HÍRES VÍRUSOK, ÉRDEKES ESETEK

Panoptikum

CD1/DVD
A cikk képei megtalálhatók a lemezmellékleten

Sorozatunk tizenkettedik epizódjában az IBM PC víruskorszak jó húsz esztendejének termésében 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 biztonsági lyukakra épített

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 átírata között volt olyan változat is, amelyik a Novell NetWare bejelentkező jelszavát lopta el.

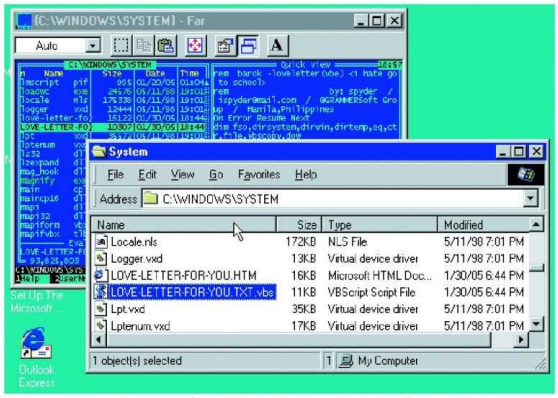
1990. február – Kavics kerül a gépezetbe

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 eset-

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

leg 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.

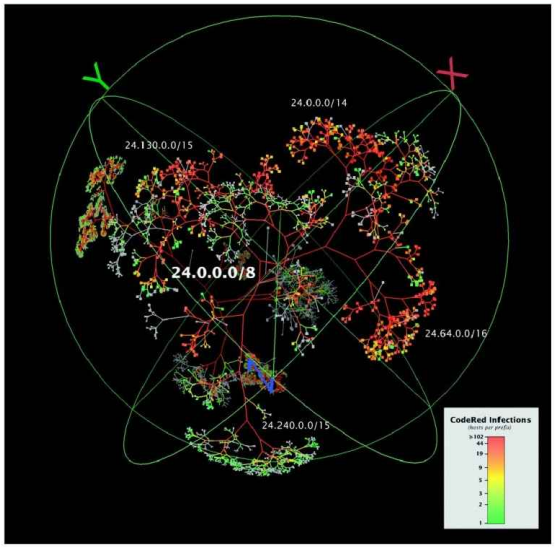
A vírus eredetileg ártalmatlannak készült, de egy programozási hiba folytán jelentős adatvesztéseket tudott okozni. Nevét a terjedésekor kiírt vicces üzenetről kapta: „Your computer is now stoned." A vírus kódban emellett egy, a marihuána



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

legalizálására vonatkozó üzenetet is lehetett találni.

1994. május – Váltságdíj az adatokért

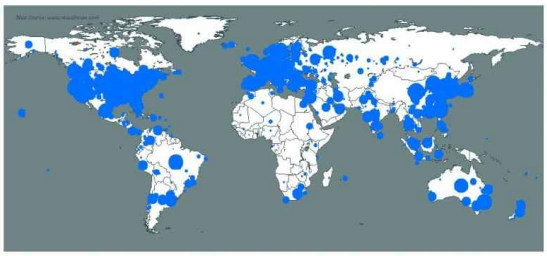
A OneHalf is új módszert honosított meg: merevlemezről történő bootolásonként 2-2 cilinder teljes tartalmát titkosította, a merevlemez végéről indulva. Ha csak simán mentesítettük a gépet, az elkódolt részhez soha többé nem fértünk hozzá. Szerencsére készült hozzá egy egyedi dekódoló segédprogram, amely a tényleges fizikai irtás 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 eseményláncot 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 Fülöp-szigeteken 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.

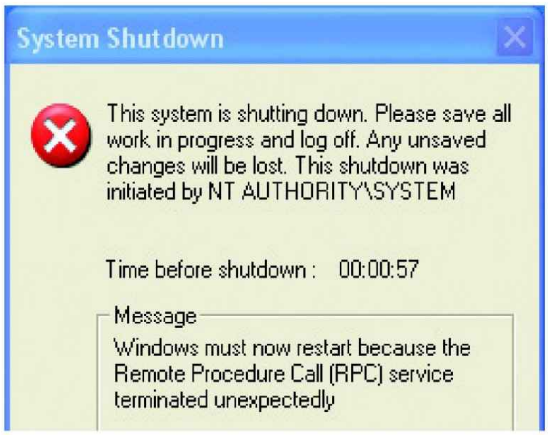
2001. szeptember – Egy gyors lefolyású támadás

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

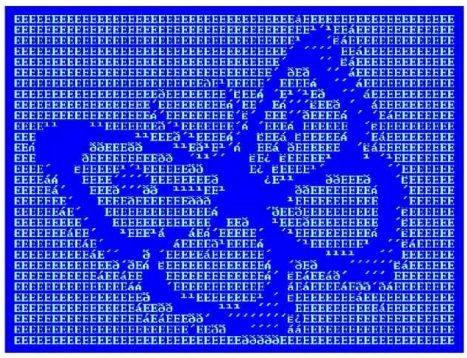
Nem, ezúttal nem a Rolling Stones Sticky Fingers című számáról lesz szó, hanem a lopkodós Klez vírusról. Ez a fertőzött gép merevlemezén található dokumentumokból véletlenszerűen kiválasztott egyet, és azt saját SMTP-motorja segítségével továbbküldte a vírussal együtt különböző címekre, így titkos vagy 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

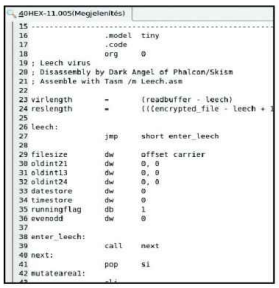
Akik korábban úgy könyvelték el, hogy csak futtatható állományokban vagy boot szektorban lehetnek vírusproblémák, nagyot csalódtak. A Microsoft SQL szervereket támadó Slammer (vagy más néven Zaphire) féreg a nem frissített rendszerekben található biztonsági rést használta ki. Támadása során az is nyilvánvalóvá 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



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 profithajhászás helyett inkább ki kellene javítani a szoftvereket – ma is aktuális.

2007. március – Animált kurzorok

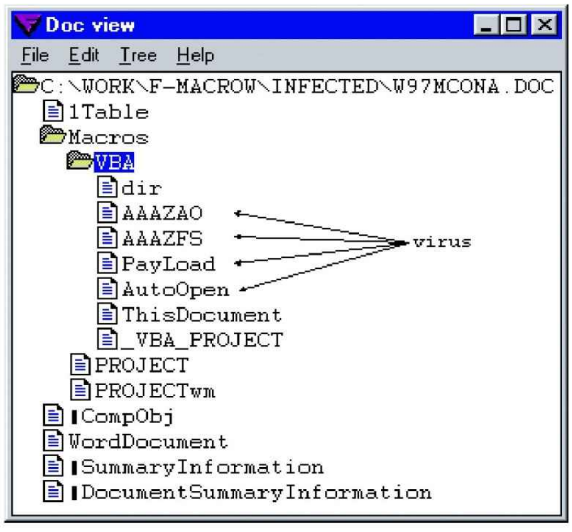
Több Windows-változaton túl vagyunk, jelenleg a szuperbiztonságosnak kikiáltott Vista a legújabb trónkövetelő. A Win32/TrojanDownloader.Ani.Gen trójai a Windows animált kurzorfájlok (.ani) kezelésével kapcsolatos, kritikus sebezhetőségét használja ki. A felfedezett hiba kihasználásával távoli kódfuttatás 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 millióit 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**