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 meg-

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

bújó 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.

Mit szeret a kártevő?

Mégis mi az, ami miatt az „íme tesék, 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.

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

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.

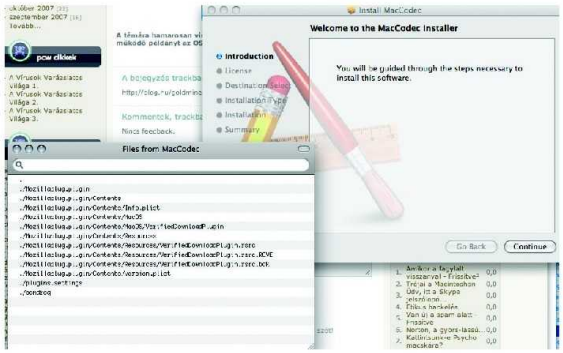
Technikai szempontból az Internet Explorer, az Outlook és a kimondottan veszélyes ActiveX-ek is sokat rontottak a Windows biztonsági helyzetén. Bár a Vista nagymértékben javított a Windows jogosultsági rendszerén, a korábbi Windowsokat még mindig olyan sokan használják, hogy a Vista újdonságai nem befolyásolják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

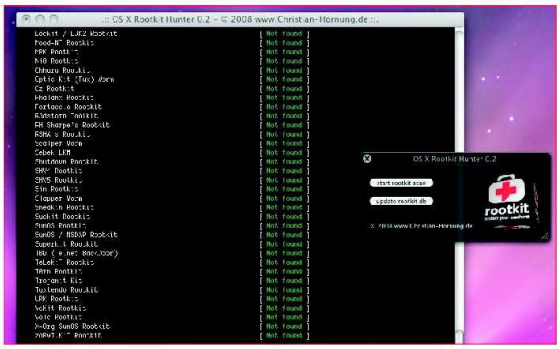
Éles ellentétben áll a Windows és a Linux a forráskód elérhetőségének szempontjából is. A nyílt (open source) alapokon nyugvó kódba bárki betekinthet, megfelelő szakértelem birtokában akár változtathat is rajta, de mindenesetre azonnal észreveheti, hogy annak belsejében pontosan mi történik. Ebből következik, 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.

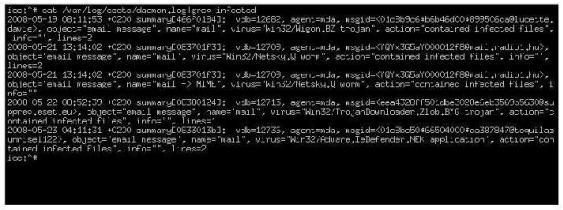
Mivel a végrehajtható fájlok szerkezete lényegesen különbözik Windows és Linux rendszerek alatt, volt, akit ez motivált egy érdekes, mindkét platformon futó vírus megírására. A 29A hackercsapat egyik tagja, *Benny* készítette el a W32/Winux nevű nyílt forráskódú kártevőt: ez képes volt megfertőzni mind 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

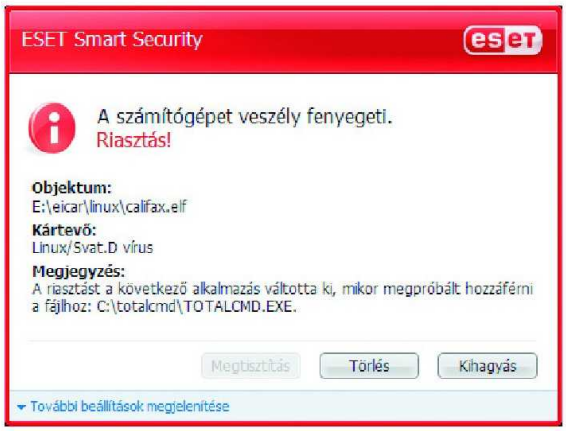
2007-ben egy igencsak érdekes kártevő bukkant fel, a Badbunny.A. Ez az OpenOffice-felhasználókat vette célba: a dokumentumfájlokban próbált meg terjedni Windows, Linux és Mac OS operációs rendszerek alatt egyaránt. Tulajdonságaiban a



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



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

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 még is letett valamit az asztalra: elmondható, hogy létezett egy, gyakorlatilag terjedésre képtelen, makróvírus OpenOffice-ra.

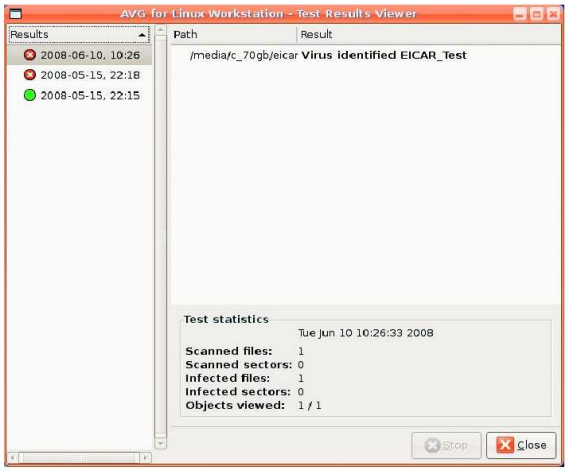
A Mac OS sem bevehetetlen

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.

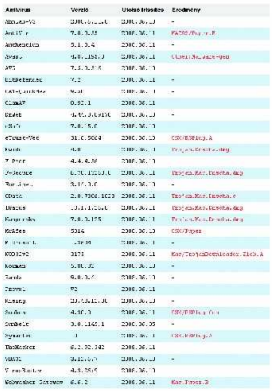


A Linux alatti víruskeresőkkel a Windows-partíciókat vagy mappákat vizsgálhatjuk, illetve a levelekhez csatolt vírusokat kereshetjük. Itt éppen az Eicar nevű tesztvírus akadt fent a horgon

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**