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. a függvénykészletbe, melyet a gépre telepített programok rendre meghívnak –, és azt magára irányítva ellenőrzi, átalakítja annak eredeti működését. Ha például egy olyan kat, amelyek által megszerezhető a rendszergazdai szintű hozzáférés. Sokkal inkább az a fő célkitűzése, hogy lehetővé tegye a behatoló számára ténykedésének, valamint

```
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

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

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?

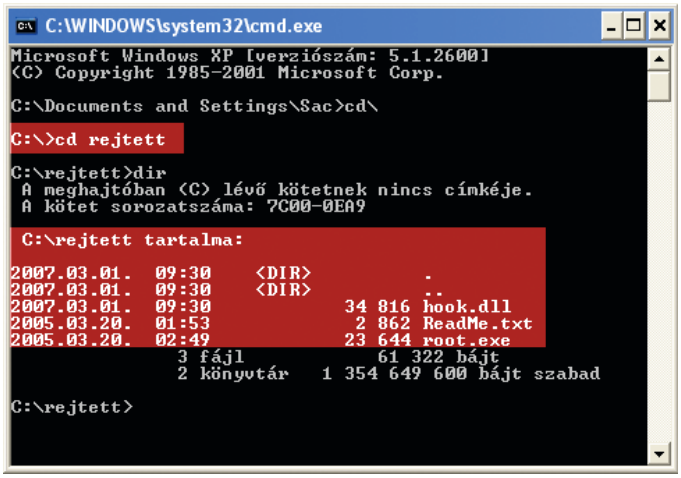
A definíció szerint olyan programokról van szó, melyek képesek eltitkolni saját vagy más szoftverek jelenlétét. Önmagában a rootkit-technológia nem jelent veszélyt: hasonlatosan például az atommaghasadáshoz, amelyet lehet jó célokkal atomerőművekben energiatermeléshez használni, de rossz szándékkal nukleáris 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?

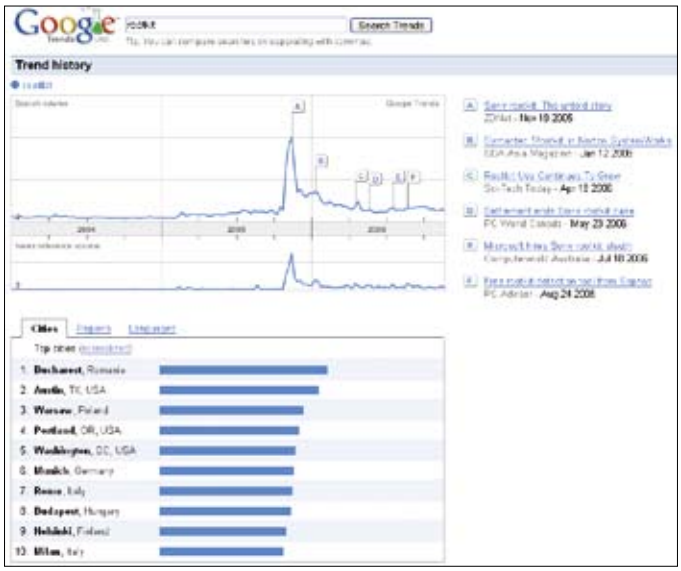
A rootkit beépül az operációs rendszer API (Application Program Interface) rétegébe – magyarul abba könyvtár listázására adunk utasítást, amelyben a rosszindulatú kódot tartalmazó program található, akkor ennek neve a manipuláció révén hiányozni fog a listából. Ugyanez történhet egy adott rendszerleíró 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 a rendszer sebezhetőségének leplezését.



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



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

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-

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

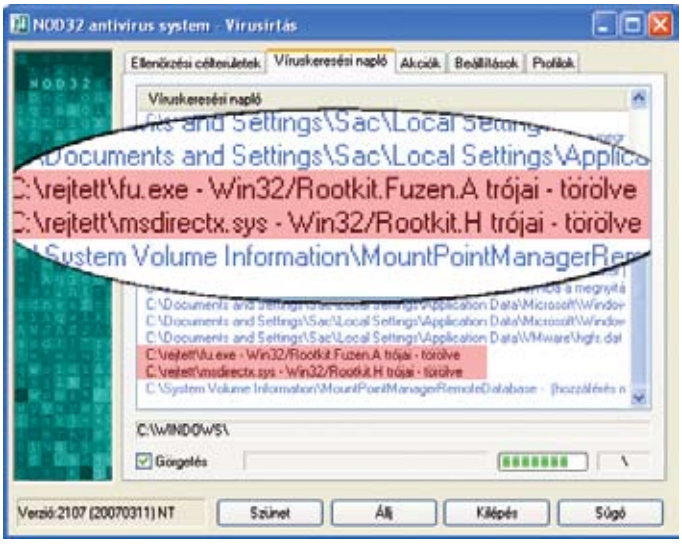
A Winternals Software társalapítója és vezető szoftvermérnöke, *Mark Russinovich* leplezte le a Sony BMG által használt, rootkitalapú CD-másolásvédelmet. Őt olyan jelentős programok készítőjeként ismerhetjük, mint a RegMon, FileMon, ProcessExplorer vagy éppenséggel a rootkiteket felderítő RootkitRevealer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



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

re, 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 Vateránban 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.

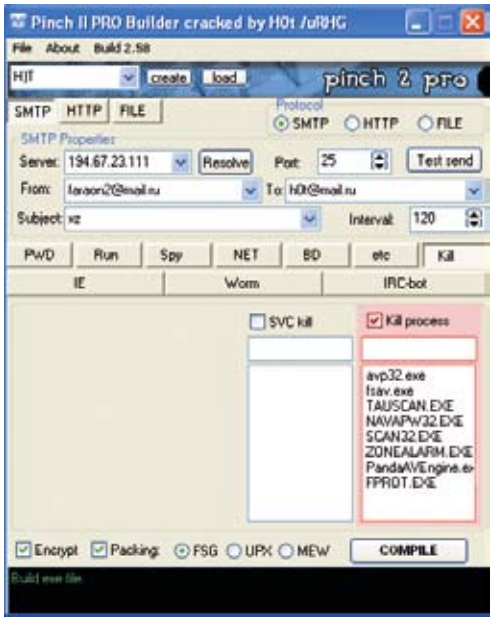
A vírusirtó nem jelzett a nagy telepítőcsomagokra, a telepítés viszont az USB-eszközök fizikai megléte nélkül nem hajtható végre. Kis nyomozgatás után aztán a BioSecure\fg.exe állományra terelődött a gyanúnk, amely része mindkét telepítőcsomagnak. A ProcessMonitorral kísért próbafuttatás során látszik, 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

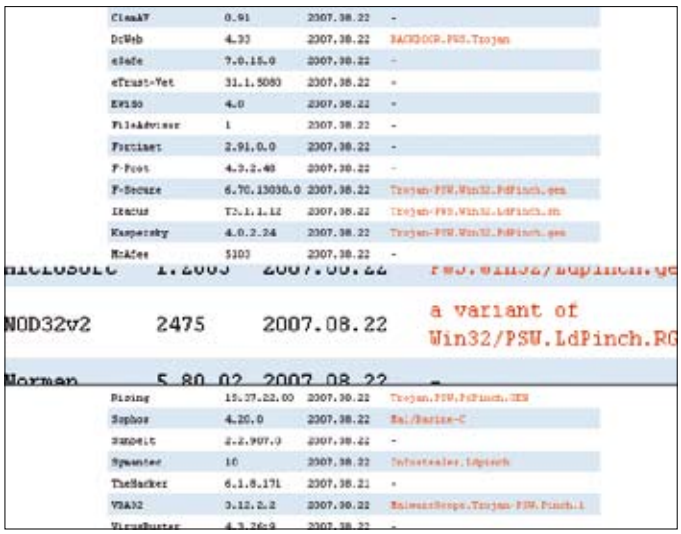
A Pinch Kill menüjében tetszés szerinti folyamat (process), például az ismert víruskeresők ellen is indítható kikapcsolási kísérlet



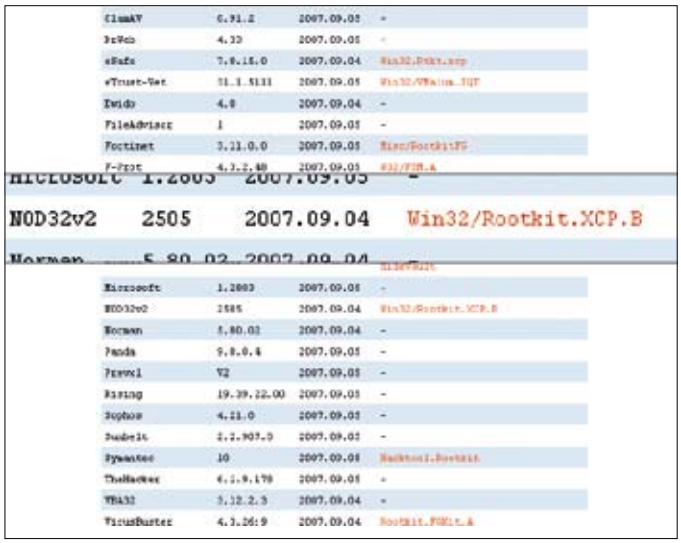
Ez az XCP nevű rootkites védelem hálózati forgalmat kezdeményezett a Sony szerverei felé, és jelentette, kik, mikor és milyen IP-címmel rendelkező számítógépen játszották le az adott zenei CD-t. Ez ijesztő módon azt mutatja, hogy a cég Nagy Testvérként figyelemmel kísérhette a felhasználók szokásait. 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 ezért tapasztalatlan felhasználóknak megfelelő segédeszköz nélkül semmiképpen nem javasolt. Egy szakszerűtlen próbálkozás indíthatatlan Windowst eredményez.

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 gépek-



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 férték 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 még is 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