# A rootkitekről – érthetően

CSIZMAZIA ISTVÁN

## Mik is azok a rootkitek?

A rootkiteket eredetileg a Unix/Linux operációs rendszerekre készítették, és céljuk a legmagasabb – az úgynevezett root, vagyis rendszergazda – jogosultság megszerzése volt, ezzel ugyanis át lehet venni az adott számítógép feletti irányítást. A Windowst futtató gépek esetén más a helyzet: itt elsősorban programok, futó folyamatok (process) vagy registry bejegyzések álcázása, biztonsági alkalmazások előli elrejtése a cél. A jogosultságnak ez esetben nincs kiemelt szerepe, hiszen szinte minden felhasználó adminisztrátori, vagyis a létező legmagasabb privilégiumokkal szerepel.

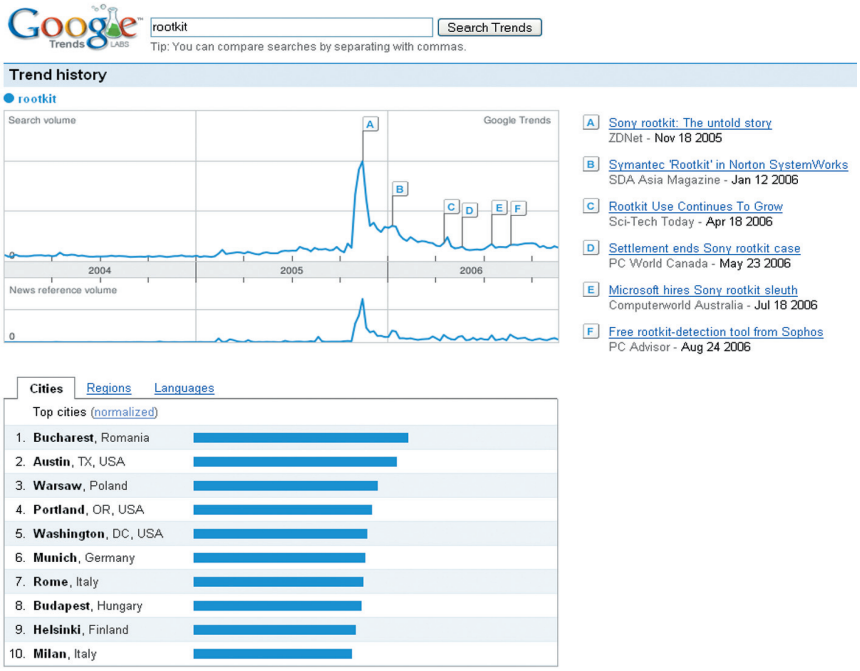
## Veszélyes dolog a rootkit?

A definíció szerint olyan programokról van szó, amelyek képesek elrejteni önmaguk vagy más szoftverek jelenlétét. Önmagában a rootkit-technológia nem jelent veszélyt: hasonlatosan például az atommaghasadáshoz, amit lehet jó céllal atomerőművekben energiatermeléshez használni, de rossz szándékkal nukleáris bombákat is előállíthatunk a segítségével.

A nagy gondot az jelenti, ha ezt a technikát különböző számítógépes kártevők, vírusok, férgek, kémprogramok elrejtésére 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 – vagyis abba a függvénykészletébe, amelyet 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 annak a neve a manipuláció révén hiányozni fog a listából. Ugyanez történhet adott registry- (rendszerleíró adatbázis) bejegyzés ellenőrzésekor is. Minden parancsforgalom az ellenőrzése alá kerül, szakmai szlenggel élve „meghookolja” a felhasználói függvényeket. A rootkitet távolról vezérlő hacker bármilyen más állományt is elrejthet ily módon, többek között a megtámadott gépre távolról feltöltött illegális – akár terrorista, pornó-, warez-anyagokat is.



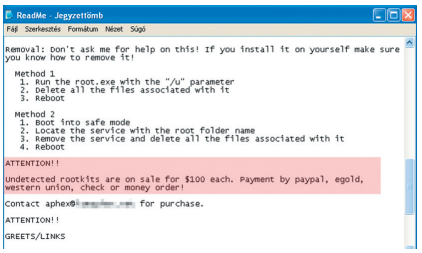

**1. ábra. Világosan látszik a Google „rootkit” szóval kapcsolatos találatain, hogyan emelkedett fel hirtelen az érdeklődés a SONY BMG-eset kapcsán.**

## A rootkit céljai

Egy rootkit fő célja nem szükségképpen az, hogy uralja a kiszolgálórendszert, még ha be is tör oda, és tartalmaz is olyan programokat, amik által megszerezhető a rendszergazda-hozzáférés. Sokkal inkább az a fő célkitűzése, hogy lehetővé tegye a behatoló számára, hogy tényked és a sebezhetőséget elleplezze.

## A rootkitek és a számítógépes kártevők kapcsolata

Bár a rootkitek csak néhány éve kerültek az érdeklődés középpontjába, valószínűleg a hackerek már korábban is használták őket, csak nem mindig vettük észre. Greg Hoglund, független biztonsági szakértő egyenesen úgy véli, hogy a Windows-alapú rootkitalkalmazások titokban ugyan, de már évek óta széles körben terjednek. Hoglund már 1999-ben figyelmeztetett a probléma veszélyességére, sőt demonstrációs céllal több rootkitet is írt – például a sokak számára ismert Hacker Defendert. Nehezíti a küzdelmet, hogy a rootkitek




**2. ábra. A fejlesztő teljesen nyíltan hirdet az AFX nevű csomag Read.me állományban, száz amerikai dollár fejében „észlelhetetlen” rootkiteket kínál eladásra, amit Pay-pal, E-Gold Western Union-átutalással, csekken vagy akár készpénzben is fizethetünk.**

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.

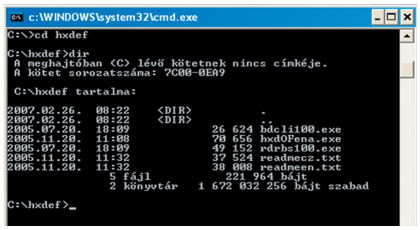
## A rootkit detektálása

A speciális, külön programként forgalmazott rootkitfelismerő programok a különféle rendszereltérítéseket (hooks) képesek észlelni. Az egyik legeredményesebb klasszikus rootkitleleplező módszer a számítógép pillanatnyi állapotának (futó folyamatok, automatikus indításra jogosult alkalmazások listája, registrybejegyzések, memóriafoglaltság stb.) mentését összehasonlítani egy garantáltan tiszta (pl. CD, DVD) lemezről történő indulás utáni hasonló mintával. Ha ebben a két

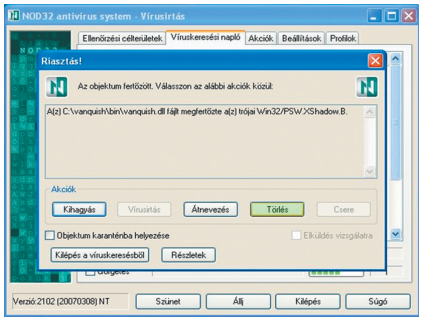
lementett állapotban eltérést látunk a futó folyamatokban, a felhasznált memória-területben, vagy bármilyen egyéb különbözőségre fény derül, az alapos további nyomozásra adhat okot.

## Védelem ideális ESET-ben

A hagyományos vírusok esetén általában megoldást jelent egy víruskeresés lefuttatása. A rootkitek azonban képesek arra, hogy aktiválásuk után láthatatlanná tegyék magukat. Így, miután a frissített antivírus-rendszer sem talál semmilyen fertőzést, a felhasználó – tévesen – biztonságban érezheti magát. Mindezek alapján a rootkitek el-




**3. ábra. A Hacker Defender tökéletesen képes álcázni magát, az adott könyvtár és a benne levő állományok láthatatlanok lesznek a Windows számára. A trükközés ellenére – ha pontosan tudjuk melyik az elrejtett könyvtár, a CD vagyis Change Directory paranccsal mégis bele tudunk lépni, igaz a rejtett fájlok ez esetben sem látszanak.**




**4. ábra. A NOD32 anitivírus alkalmazás bekapcsolt Anti-Stealth opció mellett a korábban rejtve maradt, operációs rendszert becsapó aktív, futó rootkitkomponenseket is képes észlelni és törölni.**

leni védekezés legfontosabb követelménye, hogy a fertőzést még annak aktivizálódása előtt ismerje fel és állítsa meg a számítógépre telepített antivírus-rendszer. Azonban a mai vírusvédelmi programok nem mindegyike képes erre.

Egy érdekes kivételt jelent az ESET Software vírusirtója, ami a megújult heurisztikus technológiának köszönhetően már a rootkiteket is proaktívan ismeri fel, megakadályozva azok aktiválódását. A NOD32 2.7-es változata már olyan fejlett rejtőzködésellenes technológiákat is kínál, amelyek átfogó védelmet nyújtanak a rootkitek ellen azáltal, hogy képesek a valós helyzetnek megfelelő információkat nyújtani a futó folyamatokról és a fájlrendszer állapotáról. (*I.)

A ThreatSense technológia a már aktivizálódott, feltelepült rootkitek ellen is használható, ezt korábban csak igen nehézkesen lehetett megvalósítani (4. ábra).

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. (*II.)

A cikk szerzője vírusvédelmi szakértő, a Sicontact Kft., a NOD32 magyarországi képviseletének munkatársa.

Források:
*I. ESET – The Root of All Evil? – Rootkits Revealed, White paper
*II. ESET – Product Bulletin NOD32 v2.7

A témával kapcsolatos webhelyek:
www.nod32.hu
www.eset.eu
www.eset.com/threat-center/blog/
www.rootkit.com
www.invisiblethings.org
blogs.technet.com/markrussinovich/
www.blackhat.com/html/bh-usa-07/bh-usa-07-index.html
www.bluepillproject.org/