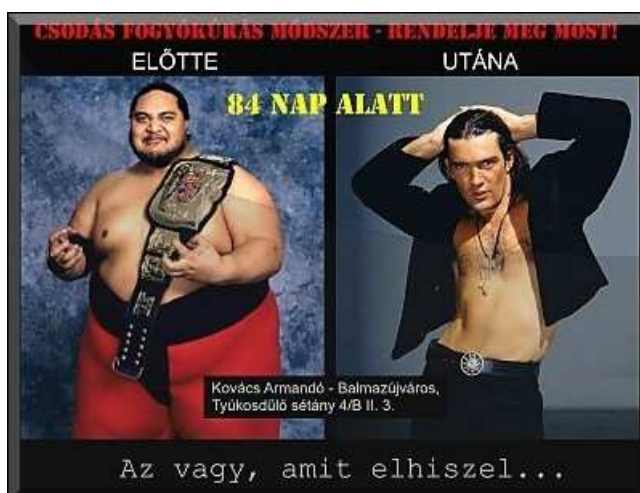
Nem nélkülözte a bulváros címadást ez a poszt sem, az incidens pedig egyenesen az USA-be vezet el bennünket. Connecticut környékén ugyanis gyanúsán megszaporodtak a bankkártya adatokkal történő visszaélések, szemlátomást rendszeresen szivárogtak az adatok valahonnan. Az áldozatok pedig meglepve tapasztalhatták, hogy időnként [a nevükben idegenek vásárolgatnak a kártyájukkal, pedig azt el sem vesztették](#).

A nyomozás később azt derítette ki, hogy azok voltak a kárvalottak, akik Connecticut térségében a Key Road Car Wash nevű autómosókban jártak, ahol a POS terminálokat a távoli hozzáférést biztosító pcAnywhere programmal figyelte meg a támadó, aki aztán az elloptott hitelkártya adatok segítségével klónozza is a kártyákat.



Szóba került emellett természetesen az egyik legklasszikusabb social engineering trükk is, amelyben egy állítólagosan be nem fizetett számla miatti figyelmeztetés formájában érkezik kényszerítő e-mail útján.

A módszer sajnos nagyon is működőképes, mert [ha valaki mérges, ideges, vagy zaklatott, akkor sokkal könnyebben elveszti az önuralmát és ilyenkor hajlamos arra, hogy mégis rákattintson](#) az állítólagos tartozást, vagy vásárlást "bizonyító" mellékletekre.



Végül [a hiszékenység vámszedőit is tollhegyre, azaz billentyűzetre tűztük amúgy virtuálisan](#), beszámolva egy csodás fogyókúrával kapcsolat spam üzenetről.

Ha valaki veszi a fáradságot és a kamu weboldalak kamu sikertörténetek szereplőinek fotóját fordított képkereséssel ellenőrzi az interneten például a TinEye segítségével, akkor akár könnyen lelepleződhet az is, hogyan lett Roberta Saumból Hertelendy Ildikó, vagy Sheile Kibe miként változott át egy csapásra Némethiné Nagy Tímeává.

Ajánlott bejegyzések:

[Beváltak-e a 2014-es jóslatok?](#)

[Uber hack - 50 ezer sofőr adata bánta](#)

[A bank sosem hív bennünket, hogy mi a PIN kód](#)

[Munkavállalói adatok szivárogtak az Nvidiatól](#)

[Képes malware történelem és novemberi toplistá](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/7019265>

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.

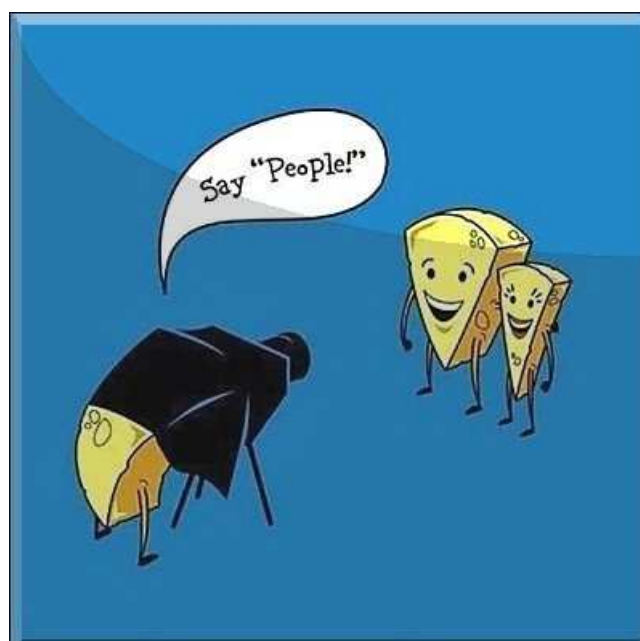
Boldog Új Évet Kívánunk! - 2015

2014.12.31. 10:59 | [Csizmazia Darab István \[Rambo\]](#) | [Szólj hozzá!](#)

Címkék: [új boldog évet 2015](#)

Az Antivirus.blog nevében Minden Kedves Olvasónknak Egészségben, sikerekben gazdag, feltörés- és adatszivárgásmentes Boldog Új Esztendőt kívánunk!







Ajánlott bejegyzések:

[Boldog Új Évet Kívánunk!](#)
[Boldog Új Évet Kívánunk!](#)
[Beváltak-e az idei jóslatok?](#)
[Safe mód a Mechagodzilla ellen](#)
[Új böngésző a háznál](#)

A bejegyzés trackback címe:

<http://antivirus.blog.hu/api/trackback/id/7025741>

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.