Ingyen véd

Ettől a számtól kezdve rendszeresen, minden hónapban szerepelni fog a CHIP CD-n és ingyenesen használható a Kaspersky Anti-Virus (KAV) Lite vírusellenes program teljes értékű változata.

CHIP – 2F Kft.

Gyártója, a Kaspersky Lab neve ismerősen csenghet a vírusvédelemben járatos szakemberek fülében. Víruskereső programjuk korábban AntiViral Toolkit Pro (AVP) néven vált ismertté, de víruskereső programmotorjuk évek óta része a finn F-Secure cég vírusvédelmi rendszerének is. Még a többi víruskereső programot gyártó céghez viszonyítva is rendkívüli az a gyorsaság, ámivel a megjelenő új vírusokra reagálnak – sokszor órák alatt megjelenik a frissítés és az új kártevő részletes elemzése. A feltérképezett új vírusok naprakész leírását a www.viruslist.com címen keresési lehetőséget is kináló angol nyelvű vírusenciklopédiában olvashatjuk.

A CHIP Edition a Kaspersky Anti-Virus különleges, a CHIP Magazin olvasói számára készített változata. A program használata ingyenes, képességeit nem korlátozták. A próbaverziók (egyszeri) 30 napra korlátozott érvényességével szemben a CHIP Edition használata hónapról hónapra meghosszabbítható az újságban megtalálható újabb kulccsal. A program ennek a kulcsnak az alapján állapítja meg érvényességét, ez biztosítja a legális felhasználók számára a működését. Megfelelő kulcs hiányában a program csak demóként tud működni: nem írtja, csak detektálja a vírusokat, és nem bővíthető a vírusismerete.

Hardverigénye nagyon szerény: Intel 80486 processzor, 8 Mbyte RAM, 15 Mbyte szabad lemezhely. Egyaránt működik Windows 95, 98, NT, 2000 és Me operációs rendszeren. A Kaspersky Anti-Virusnak vannak teljes, nem „Lite" változatai – ezek aktív, levelezőprogramhoz igazított e-mailszűréssel, hálózati képességekkel stb. is rendelkeznek.

A Scanner kereső

Telepítsünk!

A SETUP.EXE elindítása után válasszuk ki a telepítés nyelvét, ez jelenleg angol vagy orosz lehet, de a későbbiekben várható a magyar nyelvű megjelenés is. Ha a gépen már rajta van a program, automatikusan felajánlja az *Upgrade*, vagyis programfrissítés módot, különben *Clean Install*, azaz teljesen új telepítés történik. A telepítés folyamán a *SELECT KEYFILE* ablakban kell megadnunk (jóváhagynunk) a könyvtárban lévő kulcsot (sorszám.KEY).

Miből áll a program?

A program a háttérben folyamatosan futó víruskeresőből (Monitor) és távirányítóhoz hasonlító kezelőfelületből áll. A felületről az alábbi műveleteket indíthatjuk: a Monitor elindítása (ha még nem fut), a vírusadatbázist frissítő Updater indítása, víruskeresés a kiválasztott meghajtó(ko)n csak ellenőrzéssel (Detect) vagy az esetlegesen talált vírusok irtásával (Cure). A *Report* ablakot kinyitva a kézzel indított víruskeresés naplózását kísérhetjük figyelemmel, míg a *Help* ablakban a program működési útmutatóját olvashatjuk angol nyelven.

Az Updater modul felel a szoftver naprakészségéért. Szinte nem múlik el nap, hogy valamilyen új vírus vagy vírusváltozat ne jelenne meg. Fontos, hogy rendszeresen, lehetőleg naponta frissítsünk – ebben a változatban ez nem automatikus. Jó hír, hogy a KAV adatbázisának szerkezete additív frissítést tesz lehetővé, ezért a letöltés kevés időt igényel. A program arra is képes, hogy a betárcsázós Internet-kapcsolatú gépen kezdeményezze a netes kapcsolatot, és az is beállítható, hogy a frissítés végeztével automatikusan lekapcsolódjon a Hálóról.

A Monitor működését ikon jelzi a tálcán. A bekapcsolt Monitor röptében ellenőrzi a megnyitott file-okat, és ha vírust talál, előugró ablakban rákérdez, hogy eltávolítsa-e. A Monitort érdemes folyamatosan futtatni, így minden mozgatott, megnyitott file-unk azonnali vírusellenőrzésen esik át.

A Scanner, azaz a „távirányító" valójában kézi indítású víruskereső. A kiválasztott helyi vagy hálózati meghajtót, meghajtókat tudjuk vele ellenőrizni. Kétféleképpen indítható. Ha a *DETECT* gombra kattintunk (előtte legalább egy meghajtót ki kell választani), akkor a program csak keresi a vírusokat, de nem próbálja meg irtani. Ha talál, felbukkanó ablakban rákérdez, letörölje-e a fertőzött file-t. Ezt tetszés szerint elfogadhatjuk vagy elutasíthatjuk. A *CURE* gombot megnyomva a kereső által ismert vírusokkal megfertőzött file-okból eltávolítja a vírust. Ha a program nem tudja eltávolítani (sok vírust nem is lehet, mert például felülírnak egyes részleteket a megfertőzött file-okban), úgy a törlésre tesz javaslatot.

Kulcs és támogatás

A CD-mellékletünkön levő kulcs a telepítéstől számított 60 napig, de legfeljebb az év végéig érvényes. A kulcs érvényességét, vagy annak meghosszabbodását a Kaspersky embléma felett lévő kis háromszögre kattintva tudjuk ellenőrizni. Az újabb CHIP Magazin megérkezésekor mindössze az új kulcsot kell bemásolni a megfelelő helyre. Ennek menetét és a KAV adatbázisának magyar elérését CD-nken írjuk le.

Technikai támogatás is igénybe vehető a programmal kapcsolatosan. Ezt a vírusvédelemről és a tűzfalas megoldásairól ismert 2F Kft., az F-Secure és a Kaspersky Anti-Virus magyarországi képviselete adja. A technikai támogatás elsősorban e-mailben, másodsorban emelt díjas telefonszámon vehető igénybe.

E-mail: support@2f.hu
Telefon: 06-90-290-014 (150 Ft/perc)

Célkeresztben a Microsoft

Számos alkalommal fordul elő, hogy a vírusírók ismert cégek nevében írt levélben terjesztenek vírust, kihasználva a gyanútlan felhasználók hiszékenységét.

Csizmazia István (2F 2000 Kft.)

A vírusos levelek lehetnek egyszerű tájékoztató jellegűek, de figyelmeztethetnek vírus terjedésére is. Az alábbiakban mindegyikre mutatunk példát.

HardHead/VBS /Hard.A@MM

E vírusfigyelmeztetésnek álcázott féreg terjedésekor az Outlook Express címjegyzékéből vett összes névre elküldi magát. A levél angol nyelvű szövege arra hívja fel a figyelmet, hogy nagyon gyorsan terjedő, veszélyes féreg tűnt fel a Hálón, a Symantec észlelte először, 2001. április 4-én, valamint hogy a mellékelt file-ban található a féreg leírása. A levél végén „F. Jones, a Symantec vezető fejlesztője" aláírás szerepel. A mellékelt file neve: www.symantec.com.vbs.

A Hard.A büntetőrutint is tartalmaz, ez november 24-én aktivizálódik. Ekkor a féreg üzenetablakot jelenít meg az alábbi címmel és szöveggel: „Some shocking news. Don't look surprised! It is only a warning about your stupidity. Take care!" (Magyarul: „Megdöbbentő hír: ne légy meglepve! Most a hülyeségedre figyelmeztetünk. Vigyázz!")

I-Worm.Unis

A vírusírók a víruskeresőket fejlesztő cégeket is igyekeznek befeketíteni. Ha a Unis féreg levélmellékletként érkező EXE file-ját lefuttatjuk, először elindít egy rejtett alkalmazást rendszerszervizként, bemásolja magát a Windows System könyvtárába MSVBVM60.EXE néven (nem keverendő össze a Visual Basic MSVBVM60.DLL DLL-jével), és bejegyzi magát a Windows regisztrációs adatbázisába, a SOFTWARE\Microsoft\Windows\CurrentVersion\Run címen. A levél megfogalmazói a hitelesség látszatát erősítendő több cégre is hivatkoznak. Feladóként Microsoft Support van feltüntetve, és a másolatot kapók sorában egy állítólagos Symantec-munkatárs szerepel. Ez a levél is egy féreg feltűnésére figyelmeztet, amelyet az F-Secure, a Symantec és a Microsoft fedezett fel. Megadja a féreg nevét is (I-Worm.Universe), valamint hogy szerzője a Benny becenevű jól ismert európai hacker a 29A nevű vírusíró csoportból. A levél szerint számítógéprendszereket tett tönkre az FBI-nál és a Microsoftnál. A levél végén van a lényeg: a címzett ellenőrizze a rendszerét a levélhez csatolt víruskereső programmal, és az eredményt küldje el a universe@microsoft.com vagy a universe@-fsecure.com címre.

Az ilyen tartalmú levélre érdemes odafigyelni, mert a benne rejlő program akár a merevlemezt is formázhatja.

2001. szeptemberi vírusstatisztika. Írásunk készítésekor az októberi még nem állt rendelkezésre

I-Worm.Redesi

A Microsoft termékeihez kapcsolódó biztonsági javítófile-nak álcázza magát az e-mailben terjedő Redesi. Eddig két változatát fedezték fel. A Redesi.a egy listából választja ki véletlenszerűen az üzenet tárgyát (lásd a keretes cikkrészt). A levél feladójaként a Microsoft Support Desk van feltüntetve. Az üzenet szövege azt állítja, hogy a levélhez tartozó melléklet biztonsági patch, amelyet a Microsoft küldött. Valójában ott maga a vírus vár arra, hogy elindítsuk. Első indításakor üzenetet jelenít meg, amelynek címe „Microsoft Windows Update", az üzenet szövege pedig „Your Windows Update has been successful". A féreg másik variánsa a Redesi.b. Az ezt tartalmazó e-mail tárgya egy másik listából választódik ki véletlenszerűen. A melléklet elindítása után pedig a „%file path%\%filename% is not a valid Win32 application" cím alatt a következő üzenetet jeleníti meg: „%file path%\%filename% is not a valid Win32 application".

A féreg mindkét változata az alábbiak közül választja ki a csatolt file nevét: Si.exe, ReDe.exe, Disk.exe, Common.exe, UserConf.exe. Ha lefuttatjuk a mellékletet, a féreg először bemásolja magát a C: meghajtóra a fenti nevek mindegyikén, majd elküldi magát a Microsoft Outlook címjegyzékében található összes címre. Ha a gépen nincs telepítve a Microsoft Outlook, a féreg nem tud terjedni. Ha a Windows rövid dátuma „dd/mm/yy" vagy „mm/dd/yy" alakú, a Redesi 2001. november 11-én aktiválta a büntető eljárását: az AUTOEXEC.BAT file-ban olyan parancsokat helyezett el, amelyek hatására a gép következő indításakor megformázza a C: partíciót.

A Redesi.a-t hordozó e-mail tárgya

FW: Microsoft security update.
FW: Security Update by Microsoft.
FW: IT departments on state of HIGH ALERT.
FW: Important news from Microsoft.
FW: Stop terrorists computer viruses reign.
FW: Terrorists release computer virus.
FW: Emergency response from Microsoft Corp.
FW: Terrorist Emergency. Latest virus can wipe disk in minutes.
FW: Microsoft Update. Final Release Candidate.
FW: New computer virus.

www.2f.hu

Outlook előnyben!

A sokféle víruskereső között a Kaspersky Anti-Virus három változata, a Personal, a Personal Pro és a Windows Workstation igazi érdekességgel szolgál. Az Outlook Express adatbázisaiban közvetlenül megtisztítják a fertőzött leveleinket. Ezt a szolgáltatást csak a Kaspersky Lab víruskeresői nyújtják.

Csizmazia István

Először is érdemes tisztázni, hogy az Outlook Express és a Microsoft Outlook nem ugyanaz a termék, csak a nevük hasonló – a Microsoft Outlook a külön megvásárolható Microsoft Office csomag része, míg az Outlook Express a Windows 98 óta az operációs rendszerrel adott „ingyenes" levelezőprogram.

Közvetlen vírusirtás

Ha levelezésünk nem egy saját, bejövő és kimenő leveleket vírus ellen szűrő rendszeren megy keresztül, jó eséllyel kaphatunk vírusos leveleket. Ha a háttérben fut a gépen víruskereső program, az értesít minket a fertőzött levél megnyitásakor, de a levél fertőzötten az adatbázisban marad, és kitörléséig magában hordozza a vírust. A levelet melléklete nélkül ugyan elküldhetjük magunknak, hogy legalább a levél szöveges része megmaradjon, de a mellékklettel nem tudunk mit kezdeni. Az Outlook Express adatbázisainak vírusirtása mostantól megkímél bennünket ettől. Ha a levél melléklete fertőzött volt, például makrovírusos Word dokumentum volt benne, a Kaspersky Anti-Virus kiirtja a vírust. Ha pedig a melléklet netes férget tartalmaz, például I-Worm.Hybris-t, akkor a mellékletben levő file amúgy sem tartalmaz hasznos információt, ezért a víruskereső törölni fogja: az eredeti levél szövege és maga a levél megmarad, csak a melléklete tűnik el. Mitől újszerű ez a lehetőség? A tömörített file-okban – és a mi esetünkben a levelezőprog-ram adatfile-jai ennek számítanak – a vírusellenes programokkal alapesetben kizárólag keresni tudjuk a vírusokat, irtani eddig nem tudtuk őket. A Kaspersky említett programjaiban azonban helyet kapott ez az új opció, amelynek kihasználásához 5.0-s vagy újabb Outlook Express kell.

Az irtás menete

Az irtás idejére kapcsoljuk ki az Anti-Virusban a *Monitor* modult, vagy a *Monitor* beállításainál kapcsoljuk ki az e-mail üzenetek ellenőrzését. A *Scanner* modulban válasszuk a keresés helyének a *Sajátgépet*, és jelöljük ki a *Scan MS Outlook Express databases* opciót. A sikeres irtás előtt mindenképpen tömörítenünk kell a levelezőmappákat az Outlook Express *Összes mappa tömörítése* (Compress all folders) parancsával. Természetesen az ellenőrzés és irtás után vissza kell majd kapcsolni a *Monitor*t.

Aktuális kártevők

Két féregre hívjuk fel kedves olvasóink fegyelmét: az I-Worm.Alizra és az I-Worm.Badtrans II-re. Mindkét féreg a net segítségével terjed fertőzött e-mailek mellékletében. Kódjuk tömörített, Win32 platformra írt PE formátumú EXE file. Olyan fertőzött e-mail üzenetben érkezhetnek, amelynek *Subject* mezőjében különböző, véletlenszerűen kiválasztott szövegeket találunk. A férgek automatikus lefuttatásukhoz az IFRAM biztonsági rést használják ki (ez hasonló ahhoz, amit a Nimda féreg is használt). Így a kórokozók már akkor aktiválódnak, ha csak olvassuk vagy az előnézeti ablakban megjelenítjük a fertőzött üzenetet. (Hasonlóan működött a KAK.worm féreg, amely szintén a fertőzött melléklet megnyitása nélkül tudott aktiválódni).

Sor.	Százalék	Vírusnév
1.	44.9	I-Worm.Sircam
2.	14.5	I-Worm.Hybris(Family)
3.	8.2	I-Worm.Aliez
4.	3.8	I-Worm.Magistr.a
5.	3.5	I-Worm.HappyTime
6.	3.2	JS.Trojan.Seeker.based
7.	2.5	Macro.Word97.Thus(Family)
8.	2.4	I-Worm.Magistr.b
9.	1.7	Macro.Word97.Ethan
10.	1.1	Backdoor.Death
11.	1.1	Macro.Word97.Flop
12.	0.9	Macro.Word97.Misfles
13.	0.7	Win32.Parite
14.	0.7	I-Worm.Nimda.a
15.	0.7	I-Worm.Ninula.e
16.	0.6	JS.Trojan.Seeker(Family)
17.	0.5	I-Worm.Stator
18.	0.4	Backdoor.Hehet(Family)
19.	0.4	Stoned.AntiExe
20.	0.4	Backdoor.IRC.Cloner

2001. októberi vírusstatisztika a Kaspersky Lab adatai (www.viruslist.com) alapján

Forrás: Kaspersky Lab

Meglepő, hogy ezek a vírusok milyen komoly fertőzést tudtak okozni rövid idő alatt. Ennek oka nagy valószínűséggel az, hogy egyes felhasználók nem okulnak az eddigi problémákból, és a figyelmeztetések ellenére sem tartják be az alapvető számítógépes biztonsági elveket. Nyilvánvaló, hogy a legtöbb vírusfertőzésnek az az oka, hogy nem tanúsítanak kellő óvatosságot az e-mailekkel szemben, és nem telepítik a megfelelő javító patch-eket sem, amelyekkel befoltozhatók a biztonsági lyukak. A levelezés teljes védelméhez feltétlenül le kell futtatni a Microsoft megfelelő javítófile-jait. A védelem Outlook Expresshez és az Internet Explorerhez megtalálható a Microsoft webhelyén.

Végezetül következzen a 2001. október havi vírusstatisztika. A százalék oszlopban az adott vírus részesedése látható az adott hónap teljes vírusforgalmából. A Top 20 táblát e hónapban a Sircam vezeti, és az is jól látható, hogy döntő többségben vannak a netes férgek. 0A statisztika a Kaspersky Lab 2001. októberi adataiból készült (a novemberi még nem készült el cikkünk írásakor).

- A Microsoft javítófile-jai a „Patch Availability" bekezdés alatt találhatók: www.microsoft.com /technet/security/bulletin /MS01-027.asp)
- Javítások az Outlook Express és az Internet Explorer régebbi verzióihoz: www.microsoft.com /technet/security/bulletin /MS01-020.asp
- www.kaspersky.com
- www.viruslist.com
- www.2f.hu

Év végi kártevők

Egyre többször fordul elő, hogy az újabban megjelenő vírusok megpróbálják kikapcsolni és törölni a felhasználó gépén működő vírusvédelmi programokat.

Csizmazia István

Kezdetként következzen a 2001. november havi vírusstatisztika. A százalék oszlopban a tárgyhóban való előfordulás látható. A Top-20 táblát e hónapban az I-Worm.Badtransll vezeti. A statisztika a Kaspersky Lab 2001. november havi adataiból készült. További információ a weben található (➡ www.kaspersky.com és www.viruslist.com). Az aktuális vírusokra figyelmeztető friss hírek a www.2f.hu címen is olvashatók.

Sor.	Százalék	Vírusnév
1.	29.4	I-Worm.Badtransll
2.	6.1	I-Worm.Aliz
3.	2.7	Trojan.PSW.Gip
4.	1.8	I-Worm.Magistr
5.	1.7	I-Worm.Sircam
6.	1.5	I-Worm.Hybris
7.	0.7	I-Worm.Klez
8.	0.4	I-Worm.Nimda
9.	0.2	BackFormat.2000
10.	0.1	Rabbit.504
11.	0.1	Ply.3360
12.	0.1	Rape.2887
13.	0.1	VCS
14.	0.1	I-Worm.Stator
15.	0.1	MtE.Instuff
16.	0.2	Flat.1000
17.	0.1	Voronezh_Family
18.	0.1	Macro.Word97.Botk
19.	0.1	IIS-Worm.CodeRed
20.	0.1	I-Worm.MTX

2001. novemberi vírusstatisztika (Forrás: Kaspersky Lab)

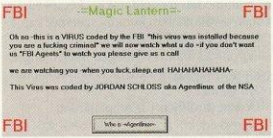
Trojan.Win32.Malantern

E vírus több névváltozattal is megjelenik: lehet Trojan.Win32.Malantarn, Magic Lantern vagy DanschI.A is.

A Trojan.Win32.Malantern butácska, Visual Basic nyelven írt, körülbelül 24 Kbyte hosszú Win32-es trójai program. Nyilvánvaló, hogy semmi köze sincs az FBI-hoz, nagy valószínűséggel egy fiatal vírusíró alkotása. Olyan levélbe rejti magát, amely a mellékletet egy Internet Explorerhez való javítófile-nak tünteti fel (IEpatch.EXE Win32 executable file).

Elindulása után törli a C:\WINDOWS\TEMP könyvtárat, majd új könyvtárakat hoz létre a Windows könyvtárán belül Magic Lantern, FBI software, John ASScroft, Bill Gatez, Desktop\666, Desktop\Bin Laden, Desktop\666 WTC, Desktop\Magic Fuckers, Desktop\Agentlinux, Desktop\iFuckedYourWife és Desktop\Biohazard Virii névvel. Ezek után kitörli az összes .SYS névkiterjesztésű file-t a C:\WINDOWS\SYSTEM32\DRIVERS\ könyvtárból, majd az alábbi üzenetet jeleníti meg egy kép kíséretében:

Thank you for using Microsoft.



I-Worm.Gokar

Szintén több névváltozata van: W32/Gokar@mm és Karen. A kórokozó egyfajta ötvözete az e-mail, az IRC és az IIS webférgeknek.

Először 2001. december 13-án észlelték. A férget Visual Basic nyelven írták, és az UPX programmal tömörítették. A Gokar a Microsoft Outlook segítségével küldi tovább magát. A levél tárgyát – akárcsak a levél szövegét és a csatolt file lehetséges nevét – meglehetősen hosszú listából választja ki véletlenszerűen.

A csatolt file-nak .PIF, .SCR, .COM, .EXE vagy .BAT névkiterjesztése lehet.

A fertőzést egyszerűen megállapíthatjuk, elárulja a KAREN.EXE file jelenléte a Windows könyvtárában. Ha a megfertőzött gép IIS webszerver, akkor a féreg módosítja a Microsoft IIS kezdőoldalát, hogy az felajánlja a WEB.EXE file-t letöltésre a weboldal minden látogatójának.

Az mIRC chatkliens beállításait is módosítja, hogy a továbbiakban az IRC-n keresztül is tudjon terjedni.

A féreg akkor fertőzi meg a gépet, amikor a felhasználó megnyit egy fertőzött levélmellékletet. Ekkor bemásolja magát a Windows könyvtárába KAREN.EXE néven, rejtett file-ként. Ezenkívül úgy módosítja a Registryt, hogy a KAREN.EXE a Windows minden indításakor lefusson. Ekkor megnyitja az Outlook címjegyzékét, és az abban szereplő összes címre elküldi magát e-mailben.

E fertőzött üzeneteknek különböző tárgya és szövege lehet. A szöveg végére azonban beírja a Windows bejegyzett felhasználójának a nevét (azt a nevet, amit a Windows telepítésekor kell megadni).

A csatolt file neve véletlenszerűen keletkezik a féreg belsejében tárolt minták alapján, névkiterjesztése pedig .PIF, .SCR, .EXE, .BAT vagy .COM lesz.

A féreg IRC-n keresztül is terjed. Lecseréli az mIRC csevegőkliens SCRIPT.INI file-ját a sajátjára.

Ez az új script engedélyezi a féreg számára a KAREN.EXE file elküldését minden IRC csatornabeli partnernek.

A féreg adott szöveget keres az IRC csatornán, és képes megváltoztatni a felhasználó becenevét (nickname) W32_Karen, W32Karen1, KarenWorm vagy KarenGobo névre, illetve be tudja léptetni a #teamvirus csatornára.

A féreg weboldalakon keresztül is terjed. Megvizsgálja, hogy a fertőzött gépen van-e telepített IIS webszerver, és ha igen, akkor a féreg bemásolja magát WEB.EXE néven a főkönyvtárba.

Ezenkívül átnevezi a DEFAULT.HTM file-t REDESI.HTM-re (a Redesi egy másik vírus neve), és elkészít egy saját DEFAULT.HTM oldalt. Ha a weboldalra látogató megnyitja ezt az oldalt, akkor az megkérdi, letöltse-e a WEB.EXE file-t. Ha ekkor a felhasználó elfogadja a „Run this file from current location" opciót, a féreg azonnal letöltődik, és aktiválódik az illető gépén.

A féreg a futó processzek között különböző vírusellenes és más biztonsági programok folyamatait is megpróbálja megkeresni és leállítani (lásd a keretes cikkrészt).

Az F-Secure Anti-Virus és Kaspersky Anti-Virus 2001. december 13-i vírusadatbázisa már felismeri a Gokart.

A Gokar és az általa keresett vírusellenes programok

Processz	Melyik vírusellenes termék része?
avpm.exe	Kaspersky
Claw95.exe	Norman
f-stopw.exe	F-Prot
ICLOAD95.EXE	Sophos
ICMON.EXE	Sophos
IOMon98.exe	Trend
NAVAPW32.EXE	Norton
VetTray.exe	CA
VSHWIN32.EXE	McAfee
_avpm.exe	Kaspersky

Szép új világ...

Lassacskán hozzászokhatunk a vírusok jelenlétéhez. Eleinte a programokat fertőző file-vírusok, majd az Office dokumentumok makrokártevői voltak többségben – mára az e-mailben terjedő férgek váltak a leggyakoribb hívatlan látogatókká.

Csizmazia István

Ma már klasszikusnak számító technikák mellett kevésbé gyakori, de legalább annyira veszélyes kártevők is terjednek. Az alább bemutatásra kerülő kellemetlen újdonságaink is ilyenek – az egyik a Napstert felváltó file-csereberélőkben terjedő trójai, a másik pedig ma még kuriózum: az első Shockware vírus.

Trojan.Win32.DIder

Névváltozatai: DIder, Troj_DIDer. Ezt a két alkotóelemből álló kémkedő trójai programot 2001. december végén fedezték fel. A program a felhasználó magánszféráját megsértve, futtatható programok letöltésével és indításával biztonsági rést nyit a rendszerben. E kémprogram a LimeWire és a Grokster file-cserélő szoftverében, valamint a Fastrack Kazaa telepítőcsomagjaiban terjed, más spyware file-ok kíséretében. A DIder még akkor is telepítésre kerül, ha a felhasználó az eredeti programcsomag egyetlen elemét sem választja ki. A trójai – ha már feltelepült a felhasználó gépére – folyamatosan frissíti a főmodulját, amely a 2001-007.com című webhelyhez kapcsolódik, és jelentést készít a felhasználó adatairól: User ID, az általa használt webböngésző, a látogatott webhelyek listája és a Windows megnyitott ablakainak adatai. A program fő eleme egy Explorer.exe nevű file, amely a Windows\Explorer alkönyvtárba kerül (nem összekeverendő az eredeti Explorer.exe-vel). Ezt a komponenst folyamatosan frissíti a trójai program második része, a DIDer.exe – ez a Windows könyvtárában található.

Amikor a DIDer.exe elindul, letölti a fent említett Explorer.exe file-t egy weboldalról, és beteszi a \Windows\Explorer\ könyvtárba.

Sor.	Százalék	Vírusnév
1	87,4	I-Worm.Bladramill
2	2,5	Trojan.PSW.Gip
3	2,3	I-Worm.Hybris
4	1,4	I-Worm.Sircam
5	1,1	I-Worm.Magistr
6	0,9	I-Worm.Aliz
7	0,6	I-Worm.Nimda
8	0,5	Trojan.PSW.Hooker
9	0,3	I-Worm.Goner
10	0,3	Macro.Word97.Thus
11	0,2	I-Worm.Petik
12	0,1	I-Worm.Zoher
13	0,1	Backdoor.Death
14	0,1	Macro.Word97.Furi
15	0,1	JS.Trojan.Seeker
16	0,1	Macro.Word97.Juta
17	0,1	I-Worm.HappyTime
18	0,1	Goutella-Worm.Mandragore
19	0,1	Macro.Word97.Verlor
20	0,1	Macro.Word97.Shere

2001. decemberi vírusstatisztika *(forrás: Kaspersky Lab)*

Ezután létrehoz egy start-up kulcsot a regisztrációs bejegyzések között. Ez a következő rendszerindításkor aktiválja az Explorer.exe-t, az létrehoz egy másik registry-bejegyzést a DIDer.exe indításához, és megpróbál kapcsolódni a már említett 2001-007.com helyre, hogy a begyűjtött adatokat oda továbbítsa.

A védekezéshez mindkét trójai komponenst törölni kell. Ha ezeket nem tudnánk törölni, mert zárolva vannak, akkor Windows 9x esetében DOS alól törölhetjük. Windows NT/2000/XP alatt átnevezhetjük őket, és az újraindítás után már törölhetők lesznek.

Az F-Secure és a Kaspersky Anti-Virus a 2002. január 3-án közzétett adatfile-okkal már felismeri a jelenlétét.

SWScript.LFM

Névváltozatai: SWF.LFM.926, Shockwave vírus, ACTS.LFM. Az SWScript.LFM olyan új vírus, amely a Macromedia Shockwave .SWF névkiterjesztésű file-jait fertőzi meg. A Macromedia Shockwave file-ok alaphelyzetben audio- és videoadatokat tartalmaznak. Egyszerűségük és tömörségük miatt nagy népszerűségnek örvendenek a netes oldalakon. Sok százezer felhasználó küldi virtuális üdvözlőlapjait .SWF file-ok formájában, és a vállalati webhelyeken is előszeretettel alkalmazzák ezt a formátumot, mert segítségével lendületes és látványos oldalak hozhatók létre.

A SWScript.LFM az első Shockwave file-okat fertőző vírus. Szerencsére egyáltalán nem fenyeget azzal, hogy egy fertőzött weboldalt meglátogatva átterjedjen a látogató gépére. A fertőzés egyetlen módja, ha kézzel letöltik a file-t, és azt olyan könyvtárba helyezik, ahol SWF névkiterjesztésű file-ok vannak, majd ezek után elindítják a Shockwave Player programot. Ekkor, és csak ekkor képes a fertőzésre.

A SWScript.LFM a Shockwave ActionScript nevű scriptjét használja fel a fertőzésre. Mialatt megfertőzi a többi file-t, a képernyőn a „Loading Flash Movie" (flash animáció betöltése) felirat látszik. E vírus széles körű terjedését még nem észlelték, és ez nem is látszik valószínűnek. Ennek ellenére érdemes lesz figyelni rá, mert új frontot nyitott a megfertőzhető file-ok terén, és egyáltalán nem zárható ki további, intelligensebben működő változat megjelenése.

Az F-Secure és a Kaspersky Anti-Virus a 2002. január 8-án megjelent adatbázisukkal már felismerik a jelenlétét.

Decemberi kártevők

Végül következzen a 2001. decemberi vírusstatisztika!

A százalék oszlopban az előfordulás látható. A Top 20 táblát e hónapban is az I-Worm.BadtransII vezette, mégpedig kiugróan magas értékkel.

A statisztika a Kaspersky Lab 2001. decemberi adataiból készült.

www.2f.hu
www.kaspersky.com
www.viruslist.com

A vírusellenes programok tesztje

A vírusellenes programok legrangosabb és legfontosabb megmérettetése a Virus Bulletin rendszeres tesztelése. Itt az összes magára valamit adó vírusvédelmi terméket fejlesztő cég igyekszik elindulni.

Csizmazia István (2F 2000 Kft.)

Amikor egy fejlesztőgárda meg akarja győzni a felhasználókat termékük kiválóságáról, az itt rendszeresen elért jó helyezés és persze a minél több begyűjtött „100% Award" trófea a legjobb ajánlólevél és bizonyíték.

A terméknek több operációs rendszeren kell bizonyítaniuk, hogy ők a legjobbak a mezőnyben.

A platformok között szerepel a DOS, a Windows 95, 98, NT, Me és 2000, de megtalálható itt a Novell NetWare is. Ezek közül mindig kiválasztanak egyet az aktuális megmérettetéshez. Az alábbi módon vizsgálják a különböző programok tulajdonságait.

A teszteket elsősorban valódi, az előző hónapban leggyakrabban előforduló vírusokkal végzik. E valós környezetben is előforduló (in the wild) vírusokon kívül szerepelnek olyan, csak laboratóriumi körülmények között előforduló vírusok is, amelyeket a tesztelés céljára hoztak létre (például több, különböző vírus által felülfertőzött file-ok).

A programoknak ezenkívül egy minden addigi vírust tartalmazó vírusgyűjteményen is bizonyítaniuk kell. E gyűjteményben mindenféle kártékony kód megtalálható: bootvírusok, file-vírusok, makrovírusok, polimorf (alakváltoztató) vírusok stb.

Minden vírusellenes terméket a telepítése utáni alapbeállításaival használnak (default settings). Ezek a beállítások rendelkeznek arról, milyen elemeket és milyen névkiterjesztésű file-okat vizsgáljon a védelem, és hogyan alkalmazza a heurisztikus keresést (a vírusszerű tulajdonságokat a konkrét vírus ismerete nélkül is felismerő elemzést).

Sor.	Százalék	Vírusnév
1.	65.6	I-Worm.Badtransfil
2.	11.2	I-Worm.Siecam
3.	4.1	I-Worm.Myparty
4.	4.1	I-Worm.Klez
5.	1.8	I-Worm.Hybris
6.	0.8	I-Worm.Magistr
7.	0.8	VCL
8.	0.4	I-Worm.Aliz
9.	0.3	Flip.2153
10.	0.2	Macro.Word97.Thus
11.	0.2	I-Worm.Nimda
12.	0.2	Trojan.PSW.Hooker
13.	0.2	Backdoor.Death
14.	0.2	JS.Trojan.Seeker
15.	0.2	I-Worm.Goner
16.	0.1	Macro.Word97.TheSecond
17.	0.1	I-Worm.Stator
18.	0.1	I-Worm.GOPworm
19.	0.1	Win32.FunLove
20.	0.1	Macro.Word97.VMPCK(Steroid)

2001. januári vírusstatisztika *(forrás: Kaspersky Lab)*

Az alapbeállítások ésszerű kompromisszumot képviselnek a gyors, illetve az eredményes védelem között. Valós idejű kereséskor csak az előre meghatározott névkiterjesztésű file-ok kerülnek vizsgálatra, mert ha minden file-t ellenőriznének a víruskereső programok, az még a legerősebb gépet is jócskán lelassítaná.

Ha egy program a vadon élő vírusok (in the wild, ITW) felderítésénél 100%-ot teljesít, az kiváló és fontos részeredmény, még akkor is, ha a végső összesítéskor csak kisebb pontszámot ér el.

A hatékony működést mind a valós idejű (on access scan, OAS), mind pedig a kézzel indított (on demand scan, ODS) keresésnél bizonyítani kell. A kézzel indított keresésnél elemzik a „csak jelentés" (report only) üzemmódban indított vírusdetektálás naplófile-ját.

Lehetséges hibák

A hálózati file-ok és CD-ROM-ok ellenőrzésekor előfordulhatnak olyan szórványos, telepítésből eredő hibák, amik befolyásolnák a teszt eredményeit, ezért mindig helyi gép merevlemezén levő tesztfile-okat vizsgálnak. Néhány terméknél az is előfordul, hogy a keletkezett naplófile használhatatlan a teszt szempontjából, vagy bizonyos file-méretet elérve összeomlik a víruskereső program. Ilyen esetekben az a kedvelt megoldás, hogy lefuttatnak egy keresést fertőzés esetére törlést választva, egy következőt karanténba helyezést választva, és egy harmadikat, amely ezek után elvileg már nem találhat(na) fertőzést. Ami vírust a program ebben az utolsó menetben jelez, azt úgy tekintik, mint kihagyott és elhibázott tételt.

A valós idejű védelem tesztjéhez olyan eszközt választanak, amely ismétlődően végigmegy az összes tesztfile-on, megnyitva azokat.

A vírusvédelmi programoknak meg kell akadályozniuk a fertőzött file-okhoz való

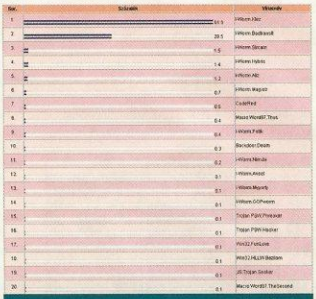
Fokozódó szigor

A számítástechnika rohamléptű fejlődése sajnos nemcsak a gyorsabb processzorok, nagyobb tárolókapacitású merevlemezek és a fejlettebb szoftverek létrejöttében, hanem az egyre ravaszabb és kártékonyabb vírusok megjelenésében is megmutatkozik.

Csizmazia István

Napjaink kártevői már nem elégednek meg a képernyőtartalom vagy a memória manipulálásával – ezek helyett a legnagyobb értéket, a gépeinken tárolt adatokat támadják meg. A hosszú hetek, hónapok munkájával létrehozott dokumentumok, hang-, video- és egyéb adatfile-ok válhatnak semmivé vagy értéktelen bithalmazzá egy-egy vírus aktivizálódásának hatására. A vírusvédelem mellőzése, a vírusadatbázis-frissítések kihagyása, vagy akár egy fertőzött levélmelléklet megnyitása komoly következményekkel járhat.

Az alábbiakban néhány aktuális vírus drasztikus hatású büntetőrutinjait mutatjuk be.



2002. februári vírusstatisztika *(forrás: Kaspersky Lab)*

I-Worm.Maldal

Névváltozatai: Keyluc, Zacker, CHRISTMAS.EXE, Reeezak. E féreg végigmegy minden helyi és hálózati meghajtón, és a DaLaL.htm tartalmát minden egyes .HTM, .HTML és .ASP névkiterjesztésű file-hoz hozzáfűzi.

Ezek után törli az alábbi kiterjesztésű file-okat: .DOC, .JPEG, .JPG, .LNK, .MDB, .MP3, .MPEG, .MPG, .PPS, .PPT, .RAM, .RM, .SWF, .TXT, .XLS és .ZIP. Ennek végeztével a vírus lemásolja magát a törölt file-ok nevén, de az eredeti névhez .VBS kiterjesztést fűz hozzá.

Végül a kezdeti fertőzés után 30 perccel öt másodpercenként megkísérli a létező összes file törlését, megjelenít egy üzenetablakot, majd leállítja a Windowst.

I-Worm.Gigger

Névváltozatai: Gigger, Gigger.A@mm, IRC/Gigger.A@mm, JS/Gigger.A@mm. E féreg végigmegy az összes helyi és megosztott hálózati meghajtón, hozzáfűzve a víruskódot minden .HTM, .HTML és .ASP névkiterjesztésű file-hoz.

Ha az adott könyvtár tartalmaz .INI vagy .HLP kiterjesztésű file-t, akkor script.ini néven másolja be magát. Ennek következtében, ha a felhasználó gépén telepítve van mIRC kliens, akkor a féreg felülírja az eredeti script.ini file-ját a vírus kódjával.

Ezek után a féreg elküldi magát minden olyan IRC csatornára, ahova a felhasználó be van jelentkezve.

Ha a pillanatnyi dátum napjának értéke 1, 5, 10, 15 vagy 20, akkor a féreg az összes elérhető meghajtón az összes hozzáférhető file-t lecseréli egy nulla byte hosszúságú file-ra, így azok elveszítik eredeti tartalmukat.

I-Worm.Klez.E

Névváltozatai: ElKern, Klaz, Kletz, I-Worm.Klez. A Klez vírus Magyarországon és világszerte is napjaink egyik leggyakoribb kártevője. A féreg minden páratlan hónap 6. napján az alábbi névkiterjesztésű file-okat semmisíti meg: .BAK, .C, .CPP, .DOC, .HTM, .HTML, .JPG, .MP3, .MPEG, .MPG, .PAS, .TXT, .WAB és .XLS.

Januárban és júliusban viszont a teljes merevlemez mindegyik file-ját véletlenszerű adatokkal írja felül. Ezek visszaállítása kizárólag mentésből lehetséges!

I-Worm.Alcaul

Névváltozatai: Alcarys, W32/Alcarys@mm, W32.Alcarys@mm, Alcaul. Ennek a féregnek is veszélyes a büntetőrutinja. Felülír minden .HTM és .HTML file-t a rendszeren az általa korábban létrehozott c:\dnserror1.html file tartalmával.

Ezenkívül az összes .COM, .SCR, .WAV és .MP3 file-t felülírja (kivétel a COMMAND.COM és a WIN.COM) saját magával. Az újonnan keletkezett .WAV és .MP3 file-okhoz .EXE kiterjesztést ad hozzá. Ezenfelül a féreg megkísérli felülírni az alábbi nevezetes, vírusvédelmi programokhoz tartozó file-okat: avpm.exe, _avpm.exe, avp32.exe, _avp32.exe, vshwin32.exe.

I-Worm.MyLife.b

Névváltozatai: I-Worm.Mylife, Caric, Cari. E féreg tulajdonképpen PE formátumú EXE file, Visual Basicben írták. Programkódja ténylegesen 32 Kbyte hosszúságú, de az UPX programmal összetömörítették, így a féreg mérete 11 Kbyte.

Terjedési részében a féreg összegyűjti az összes levelezési címet az Outlook könyvtáraiból és a Windows címjegyzékéből (Windows Address Book), és minden egyes címre elküldi magát. Ha már sikerült megfertőznie a rendszert (a fertőzött gép újraindult), ellenőrzi a pillanatnyi dátumot, és ha az órák száma egyenlő nyolccal, végrehajtja a büntető rutinját. Ez az alábbiakat törli: c:*.*, d:*.*, e:*.*, f:*.*. Ezenfelül törli a .SYS file-okat a Windows könyvtárából, és a .VXD, .SYS, .OCX, .NLS file-okat annak System alkönyvtárából, ezzel teljesen működésképtelenné téve a Windowst.

Az F-Secure és a Kaspersky Anti-Virus programjai naprakész adatfile-okkal mindegyik itt ismertetett vírus jelenlétét felismerik.

Februári adatok

Végül következzen a 2002. február havi vírusstatisztika. A százalék oszlopban a tárgyhóban észlelt előfordulás gyakorisága látható. A Top 20 táblában a vezető helyet e hónapban az I-Worm.Klez átvette a sokáig listavezető I-Worm.BadtransII előtt. A statisztika a Kaspersky Lab 2002. február havi adataiból készült. (↬ További információk: www.kaspersky.com és www.viruslist.com)

●

Az aktuális vírusokra figyelmeztető friss hírek olvashatóak cégünk webhelyén: www.2f.hu.

Régi új féreg a netről

A Klez nevű féreg új változata kezdett terjedni a neten. Az új mutáns, amely több néven ismert, több országban is észlelték, köztük Japánban, Kínában, Ausztriában, Csehországban és az Egyesült Államokban.

Csizmazia István

Az utóbbi hetekben már Magyarországon is tömegesen kapnak a felhasználók ilyen leveleket. A napi statisztikát megjelenítő weboldalon láthatjuk, hogy cikkünk írásakor (2002. április 26-án) a Klez.H vírus elképesztő értékkel vezeti a fertőzési listát.

Ez a féregvírus a net segítségével terjed, fertőzött e-mail üzenetek mellékleteként.

Érdekessége, hogy magát Klez.E elleni irtóprogramnak állítja be – valójában új vírusverziót tartalmaz.

A levél szövegében a furfangos vírusíró még azt is írja, hogy ne törődjünk vele, ha a víruskereső riaszt a mellékelt programra, ez így helyes.

Az I-Worm.Klez.h névváltozatai: I-Worm.Klez.H, W32/Klez.H, Klez.K (Messagelabs), Klez.G (Trend).

A fertőzött üzenet tárgysorában (Subject) a „Worm Klez.E immunity" szöveg olvasható. A levél szövege:

Klez.E is the most common world-wide spreading worm.It's very dangerous by corrupting your files.

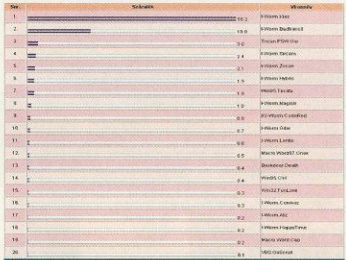
Because of its very smart stealth and anti-anti-virus technic, most common AV software can't detect or clean it.

We developed this free immunity tool to defeat the malicious virus. You only need to run this tool once,and then Klez will never come into your PC.

NOTE: Because this tool acts as a fake Klez to fool the real worm, some AV monitor maybe cry when you run it. If so, Ignore the warning,and select 'continue'. If you have any question,please mail to me.

Sor.	Előfordulás	Vírusnév
1.	(1547)	I-Worm.Klez.h (Klez Family)
2.	(750)	Win32.Elkern.c
3.	(634)	Exploit.IFrame.FileDownload
4.	(447)	JS.Trojan.Seeker
5.	(412)	I-Worm.Sircam
6.	(404)	Exploit.IFrame
7.	(350)	I-Worm.Nimda
8.	(340)	I-Worm.Hybris
9.	(328)	I-Worm.Magistr.B
10.	(241)	I-Worm.BadtransB
11.	(231)	I-Worm.Magistr
12.	(199)	April
13.	(190)	I-Worm.Badtrans
14.	(186)	Win32.FunLove (a.k.a. Fun Loving Criminals)
15.	(179)	Joke.Buttons
16.	(168)	Win95.CIH-Killer
17.	(161)	Trojan.PSW.OIP
18.	(146)	Riot Family
19.	(143)	I-Worm.MTX
20.	(141)	BigMouse Family

Április 26-án a vírusok elterjedési listáját a Klez.H vezeti



2002. márciusi vírusstatisztika *(forrás: Kaspersky Lab)*

A levél mellékletében a víruson kívül egy, a helyi gépen megtalálható file is szerepel, amelyet véletlenszerűen választ ki az alábbi névkiterjesztésű file-ok közül: TXT, HTM, HTML, WAB, ASP, DOC, RTF, XLS, JPG, CPP, C, PAS, MPG, MPEG, BAK, MP3 vagy PDF. Ez a módszer nagyon veszélyes (korábban a Sircam vírusnál tapasztalhattunk hasonlót), hiszen így személyes és bizalmas dokumentumaink kerülhetnek közkézre.

A féreg az IFRAME biztonsági rést használja ki, ugyanazt, amelyet a Nimda és az Aliz féreg is használt. Így már akkor is aktiválódik, ha csak olvassuk vagy az előnézeti ablakban megjelenítjük a fertőzött üzenetet (ehhez hasonló volt a KAK.worm, amely szintén a fertőzött melléklet megnyitása nélkül tudott aktivizálódni).

A féreg ezenkívül próbálja megkeresni az adott gépen az ismertebb víruskereső programokat, és kísérletet tesz azokat hatástalanítására. Az alább felsorolt folyamatokat a „TerminateProcess" utasítással kísérli meg leállítani: _AVP32, _AVPCC, _AVPM, ALERTSVC, AMON, AVP32, AVPCC, AVPM, N32SCANW, NAVAPSVC, NAVAPW32, NAVLU32, NAVRUNR, NAVW32, NAVWNT, NOD32, NPSSVC, NRESQ32, NSCHED32, NSCHEDNT, NSPLUGIN, SCAN, SMSS.

A Klez.H elleni védekezéshez először is azonnal frissíteni kell a vírusismereti adatbázist.

A fertőzés további megelőzéséhez érdemes lefuttatni a megfelelő javító patch-eket a Microsoft Outlook Express biztonsági lyukainak befoltozására (↷ letöltési helyük:www.microsoft .com/windows/ie/downloads/critical/Q319182/default.asp).

Mentesítéshez a Kaspersky Labs *CLRAV utility* nevű célprogramját ajánljuk (↷ www .2f.hu/files/utility /clrav.com).

Az F-Secure és a Kaspersky Anti-Virus a 2002. április 17. délutáni adatbázisfile-jaival már képes detektálni ezt az új változatot is.

Márciusi kártevők

Végezetül következzen a 2002. márciusi vírusstatisztika. A százalék oszlopban az előfordulás gyakorisága látható. A Top 20 táblában az I-Worm.Klez család átvette a vezetést a sokáig listavezető I Worm .BadtransII-től. A statisztika a Kaspersky Lab 2002. március havi adataiból készült. További információ a weben a www.kaspersky .com és a www.viruslist.com, valamint a www.2f.hu címen található.

Automatikus frissítés

A víruskereső programok forgalmazói nem győzik hangsúlyozni, hogy az eredményes használat egyik legfontosabb kritériuma, hogy a program vírusismerete naprakész legyen.

Csizmazia István

Felvetődik a kérdés: egy ilyen fontos műveletet nem lehetne-e teljesen „gépesíteni"? Az élvonalbeli víruskeresők általában törekszenek erre.

Az F-Secure víruskereső programban a kézi frissítésen felül egy minden igényt kielégítő megoldással találkozhatunk. A BackWeb nevű frissítőprogramot az egyedi felhasználók és a hálózatos környezetben üzemelő cégek is eredményesen használhatják. A frissítés az anyacég finnországi nagy teljesítményű BackWeb szerveréről történik a neten keresztül. A letöltést minimális adatforgalomra optimalizálták: csak a szükséges különbözetek töltődnek le. Ugyaninnen kérésre percrekész biztonsági híreket és információkat is kaphatunk. A programot egyszer, a telepítésekor kell jól beállítanunk, ezután ezzel a résszel többet nem lesz gondunk.

A Kaspersky Anti-Virus program (nem a Lite! változat) szintén igyekszik hatékonyan automatizálni a frissítést. Alapbeállításában naponta egyszer tölti le a neten keresztül a frissítést. A frissítés folyamata azonban részletesen beállítható. Indítható a frissítés kézzel, indulhat megadott esemény bekövetkeztekor (például a Monitor modul betöltődése után), vagy ütemezhető egy hónapra előre. Megadható, hogy a beírt HTTP, illetve FTP címeket a beírás sorrendjében használja (foglaltság esetén automatikusan a következő címen próbálkozik), vagy ezek közül véletlenszerűen válasszon. Beállítható az is, hogy a frissítéshez aktiválja a netkapcsolatot, majd a letöltés végeztével bontsa. A teljes folyamat eredménye naplózható, hogy később ellenőrizhessük, mikor és hogyan történtek a frissítések.

A BackWeb beállítási lehetőségei

A hálózatos környezetben működő Kaspersky Anti-Virus for Windows Workstation hálózati felügyeleti eszközével, az Admin Kittel képes Alert Routingra is. Ez a rendkívüli eseményekről szóló értesítéseket továbbítja az adminisztrátoroknak. A frissítés szemszögéből nézve ez azt jelenti, hogy nemcsak a futási problémákról és vírusfertőzésekről, hanem vírusismereti adatfile-ok frissítéséről is kaphat egy vagy több tetszőleges cím e-mailt. Ez a lehetőség az F-Secure felügyelőprogramjában, a Policy Manager Console-ban is megtalálható.

File-cserés támadás

Aktuális kártevőnk a Worm.Kazaa.Benjamin (névváltozatok: Benjamin, Kazaa worm). Terjedési sebessége még az előző hónapban – hazánkban is – rekordot döntő Klez vírusét is túlszárnyalta. E féreg a terjedéséhez a KaZaa file-átvitelét használja peer to peer (P2P) hálózaton. A KaZaa hálózata lehetővé teszi, hogy felhasználói file-okat vigyenek át egymáshoz a KaZaa klienst használva. A Benjamin nevű férget Borland Delphiben írták, mérete körülbelül 216 Kbyte, és az AsPack eszközzel tömörítették. Minden file végére szemetet ír az álcázás végett, így a file mérete nagyban változhat.

A féreg először egy hamis hibaüzenetet jelenít meg, majd bemásolja magát a Windows SYSTEM könyvtárába a következő néven: EXPLORER.SCR.

Sor.	Százalék	Vírusnév
1.	(94.5)	I-Worm.Klez
2.	(1.5)	I-Worm.Badtransfl
3.	(0.6)	Win32.Eikern.c
4.	(0.6)	I-Worm.Sircam
5.	(0.4)	I-Worm.HappyTime
6.	(0.3)	I-Worm.LoveLetter
7.	(0.2)	I-Worm.Hybris
8.	(0.2)	Win95.CIH
9.	(0.2)	I-Worm.Cervivec
10.	(0.1)	Trojan.PSW.Delf
11.	(0.1)	Trojan.PSW.Dip
12.	(0.1)	I-Worm.Magistr
13.	(0.1)	Macro.Word97.Thus
14.	(0.1)	I-Worm.Gibe
15.	(0.1)	I-Worm.Nimda
16.	(0.1)	I-Worm.Stator
17.	(0.1)	JS.Trojan.Seeker
18.	(0.1)	Backdoor.Death
19.	(0.1)	W3-Worm.CodeRed
20.	(0.1)	Backdoor.Osirdoor

2002. áprilisi vírusstatisztika *(forrás: Kaspersky Lab)*

Ez után létrehoz két kulcsot a registryben, majd a rendszer újraindítása után aktivizálódik.

Terjedése csak akkor valósulhat meg, ha a KaZaa P2P kliens telepítve van.

A program információk után kutat a registryben a KaZaa kliensről, és létrehozza a %WinDir%\Temp\Sys32 könyvtárat, amelyet hozzáférhetőnek regisztrál a KaZaa hálózat használói számára. Ezt a könyvtárat a program a saját másolataival tölti meg, amelyek nevét a féreg törzsében található listából választja. A terjedés a következőképpen zajlik.

Az „áldozat" egy file után kutat a KaZaa hálózaton, amit a már megfertőzött gép hozzáférhető file-jainak listáján talál meg. A felhasználó gyanútlanul letölti a keresett file-t, és megnyitja, így megfertőzi a saját gépét. A féreg mindezek mellett megnyitja a www.benjamin.de weboldalt, amelyen egy hirdetés látható.

Az F-Secure és a Kaspersky Anti-Virus a 2002. május 20-i adatbázisfile-jaival már képes detektálni ezt a férget. Aktuális vírusokra figyelmeztető friss híreket a neten, a www.2f.hu címen találhatnak olvasóink.

Netes feneegyedek

A számítástechnikában is igaznak tűnik: a kihasználható biztonsági hibákat valaki mindig ki is használja. E havi „kedvenceink" alkotói sem szenvedtek ötlethiányban.

Csizmazia István

A megszokottnak számító e-mailes férgek mellett felütötte fejét egy ritka jövevény, amitől az adatbázisszerverek üzemeltetőinek van okuk félni. Ez az új SQL vírus a SQLSpida (névváltozatai: Worm.SQLSpida, SQLsnake, Digispid). Az SQLSpida.A és B (DigiSpid.A/B) netes féreg a Microsoft SQL szervereit felhasználva terjed. A Code Red/Blue és a Nimda hagyományait folytatva a Microsoft kiszolgálóalkalmazásait fertőzi.

Terjedése során véletlenszerűen választott C osztályú hálózatokat néz át, és ha talál 1433-as TCP porton hallgató gépet, azt megpróbálja megfertőzni.

Csak akkor lehet sikeres, ha a megtámadott gép biztonsága nem megfelelő. A biztonság akkor hiányos, ha az SQL szerverhez kapcsolódó „SA" Windows-felhasználó jelszava üres, és maga az SQL kiszolgálóalkalmazás rendszergazdai privilégiumokkal fut (egyébként nem ez az alapállapota).

Sajnos a valóságban ezek a feltételek gyakran teljesülnek, ami jó táptalaj a Spida terjedéséhez.

Bár 10 másik SQL gép megfertőzése után magától megpróbál „eltűnni" a szerverről, érdemes rá figyelni, hiszen értékes, esetleg titkos adatokat szivárogtathat ki, illetve a rendszer instabillá válhat.

Védekezni többféleképpen is lehet ellene. Mindenekelőtt a fertőzés megelőzhető a 1433-as port forgalmának blokkolásával a tűzfalon; ha erős jelszó van beállítva az SA felhasználónak; ha telepítjük a megfelelő Microsoft SQL-javításokat.

Ha gyanítjuk, hogy fertőzött a gépünk, az alábbi nyomok után kutassunk:

– a cégtől levelek mennek ki az ixltd@postone.com címre, vagy a kimenő levelek tárgysora a „SystemData-" szöveggel kezdődik;

– szokatlan hálózati forgalom folyik a 1433-as porton;

Sor.	Százalék	Vírusnév
1.	(36.49)	I-Worm.Klez
2.	(9.84)	Win95.CIH
3.	(5.52)	I-Worm.Badtransit
4.	(3.30)	I-Worm.Hybris
5.	(0.24)	Trojan.PSW.Delf
6.	(0.21)	I-Worm.Sircam
7.	(0.18)	Win32.Elkern.c
8.	(0.13)	Macro.Word.Cap
9.	(0.09)	Win32.FunLove
10.	(0.07)	I-Worm.Magistr
11.	(0.06)	Backdoor.NetBus
12.	(0.05)	Macro.Word97.Thus
13.	(0.04)	Trojan.PSW.Qip
14.	(0.03)	I-Worm.HappyTime
15.	(0.03)	I-Worm.Cenvlec
16.	(0.03)	Trojan.Downloader.Web.Down
17.	(0.03)	I-Worm.Oibe
18.	(0.02)	Trojan.PSW.M2
19.	(0.02)	Macro.Word97.Flop
20.	(0.02)	Trojan.PSW.Spion

2002. májusi vírusstatisztikák...

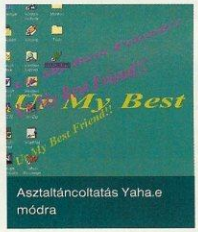
– az „SA" és az „sqlagentcmdexec" nevű felhasználó jelszava nulláról négykarakteresre változik;

– engedélyezettre változik a „Guest" felhasználó, és bekerül a rendszergazdai csoportba;

– az alábbi file-ok jelennek meg a Windows system32 könyvtárában: sqlexec.exe, clemail.exe, sqlprocess.js, sqlinstall.bat, sqldir.js, run.js, timer.dll, samdump.dll, pwdump2.exe;

– a registryben megjelenik a *HKLM\System\CurrentControlSet\Services\NetDDE\ImagePath* kulcs.

Az F-Secure és a Kaspersky Anti-Virus 2002. május 22-től képes detektálni a Spidát.



Asztaltáncoltatás Yaha.e módra

Lentin (Yaha.e)

2002. június 20-án számos országból érkezett jelentés a fertőzött e-mailekhez csatolva terjedő, Yaha.e nevű új féreg megjelenéséről. Névváltozatai: I-Worm.Lentin.G, Lentin.G, Yaha, W32/Lentin.F@mm.

Maga a féreg 27 Kbyte hosszúságú windowsos PE struktúrájú EXE file, amit UPX-szel tömörítettek.

A féreg file-jainak végén általában véletlenszerű dátum található – e terület hossza és tartalma eltérő volt a különböző mintákban.

Ha a féreg aktivizálódik egy tiszta rendszerben, és az általa megfertőzött file névkiterjesztése SCR, előfordulhat, hogy megjelenít a képernyőn egy üzenetablakot, és/vagy lejátszik egy videót, végül megjelenik egy felirat, közben a képernyő rázkódik.

A féreg véletlenszerűen választott néven telepíti önmagát a C:\Recycler vagy a C:\Recycled könyvtárba, vagy ha ezek nem elérhetőek, akkor a \Windows könyvtárba. Ezt követően módosítja az alapbeállítás szerinti .EXE file-indítási kulcsot, így mindegyik EXE indításakor lefuttatja saját magát. Folyamatosan ellenőrzi a kulcsot, hogy semlegesítse a felhasználó és a mentesítőprogram módosításait.

E-mail mellékletben terjed.

Az üzenet létrehozásának szabályai meglehetősen összetettek. Előre meghatározott SMTP szervernevek, üzenettárgyak, mellékletnevek és kiterjesztések közül véletlenszerűen választja ki az e-mail tartalmát, majd elküldi az összes megtalálható e-mail címre. A Klez féreghez hasonlóan különböző típusú e-maileket tud szétküldeni.

Az F-Secure és Kaspersky Anti-Virus 2002. június 25-től képes detektálni.

●

A Top 20 tábla vezető helyét májusban még mindig az I-Worm.Klez család őrzi. További információ a weben a www.kaspersky.com és a www.viruslist.com címen érhető el. Az aktuális vírusokra figyelmeztető friss hírek a www.2f.hu helyen olvashatók.

Hogyan válasszunk víruskeresőt?

Napjainkban a kor kihívásainak megfelelő víruskereső szoftvernek mind komolyabb igényeknek kell eleget tennie, egyre összetettebb és rugalmasabb megoldást kell nyújtania.

Csizmazia István

A víruskeresők piacán bőséges a választék, ezért az optimális eszköz kiválasztása gyakran nagyon nehéz. Néhány pontban összefoglaljuk a korszerű vírusvédelmekkel szembeni követelményeket:

● Kiemelkedő eredményesség: fontos követelmény a víruskeresőkkel szemben a találati arány maximalizálása. Szinte mindig az új vírusok felismerésénél találhatók rések a víruskeresők tudásában – és pontosan az új vírusok jelentik a legkomolyabb fenyegetést, mert ezek okozzák a legtöbb fertőzést. Ezért a víruskeresők találati arányában megmutatkozó parányi eltérések jókora különbséget jelentenek a védelem eredményessége szempontjából!

● Rendszeres, naprakész frissítés: a vírusok rendkívül gyors „evolúciója" következtében újabb és újabb kórokozók ütik fel a fejüket, amelyek fejlődési sebességénél csak az agresszív pusztítási vágyuk nagyobb, ezért a rendszeres és naprakész frissítés mára alapkövetelménnyé vált.

● Többféle keresési módszer: a manuális (on-demand) keresési módszer a felhasználó által bármely tetszőleges időpontban, meghatározott területekre vonatkozó, külön indítható víruskeresés. A valós idejű (on-access) keresési módszernél folyamatosan, működés közben, az épp használatba vett file-okat vizsgálja át a víruskereső. A két módszer közül az utóbbi a fontosabb, mert így a számítógépre kerülő file-ok azonnal ellenőrzésre kerülnek.

● Tömörített file-ok vizsgálata: sok víruskereső nem tud megbirkózni a tömörített file-okban rejtőző vírusok detektálásával. A tömörített file kibontása után aktívvá váló kórokozók komoly károkat idézhetnek elő a rendszerben, ezért a hatékony víruskereső program a tömörített file-okban is felderíti a károkozó szoftvereket.

● Szakszerű támogatás: a vírusvédelmi szoftvereknél nagyon fontos, hogy a felmerülő problémákra gyors és szakszerű megoldást találjunk. Ezért fontos a víruskereső szakszerű és magyar nyelvű támogatottsága. Vállalati hálózatok vírusok és más károkozók elleni védelménél fontosak a következő szempontok.

Sor.	Százalék	Vírusnév
1.	(79,7)	I-Worm.Klez
2.	(10,5)	I-Worm.Lentin
3.	(0,5)	I-Worm.Badtransfl
4.	(0,4)	I-Worm.Sircam.c
5.	(0,4)	Win95.Cih
6.	(0,2)	Win32.FunLove.4070
7.	(0,1)	PS-MPC-based
8.	(0,1)	I-Worm.Hybris.b
9.	(0,1)	Macro.Word97.Thus.ew
10.	(0,1)	I-Worm.Frethem.a
11.	(0,1)	Win32.Elkern.c
12.	(0,1)	Macro.Word.Concept
13.	(0,1)	02-based
14.	(0,1)	Exploit.Applet.ActiveXComponent
15.	(0,1)	I-Worm.Magistr
16.	(0,03)	I-Worm.HappyTime
17.	(0,03)	Macro.Word.Cap
18.	(0,03)	Jerusalem.a
19.	(0,03)	Dirti.1024.a
20.	(0,03)	Win32.Weird.19240

2002. júniusi vírusstatisztika *(forrás: Kaspersky Lab)*

● Központi felügyelet: a teljes víruskereső rendszernek egyetlen gépről, akár földrajzilag távol eső helyről is egyszerűen és precízen kezelhetőnek kell lennie annak érdekében, hogy a rendszer karbantartását és módosítását a felhasználótól függetlenül az adminisztrátor bármikor elvégezhesse.

● Széles körű lefedettség: a hálózatok heterogén volta miatt fontos, hogy a víruskereső többféle platformon is hatékonyan működjön. A programok a Windows 9x/Me/NT/2000/XP-s munkaállomás- és NT/2000-es szerverváltozatokon felül szinte minden operációs rendszer alá elérhetők, például Novell NetWare, Linux, BSDi, FreeBSD és Solaris Unix platformra.

● Központi naplózás: a vírusriadók és egyéb jelentések mindig egy helyre futnak be, ezáltal az események pontosan nyomon követhetőek, az adatok elemzése és kiértékelése gyorsan elvégezhető.

Az aktuális havi kártevők

Új féregvariáns, az I-Worm.Frethem.J/K/L ütötte fel fejét e hónapban (névváltozatai: W32.Frethem.J@mm, W32/Frethem.gen@MM, WORM_FRETHEM.J). Ez a féreg fertőzött e-mailek mellékletében terjed. Tulajdonképpen 35 Kbyte-os PE formátumú EXE file, Visual C++-ban írták. Programkódja ténylegesen 32 Kbyte hosszú, ezt a PE-Pack és az UPX programmal tömörítették.

A fertőzött üzenet az alábbiak szerint néz ki. Tárgy (Subject): *Re: Your password!*

A levél szövege:

ATTENTION!

You can access very important information by this password

DO NOT SAVE password to disk use your mind now press cancel

Csatolt file (attachment): *decrypt-password.exe, password.txt.*

A féreg a lefuttatásához egy biztonsági rést használ ki – IFRAME, hasonló ahhoz, amit a Nimda féreg is használt –, így már akkor aktiválódni tud, ha csak olvassuk vagy az előnézeti ablakban megjelenítjük a fertőzött üzenetet (ehhez hasonló volt a KAK.worm, ahol szintén a fertőzött melléklet megnyitása nélkül tudott aktiválódni a féreg). Ekkor telepíti magát a rendszerre, lefuttatja a terjedéséhez szükséges rutinját és a büntetőrutint. A féreg bemásolja magát a Windows Startup könyvtárába, setup.exe néven: *Start Menu → Programs → Startup → setup.exe.*

Terjedés: a féreg összegyűjti az összes levelezési címet az Outlook könyvtáraiból és a Windows címjegyzékéből (Windows Address Book), és elküldi magát minden egyes címre az alapbeállítás szerinti SMTP szerver segítségével.

Büntetőrutin: a féreg parancsokat küldözget különböző HTTP oldalakra. Az oldalak címeit a féreg a belsejében tárolt listából veszi.

Az F-Secure és a Kaspersky Anti-Virus programjai a 2002. július 15-i délutáni adatfile-jaikkal már képesek detektálni.

A 2002. júniusi havi vírusstatisztika szerint őrzi vezető helyét az I-Worm.Klez család, bár a hatása már kezd lecsengeni. A statisztika a Kaspersky Lab 2002. júniusi havi adataiból készült. További információ a weben a www.kaspersky.com és a www.viruslist.com címen érhető el. Az aktuális vírusokra figyelmeztető friss hírek olvashatók a www.2f.hu webhelyen.

Híres vírusok

Murphy egyik, számítógépes vírusokról szóló mondása szerint: „Mindig olyan vírus támad meg, amelyről azt állítják, hazánkban még nem fertőzött; amihez még nincs kereső- és irtóprogram; ami rombolásban és gonoszságban újat tud mutatni."

Csizmazia István

A híres vírusok története leginkább azzal az egyértelmű tanulsággal szolgálhat, hogy a korszerű víruskereső programok használata mára elengedhetetlenné vált.

● 1986, BHP: a 64 User nevű újság egyik számában azt írta, hogy a Commodore 64 gépre szerencsére lehetetlen vírust írni. Egyik este a mailboxukba érkezett a BHP vírus a Bayerische Hacker Post szervezettől.

A vírus lemezről lemezre tudott terjedni, már ezen a platformon is. Alaposabb vizsgálatakor látszott, hogy 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.

● 1989, Yankee Doodle: a COM és EXE file-okat fertőzi meg felülírással, és délután 17:00-kor eljátssza a Yankee Doodle amerikai népdalt a számítógép hangszóróján. Memóriarezidensen rátelepedett a 21-es megszakításra, és elmentette annak kezdeti értékét. Ezzel a trükkel át tudta verni a rezidens víruskeresőket és képes volt elrejtőzni előlük.

A több mint negyven átirata között volt olyan változat is, amelyik a Novell NetWare bejelentkező jelszavát lopta el.

● 1990, Stoned: rezidens lopakodó vírus, a floppyk bootszektorát és a merevlemez partíciós tábláját fertőzi meg. Floppyról floppyra terjed.

A rezidens rész figyeli, hogy a vírus ott van-e még a bootszektorban, és ha úgy látja, hogy mentesítették azt, akkor a következő pillanatban megint visszaírja. A helyes megoldás ilyenkor, hogy a víruskereső először a memóriában lévő komponenst törli és csak utána mentesít a lemezen.

● 1994, Onehalf: bootolásonként 2-2 cilinder teljes tartalmát titkosítja, a merevlemez végéről indulva. Ha csak simán mentesítjük a gépet, az elkódolt részhez soha többé nem férünk hozzá. Szerencsére készült hozzá egyedi gyógyír, amely a tényleges fizikai mentesítés előtt képes visszaalakítani az eredeti adatokat.

● 1998, CIH-Chernobyl: érdekes eseménylánccolatot indított el a sokak által ismert CIH vírus.

Az első róla szóló jelentések 1998 elején származnak, és jó néhány változata született az idők során. Különlegessége, hogy olyan hibát képes okozni, amely a hardver javítása nélkül nem orvosolható: a gép elindulásához szükséges Flash BIOS-t teszi tönkre. Legismertebb és legelterjedtebb változata minden év április 26-án aktivizálódik, ekkor fejti ki hatását.

Sor.	Százalék	Vírusnév
1.	(34,28)	I-Worm.Klez
2.	(9,24)	I-Worm.Lentin
3.	(0,93)	Win95.CIH
4.	(0,90)	I-Worm.Frethem
5.	(0,28)	I-Worm.Desos
6.	(0,15)	Win32.FunLove
7.	(0,12)	I-Worm.Hybris
8.	(0,10)	I-Worm.Badtransit
9.	(0,09)	I-Worm.Magistr
10.	(0,07)	Win32.Elkern
11.	(0,06)	I-Worm.HappyTime
12.	(0,07)	I-Worm.Kitro
13.	(0,05)	Win32.Kriz
14.	(0,05)	Macro.Word97.Thus
15.	(0,05)	Backdoor.VB
16.	(0,03)	I-Worm.Duni
17.	(0,03)	Backdoor.CyberSpy
18.	(0,03)	Backdoor.Casus
19.	(0,03)	Win95.Tecata
20.	(0,03)	Macro.Word97.Nori

2002. júliusi vírusstatisztika *(forrás: Kaspersky Lab)*

Ez a változat azonban csak 1998 közepén terjedt el szélesebb körben, így első aktivizálódási dátuma 1999. április 26-a lett.

● 2001, SirCam: hat nappal július 18-i felfedezése után a SirCam internetes féreg már az egész világon elterjedt, és az egyik leggyakoribb károkozóvá vált. A SirCam a fertőzött gép merevlemezén található dokumentumokból továbbküld egyet – a vírussal együtt – különböző címekre.

Az indiszkréció által okozott károkon túl figyelmet érdemel a SirCam pusztító rutinja is: 5% esély van rá, hogy a féreg a Windows mappájának minden almappáját és file-ját kitörölje – ezután a gép már nem fog elindulni.

● 2001, Nimda: e vírus érdekessége, hogy egyszerre négy különböző fertőzési mechanizmust is képes alkalmazni. Megjelenésekor 24 óra leforgása alatt 2,2 millió gépet fertőzött meg. A hosszú távú hatásos védekezéshez nem elég a vírusmentesítés, hanem mindenképpen szükséges a Microsoft megfelelő javító patcheinek lefuttatása is. E vírus hálózati kapcsolatokon keresztül is fertőz, ezért hálózatos környezet mentesítésekor a gépeket le kell választani a hálózatról, és mind-egyiket külön-külön kell mentesíteni. Csak ezután szabad újra hálózatba kapcsolni. Érdemes a vírus nevét visszafelé is elolvasni.

● 2002, Klez: a Klez.H vírus a fertőzött gép merevlemezén található dokumentumokból véletlenszerűen kiválaszt egyet, és továbbküldi a vírussal együtt különböző címekre, így titkos vagy bizalmas információk kerülhetnek idegenkezekbe. Ezenkívül az is sűrűn előfordul, hogy a vírusok megpróbálnak hátsó ajtót nyitó (backdoor) programot telepíteni az áldozatok gépére, amelyen keresztül minden adatunk, merevlemezeink teljes tartalma kiszolgáltatottá válik a rosszindulatú vírusterjesztő számára. Megjelenése óta a vírusstatisztikák éllovasa, rengeteg levelet küldenek a fertőzött gépek, és ezekben a levelekben a feladó legtöbbször hamis, így a visszaküldött figyelmeztetésünk sem éri el a célját.

●

A vírusok száma napjainkban már a 60 ezerhez közelít, ezért meg kell tanulnunk együtt élni velük, és hatékonyan felvenni a harcot támadásaikkal szemben.

Jó példa erre a júliusi Top 20 táblát ismételten vezető I-Worm.Klez.

A sok fertőzött gép, amelyeken egyáltalán nincs víruskereső, egyre csak ontja és ontja a hamisított címmel érkező fertőzött leveleket.

További információ a weben a www.kaspersky.com és a www.viruslist.com, magyarul a www.2f.hu címen érhető el.

Rés az Apache-on

Mint várható volt, a Linux sem kerülhette el a netes férgek támadásait. És az sem okozott meglepetést, hogy a leggyakrabban futtatott webes alkalmazások hibáit kihasználva kerül a betolakodó a rendszerbe.

Csizmazia István

A linuxos szervereken az Apache az egyik leggyakoribb lakó, egyben a férgek egyik legújabb célpontja. A Slapper (Ütő) is ezt támadja meg. Névváltozatai: Linux.Slapper-A, Linux.Slapper-Worm, Apache/mod_ssl Worm, Slapper.source. A 2002 augusztusában felfedezett OpenSSL könyvtárbeli hibát használja ki, hogy linuxos hálózati környezetben terjedhessen. Először 2002. szeptember 13-án pénteken, Kelet-Európában észlelték. A féreg azokat a gépeket veszélyezteti, melyeken Apache webszerver fut, OpenSSL támogatással. Ez elég sok gépet érinthet, nagyjából a nyilvános netes webszerverek 60%-át. Becslések szerint ezek kevesebb mint 10%-án engedélyezték az SSL szolgáltatást. Leggyakrabban az online kereskedelmi, banki és egyéb, titkosságot igénylő alkalmazásoknál használják.

Ha megfertőz egy gépet, a féreg megpróbál onnan tovább terjedni más gépekre. Emellett a kódja megvalósít egy peer-to-peer hálózati támadást is, ennek következményeként a fertőzött gépeket távolról lehet DDoS (Distributed Denial of Service) típusú támadásra használni. Red Hat, SuSE, Mandrake, Slackware vagy Debian disztribúciót futtató Intel-alapú gépeket veszélyeztet, ha azok Apache-ot és 0.96d verziójú vagy régebbi OpenSSL-t használnak. A Slapper nagyon hasonlít a korábbi, szintén az Apache-ot veszélyeztető Scalper féreghez – azt 2002 júniusában fedezték fel –, de működése sok hasonlóságot mutat a Code Reddel is. Eddig Norvégiából, Litvániából, Romániából, Portugáliából, Japánból, Hollandiából, Kínából, Törökországból, Indiából, az Egyesült Államokból, Tajvanról és Angliából jelentettek fertőzéseket.

Sor.	Százalék	Vírusnév
1.	(76,45)	I-Worm.Klez
2.	(11,66)	I-Worm.Lentin
3.	(5,45)	Win95.CIH
4.	(1,24)	Aboa
5.	(0,10)	I-Worm.Hybris
6.	(0,07)	Win32.FunLove
7.	(0,03)	I-Worm.Sircam
8.	(0,01)	I-Worm.Magistr
9.	(0,01)	Win95.Tecalla
10.	(0,01)	Backdoor.Antitrim
11.	(0,01)	I-Worm.HappyTime
12.	(0,01)	Trojan.Win32.Filecoder
13.	(0,01)	Armagedon
14.	(0,01)	Backdoor.Arcanum
15.	(0,01)	Alberton
16.	(0,01)	I-Worm.Badtransfi
17.	(0,01)	Backdoor.Cabledor
18.	(0,01)	Trojan.PSW.Stealth
19.	(0,01)	Backdoor.Death
20.	(0,01)	Trojan.Ji3.Seeker

2002. augusztusi vírusstatisztika *(Forrás: Kaspersky Lab)*

A Slapper.A a rendszer megfertőzésekor létrehozza a /tmp/.uubugtraq file-t, az abban tárolt saját elkódolt (uuencoded) másolatával és a GCC fordító segítségével készít egy végrehajtható file-t /tmp/.bugtraq néven, amit aztán le is futtat. Ekkor elkezd keresni védtelen „A" osztályú hálózatokhoz tartozó gépeket, rácsatlakozva a httpd szerverre (80-as port). Ha létre tudja hozni a kapcsolatot, akkor ellenőrzi, mi szerepel a válasz fejlécében a „Server:" szövegben. Ha ott megtalálja az „Apache" stringet, megkísérel csatlakozni az SSL szerverre (443-as port), és megpróbálja megfertőzni az említett OpenSSL hibát kihasználva. A féreg tartalmaz egy backdoort is, ami a 2002-es UDP portot hallgatja le, és távolról vezérelhető. A backdoor engedélyezi, hogy a fertőzött gépre tetszőleges programokat tölthessenek fel, illetve futtathassanak le, valamint lehetővé teszi, hogy az adott gépről DDoS támadást lehessen indítani.

Eltávolítás

A fertőzött gépeken a futó processzek között látható a *.bugtraq* is. Először ezt kell leállítani, majd le kell törölni a hozzá tartozó file-okat: /tmp/.uubugtraq; /tmp/.buqtraq.c; /tmp/.bugtraq. Az Apache webszervert le kell állítani, amíg az OpenSSL könyvtárat nem frissítjük a javított verziójával (0.9.6e vagy újabb), nehogy visszafertőződjön a rendszer.

Időközben a féreg két további variánsa is felbukkant. A Slapper.B: (névváltozata: Cinik) a fertőzött gépen feltölti magát a /tmp/.cinik.uu helyre, kikódolja magából a forráskódot /tmp/.cinik.c néven, majd lefordítja magát futtathatóvá a /tmp/.cinik helyre. Ez a változat már az 1978-as portot használja a 2002-es helyett.
A Slapper.A-hoz hasonlóan beírja magát a crontab file-ba, elérve ezzel a féreg óránkénti indítását, ezért a mentesítéskor a crontab bejegyzést is törölni kell.

A Slapper.C (névváltozatai: httpd, unlock) csak egy alig módosított változat, amely a 4156-os portot használja a 2002-es helyett, illetve a keletkező file neve is más: /tmp/.unlock. Ez is küld IP-címeket tartalmazó e-maileket a fertőzött gépekről a vírus írójának. A mentesítés a szokott módon történik: az Apache szerver leállítása után le kell lőni a féreg processzét, majd törölni kell azt a /tmp/.unlock helyről.

Végül az Apache újraindítása előtt frissíteni kell a megfelelő OpenSSL könyvtárakat.

Az F-Secure és a Kaspersky Anti-Virus a Slapper összes variánsát képes detektálni.

Augusztusi „kedvencek"

A 2002. augusztusi Top 20 első helyén továbbra is az I-Worm.Klezt találjuk, számszerint ez okozza a legtöbb fertőzést. További információ a weben a www.kaspersky.com és a www.viruslist.com címen érhető el. Az aktuális vírusokra figyelmeztető friss hírek a www.2f.hu címen olvashatók.

Info

- OpenSSL-lel kapcsolatos tanácsok: www.openssl.org/news/secadv_20020730.txt
- A CERT hivatalos közleménye: www.cert.org/advisories/CA-2002-23.html

Linuxos biztonsági információk:

- www.debian.org/security/2002/dsa-136
- www.mandrakelinux.com/en/security/2002/MDKSA-2002-046.php
- rhn.redhat.com/errata/RHSA-2002-155.html
- www.suse.com/de/security/2002_027_openssl.html

Mumus az ajtó mögött

Új, veszélyes fegyverzetű e-mail féregvírus terjed az interneten, Tanatos avagy Bugbear (Mumus) néven. Az F-Secure cég és a Kaspersky Labs is jelentősnek ítélte a vírus által okozható károkat, és azonnal közreadták a riasztást, a vírus leírását és a soron kívüli vírusadatbázis-frissítésüket.

Csizmazia István

Névváltozatai: I.Worm. Tanatos/Bugbear, W32/Bugbear, Tanat, W32/Tanat. A Tanatos beépített trójai (kémprogram) lehetőségekkel bír, többek között a begépelt szöveget (például jelszavakat!) naplózza. A féreg tulajdonképpen egy 50688 byte nagyságú, UPX tömörítésű PE EXE file, így könnyen terjedhet levelek mellékleteként, vételenszerű file-neveket használva. Megtévesztés céljából több névkiterjesztése is lehet, így az igazi típusa Windows alatt alapesetben el van rejtve. A fertőzött levelek tárgysora és törzse (szövege) is változik, így az nem nyújt igazi segítséget a szűréshez.

A víruskód az Internet Explorer-beli, már sokat emlegetett I-Frame.exploit böngészőhiba felhasználásával megpróbál automatikusan lefutni az Outlook és Outlook Express levelezőrendszerek betekintő ablakában – ez nagyon hatékony módszer a vírusok terjedésére. Ezért mindenkinek javasoljuk, hogy telepítsék, illetve frissítsék Internet Explorerük biztonsági javítását Windows rendszerükön! (➥ www.microsoft.com /windows/ie/downloads/critical/q323759ie /default.asp)

Ha a féreg bejutott a gépbe, változó neveken (például JFMV.EXE) másolja be magát a Windows rendszerkönyvtárba, és létrehozza az őt rendszerindításkor lefuttató registrybejegyzést a *[HKLM\Software\Microsoft\Windows \CurrentVersion\RunOnce]* kulcs alatt. Ugyancsak telepítésre kerül egy kémkomponens, amely a billentyűleütéseinket naplózza, ez is vételenszerűen kap nevet (például ZLQPUPP.DLL). Két másik, a Bugbear által létrehozott DLL file célja még nem ismert közelebbről, ezekben kódolt adatok vannak. További két file (.DAT típusúak) a Windows gyökérkönyvtárába kerül.

A kártevő megpróbálja hatástalanítani a gépünkre telepített különböző biztonsági – vírusellenes és tűzfal- – szoftvereket, és letiltja komponenseik működését a memóriában. Így ha víruskeresőnk adatállománya a fertőzési kísérlet pillanatában régi, és még nem ismeri a Tanatost, akkor a gép megfertőződhet. Ezért is fontos a rendszeres adatbázis-frissítés – állandó netkapcsolat esetén akár naponta javasolt frissíteni.

Sor.	Százalék	Vírusnév
1.	(72.93)	I-Worm.Klez
2.	(23.82)	I-Worm.Lentin
3.	(0.27)	Win95.CIH
4.	(0.17)	Trojan.Win32.Filecoder
5.	(0.13)	Macro.Word97.Thus
6.	(0.13)	I-Worm.Sircam
7.	(0.11)	I-Worm.Magistr
8.	(0.04)	Macro.Word97.Flop
9.	(0.04)	I-Worm.Cenvec
10.	(0.03)	I-Worm.Hybris
11.	(0.02)	Backdoor.Death
12.	(0.02)	Macro.Word97.Elban
13.	(0.02)	Win32.FunLove
14.	(0.02)	Macro.Word97.Marker
15.	(0.02)	Macro.Word97.TheSecond
16.	(0.01)	Trojan.PSW.W2
17.	(0.01)	Backdoor.Antilam
18.	(0.01)	Worm.Linux.Slapper
19.	(0.01)	Palm.Phage
20.	(0.01)	Nuker.Win32.Nabber

2002. szeptemberi vírusstatisztika *(Forrás: Kaspersky Lab)*

A trójai komponens a 36 794-es TCP porton hallgatózik, és lehetővé teszi, hogy távolról bejussanak gépünkre, majd azon keresztül a helyi hálózatunkra. A Tanatos ehhez egyszerűen kezelhető webes felületet kínál, ezért veszélyes fegyver lehet kevésbé képzett hackerek (script kiddie) kezében is.

Valamilyen okból – feltehetően programozási hiba miatt – a hálózati terjedési részben a féreg a megosztott hálózati nyomtatókra is elküldi saját másolatát.

Worm.Win32.Opasoft

Névváltozatai: I-Worm.Opasoft, W95/Scrup.worm, W32.Opaserv.Worm, Opasoft, Scrup. Az Opasoft egy 28 Kbyte hosszú Windows PE EXE file-ban terjedő hálózati féreg. Beépített trójai (kémprogram) képességekkel is bír, a helyi és távoli hálózatokon való terjedéshez a Windows NetBIOS szolgáltatását használja.

Amikor a féreg telepíti magát, létrehozza a scrsvr.exe nevű file-t a Windows könyvtárában, és elkészít egy olyan registrykulcsot, amely ezt minden rendszerindításkor lefuttatja *(HKLM\Software\Microsoft\Windows \CurrentVersion\Run ScrSvr = %worm name%)*, majd törli az eredeti file-t.

A féreg ellenőrzi a helyi hálózat IP-címeit, valamint véletlenszerűen választott IP-címtartományokat. Ellenőrzéskor adatokat küld a 137-es portra (NetBIOS Name Service). Megfelelő válasz esetén lefuttatja a fertőzési rutinját. Ez meghatározott SMB csomagokat küld a fellelt IP-címre a 139-es portra (NetBIOS Session Service). Ennek eredményeképpen új program keletkezik az áldozat Windows könyvtárában – scrsvr.exe –, valamint a WIN.INI-be olyan utasításokat ír, amitől a féreg a gép következő újraindításakor végrehajtódik („run=" parancs a [windows] részben). A fertőzés sikerét a C:\TMP.INI file létrejötte jelzi a „master" gépnek.

A trójai rutin megpróbálja frissíteni magát az azóta már leállított www.opasoft .com weboldalról. A hátsó ajtó (backdoor) rész a ScrSin.dat és a ScrSout.dat file-t használja futása során, ezeket erős titkosítással kódolták le. Mivel a www.opasoft. com webszervert időközben kikapcsolták, nem lehetséges több információt szerezni e hátsóajtó-rutin lehetséges felhasználásáról.

A féreg arról is gondoskodik, hogy egyazon gépet ne fertőzze meg többször. Ehhez elkészít egy windowsos mutexet ScrSvr31415 néven. A féreg a Windows 9x és Me operációs rendszerű gépeket képes megfertőzni, míg a Windows NT/2000/XP-t futtató gépeket nem.

●

A szeptember havi vírusstatisztika Top 20 táblájában a vezető helyen továbbra is az I-Worm.Klez trónolt. A szeptember 30-án megjelent I-worm.Tanatos/Bugbear és Worm.Win32.Opasoft itt egy nap alatt még nem éreztette a hatását.

További információ a weben a www .kaspersky.com és a www.viruslist .com címen érhető el. Az aktuális vírusokra figyelmeztető friss hírek a 2F honlapján olvashatóak a www.2f.hu címen.

Egy programban több védelem

Igazi különlegesség az olyan víruskereső, amely több keresőmagot is használ. Általánosságban elmondható, hogy (valós idejű) víruskeresőből egy gépre egyszerre csak egy telepíthető fel problémamentesen.

Csizmazia István

Egynél több program használata rendellenes működést okozhat. A több keresőmotoros program viszont többszörös védelmet nyújt – a párhuzamos használat hátrányai nélkül. Ez nem csak azt jelenti, hogy ilyenkor nem zavarják egymás működését a programok, hanem a sebessége is kedvezőbb, mint több különböző program futtatása. A vizsgálandó file fizikai, alacsony szintű olvasása csak egyszer történik meg, ezután – esetleges dekódolás és kibontás után – sorban mindegyik víruskereső motor megkapja ellenőrzésre. Így például három keresőmotor használata nem fog oktvetlenül háromszoros időráfordítást igényelni. Az F-Secure ezt valósította meg 1997-ben. Az F-Secure program három különböző keresőmotort ötvözött egy rendszerbe: az F-Protot, az AVP-t (a Kaspersky cégtől) és az Oriont. Az F-Secure Framework keretrendszere nemcsak vírusvédelmi eszközei, hanem az összes F-Secure termék központi vezérlését megoldotta, így vírusellenőrzéskor nem okoz semmilyen gondot a titkosított file-ok használata. Az átvizsgálandó file – prioritása folytán – először mindig a FileCryptóhoz kerül, itt ha szükséges, megtörténik a visszakódolása. Ezek után, ha a program valamilyen futtatható tömörítővel vagy valamilyen általános tömörítővel (Zip, Rar stb.) volt sűrítve, akkor kibontásra kerül, és ezek után fogják a víruskereső magok átvizsgálni a file-t. Ebből az is következik, hogy a használt titkosítóprogramnak és a víruskereső szoftvernek együtt kell tudni működni ebben a folyamatban.

I-Worm.Winevar

Névváltozatai: HLLM.Seoul, W32.HLLW.Winevar, Korvar, Braid.C, Winevar. Ez a féreg e-mail üzenetek mellékletében terjed. A kódja 91 Kbyte hosszúságú PE EXE file. Az általa megfertőzött üzenet így néz ki:

Sor.	Százalék	Érték	Vírusnév
1.		44.9	I-Worm.Tanatos
2.		21.6	I-Worm.Lentin
3.		14.0	I-Worm.Klez
4.		3.1	Macro.Word97.Thus
5.		1.1	I-Worm.Hybris
6.		1.0	I-Worm.Magistr
7.		1.0	Macro.Word97.Marker
8.		0.7	I-Worm.Bircam
9.		0.7	Macro.Word97.Flop
10.		0.5	Macro.Word97.Ethan
11.		0.5	Macro.Word97.TheSecond
12.		0.4	Macro.Word97.Onax
13.		0.3	Macro.Word97.Story
14.		0.3	I-Worm.Cervivec
15.		0.3	Joke.Win32.Train
16.		0.3	Backdoor.Death
17.		0.3	Macro.Word97.Dig
18.		0.3	Macro.Word97.Melissa
19.		0.2	Trojan.PSW.Gip.113
20.		0.2	Trojan.Win32.Erase2002

2002. októberi vírusstatisztika. A szeptember 30-án megjelent I-worm.Tanatos/Bugbear jócskán megelőzte a korábbi listavezető I-Worm.Klezt *(Forrás: Kaspersky Lab)*

Tárgy (Subject): „Re: AVAR(Association of Anti-Virus Asia Reseachers)"

A levél szövege (Body):

AVAR(Association of Anti-Virus Asia Reseachers) - Report. Invariably, Anti-Virus Program is very foolish.

A levélhez két csatolt file tartozik: a MUSIC_1.HTM és a MUSIC_2.CEO.

A féreg a lefuttatásához az IFRAME Exploit biztonsági rést próbálja meg kihasználni. Telepíti magát a rendszerbe – bemásolja magát a Windows System alkönyvtárába, WINxxxx.EXE vagy WINxxxx.PIF néven –, majd lefuttatja a terjesztő- és a büntető-rutinját. A file nevében az „xxxx" véletlenszerű szám. Végül a féreg létrehoz egy olyan registrykulcsot, amely ezt a file-t minden rendszerindításkor elindítja:

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]

Létrehoz továbbá egy Funlove.4099 vírusvariánst is (dropper), amelyet WINxxxx.PIF néven néven bemásol, szintén a Windows System mappájába. A Funlove eredeti szövege helyett ezt a karaktersorozatot tartalmazza: *~AAVAR 2002 in Seoul~*. Az eredeti Funlove vírus neve FLCSS.EXE volt, itt AAVAR.PIF néven keletkezik.

Bizonyos körülmények között az I-Worm .Winevar megjeleníti még az alábbi üzenetet:

Make a fool of oneself
What a foolish thing you have done!

A féreg a *.HTM file-okban és a *.DBX (Outlook Express) levelezőmappa file-okban kutat címek után, és ezekre küldi tovább magát. A címek közül azonban nem használja a „microsoft@" karaktersorozattal kezdődőket. Terjedéséhez közvetlenül az alapbeállításban szereplő SMTP levelezőszervert használja, ezt a Windows regisztrációs adatbázisából olvassa ki.

Tartalmaz egy hálózati terjedési rutint is, amely bemásolja magát EXPLORER.PIF néven a hálózati megosztásokba, de az első vizsgálat alapján úgy tűnik, ezt a rutint nem fejezte be a féreg írója.

A büntetőrutin a futó processzek közül vírusellenes, tűzfal- és debugger programok folyamatait próbálja megkeresni és leállítani, valamint a hozzájuk tartozó file-okat letörölni. Néhány esetben (vagy talán minden alkalommal?) ha vírusellenes programot talál, minden file-t töröl az összes meghajtóról. A féreg megváltoztatja a regisztrációs adatbázisban (registry) az alábbi kulcsokat: SOFTWARE\Microsoft\Windows NT \CurrentVersion, SOFTWARE\Microsoft \Windows\CurrentVersion – ezek eredeti értéke helyett a következő szövegeket írja be: *RegisteredOrganization = Trand Microsoft Inc.* és *RegisteredOwner = AntiVirus*. Emellett a féreg végtelen ciklusban keresi a www.symantec.com oldalt, evvel DoS-támadást próbál intézni a szerver ellen.

Az F-Secure és a Kaspersky Anti-Virus programok a 2002. november 25-i adatfile-okkal már képesek detektálni.

●

Az aktuális vírusokra figyelmeztető friss hírek a 2F honlapján olvashatóak a www.2f.hu címen.

Kaspersky Anti-Hacker

A Kaspersky Labs bejelentette, hogy rövidesen piacra dobja a Kaspersky Anti-Hacker nevű személyi tűzfalprogramot.

Csizmazia István

A Kaspersky Anti-Hacker könnyen használható védelmi eszköz a netes támadások veszélyeinek csökkentésére windowsos gépeknél. Segítségével felügyelhetők a számítógépen történő hálózati események (a szoftver nyomon követi az alkalmazások tevékenységét, ellenőrzi a neteléret, és megszűri a bejövő és kimenő adatcsomagokat). Lehetőséget nyújt bizalmas adatainak védelmére mind a helyi hálózatban, mind pedig az interneten.

Képes „önálló tanulásra", továbbá az alkalmazások adatforgalmának szűrésére engedélyező-tiltó szűrőszabályok alapján. Minden alkalmazáshoz tetszőleges számú szabályt rendelhetünk, és ha a program hálózati forgalmat észlel, a szabályok alapján hozott döntése után azt megakadályozhatja. A felhasználó figyelmeztetést kap a nem kívánt eseményekről, és így meggátolhatja azokat.

Szabályoknak kétféle tulajdonságát adhatjuk meg: alkalmazásszűrést a program típusa szerint (e-mail, üzenettovábbító rendszer, böngésző, konferenciaprogram stb.); csomagszűrést az egyes alkalmazások által használt protokollokra, IP-címekre és a forgalom irányára vonatkozó engedélyek szerint. A beállítás lehet engedélyező (ALLOW) – ekkor az adott elérés nem szakad meg; másrészt lehet tiltó (BLOCK), amely megtiltja, hogy egy kívülről indított kapcsolaton jogosulatlanul érhessenek el információkat a gépünkről. A számítógép jelenléte elrejthető a külvilág elől a SmartStealth, azaz a lopakodó mód használatával.

Az Anti-Hacker emellett az engedélyezett alkalmazásokat nemcsak név szerint, hanem hosszuk és CRC értékük szerint is ellenőrzi végrehajtásuk előtt.

Sor.	Százalék	Érték	Vírusnév
1.		27.7	I-Worm.Lentin
2.		23.4	I-Worm.Klez.h
3.		3.2	I-Worm.Tanatos
4.		2.5	Macro.Word97.Thus
5.		1.4	I-Worm.Bridex
6.		1.3	Worm.Win32.Opasoft
7.		1.3	Macro.Word97.Marker
8.		1.3	I-Worm.Hybris
9.		1.3	Macro.Word.Cap
10.		0.9	Win32.Elkern
11.		0.8	Macro.Word97.VMPC
12.		0.8	Macro.Word97.Flop
13.		0.6	Win32.FunLove
14.		0.6	I-Worm.Magistr
15.		0.6	Macro.Word97.Saver
16.		0.6	Win95.Spaces
17.		0.5	Macro.Word97.TheSecond
18.		0.5	I-Worm.KakWorm
19.		0.5	I-Worm.Winevar
20.		0.5	Macro.Word97.Claud

2002. novemberi vírusstatisztika. Bár már jelentkezett némi kimutatható I-Worm.Winevar-fertőzés, ez egyelőre még nem számottevő *(Forrás: Kaspersky Lab)*

Előzetes információk szerint a termék használatához az alábbi hardver-, illetve szoftverelemek szükségesek: Windows 95OSR2/98/Me/NT 4 Workstation/2000 Professional/XP, 50 Mbyte lemezhely, 150 MHz-es Pentium, WinSock2, 64 Mbyte RAM (Windows XP esetén: legalább 300 MHz-es Pentium és 128 Mbyte RAM). Az ismerkedéshez letölthető a program 30 napos próbaváltozata a netről (➥ www.2f.hu /letoltes/avptrial.html#anti).

A hónap réme: I-Worm.Galil

Az I-Worm.Galil e-mail üzenetek mellékletében terjed. E féreg több összetevőből áll, ezek mindegyike Visual Basic nyelven írt Windows PE EXE file. Névváltozatai: Galil, W32/Holar.c@MM, W32/Lagel.A, W32/Crillegal.A@mm.

A fő komponense az iLLeGaL.exe, melynek hossza 81 Kbyte. Terjedési komponense a Mplayer.exe, ennek hossza 14 Kbyte (UPX-szel tömörítették, eredeti hossza 37 Kbyte); az SMTP komponens pedig az SMTP.ocx, melynek hossza 26 Kbyte (szintén UPX-szel tömörítve, eredetileg 90 Kbyte). Ha a féreg főkomponense lefut, akkor telepíti saját magát és többi modulját – bemásolja magát a Windows System alkönyvtárába iLLeGaL.exe néven, majd a többi programrészt is bemásolja ebbe a könyvtárba.

Az Mplayer.exe komponens létrehoz egy olyan registrykulcsot, amellyel minden rendszerindításkor lefuttatja saját magát: *HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices iLLeGaL = %SystemDir%\Mplayer.exe*

A féreg egy hamis Flash animációt jelenít meg és az alábbi üzenetet írja ki:

„Sorry !
Looooooooool, thanx fo da time u spent thinkin ov me"

Terjedési részében a féreg összegyűjti az összes levelezési címet a Microsoft Outlook címjegyzékéből és e-mail címeket keres a .HTM és .HTML névkiterjesztésű file-okban. Terjedéséhez közvetlenül az alapbeállításban szereplő SMTP levelezőszervert használja, ezt a Windows regisztrációs adatbázisából olvassa ki, majd elküldi magát minden egyes címre az alábbi formátumú levélben:

Tárgy (Subject): *Fwd: Crazy illegal sex !*

A levél szövegét (Body) véletlenszerűen választja ki a C: meghajtó file-jaiból, és van egy melléklete is, az iLLeGal.exe vagy az illegalSex.zip. A fertőzésre csak akkor kerül sor, ha a felhasználó megnyitja a mellékletet. Ekkor a féreg telepíti magát a rendszerre, majd lefuttatja a terjedési és büntetőrutinját: új kulcsot (egy számlálót) készít a regisztrációs adatbázisban *HKLM\iLLeGal* néven, aminek a féreg minden indításakor megnöveli az értékét. Ha az érték eléri az ötöt, akkor minden file-t töröl a D:, az E:, az F: és a G: meghajtóról, és megjeleníti az alábbi üzenetet:

„ZaCker
No Peace Without war,i hate war but im forced to love it,Hidden Power's gonna b there wherever u r"

●

Aktuális vírusokra figyelmeztető friss hírek olvashatók a www.2f.hu címen.

Egymást támadó vírusok

„Kutyaharapást szőrivel", „Sárkány ellen sárkányfű" – és még sorolhatnánk a frappáns gyógymódokat olyan esetekre, amikor hirtelen nem tudunk egy problémára hathatós megoldást találni.

Csizmazia István

A vírus ellen ellenvírus elv jónak tűnik a futurisztikus filmekben, de a valóságban nem biztos, hogy örülünk neki. Ha beköltözik a gépünkre, akkor (még) eggyel több vírus lesz a rendszerben, mint amennyire szükségünk van.

2003. január 15-én tűnt fel egy elég érdekes tulajdonságokkal bíró vírus, a Sahay (W32.Sahay.A@mm). E-mail üzenetek mellékletében terjed. A fertőzött üzenet így néz ki:

Tárgy (Subject): Fw: Sit back and be surprised

Csatolt file (Attachment): mathmagic.scr

Eddig semmi rendkívülit nem látunk, szokásos e-mail féregnek tűnik. Ha viszont rákattintunk a mellékletre, létrejön a gép főkönyvtárában egy Yahasux.vbs nevű file. Az érdekesség az, hogy ez megkísérli a Yaha (I-Worm.Lentin) családba tartozó férgeket leírtani (ebben az esetben ez a törlést jelenti), majd újraindítja a gépet.

Az, hogy nemcsak látszólag végez „hasznos" tevékenységet, abból is kitűnik, hogy megkísérli önmagát hozzáfűzni a Windows és – ha telepítve van – a mIRC IRC-kliens könyvtárában található minden .EXE file-hoz. Ezenkívül kéretlenül továbbküldi magát e-mailben. A terjedéshez szükséges e-mail címeket a Windows címjegyzékéből (WAB) veszi. Emellett – valószínűleg valamilyen programozási hiba miatt – le is fagyaszthatja a számítógépet.

Bár nem ez az első eset a vírustörténelemben, amikor olyan vírust írnak, amely egy másikat hatástalanít, az esettel kapcsolatban érdemes felidézni a számítógépes vírus klasszikus definícióját: egy vírusnál nem okvetlenül követelmény, hogy kártékony büntetőrutinja is legyen, elég ha fertőző- és terjedőképes.

A fő probléma persze az, hogy a felhasználó tudta, illetve jóváhagyása nélkül fut kód a gépen. Büntetőrutin nélkül is elég kárt tud okozni egy vírus azzal, hogy telíti a kommunikációs csatornákat, illetve az eltávolítása időbe és pénzbe kerül.

Aktuális havi kártevő: I-Worm.Avron

Névváltozatai: W32/Lirva.B, W32.Arvil.A, W32.Naith.A, Lirva. Az Avron vírus fertőzött e-mailek mellékletében terjed az interneten.

Sor.	Százalék	Érték	Vírusnév
1.		24.74	I-Worm.Klez
2.		10.93	I-Worm.Lentin
3.		6.88	Macro.Word97.Thus
4.		3.31	I-Worm.Hybris
5.		3.07	I-Worm.Tanatos
6.		2.97	Win32.Elkern
7.		1.93	Worm.Win32.Opasoft
8.		1.45	Macro.Word97.Marker
9.		1.14	Macro.Word97.TheSecond
10.		1.03	VBS.Redlof
11.		0.94	Win32.FunLove
12.		0.94	Macro.Word97.Saver
13.		0.86	Win95.Spaces
14.		0.77	I-Worm.Winevar
15.		0.64	Backdoor.NetDevil
16.		0.61	I-Worm.KakWorm
17.		0.58	Macro.Word97.VMPC
18.		0.58	Win95.CIH
19.		0.58	Backdoor.Optix
20.		0.57	Macro.Word97.Flop

2002. decemberi vírusstatisztika *(Forrás: Kaspersky Lab)*

Emellett más csatornákat is igyekszik kihasználni: a Kazaa file-cserélő hálózatot, az ICQ és mIRC csatornákat, valamint a windowsos gépek megosztásait. Megkísérli leállítani különféle vírusellenes és tűzfalprogramok futását. Ha az Avron már aktív, akkor trójai komponense a megfertőzött gépről információkat (jelszavakat) próbál meg továbbítani egy meghatározott e-mail címre. Terjedéséhez a Windows címjegyzékében (Address Book) és a .DBX (Outlook Express) file-okban, illetve a .HTML, .EML, .HTM, .TBB, .SHTML, .NCH és .IDX névkiterjesztésű file-okban kutat e-mail címek után.

A féreg elküldi magát az összes fellelt e-mail címre, ehhez véletlenszerű tárgyat, levélszöveget és mellékletnevet választ saját listájából. A küldött levél HTML formátumú, és tartalmazza a nevezetes IFRAME exploitot. Ennek segítségével a féreg már akkor tud aktiválódni, ha csak olvassuk vagy az előnézeti ablakban megjelenítjük a fertőzött üzenetet, vagyis megnyitás nélkül futtatja az Internet Explorer a mellékletet, ha a gépen Outlook Expresst használunk, és nem futtattuk le a Microsoft megfelelő hibajavító patch-ét.

Mentesítéshez jól használható a Kaspersky Labs CLRAV segédprogramja, amelynek 8.2.0-s verziója már az Avron vírust is írtja (⇨ letölthető: www.2f.hu/files/utility/clrav.zip).

Az F-Secure és a Kaspersky Anti-Virus a 2003. január 8-i adatfile-jával már képes detektálni.

Rémek év végén

Végül következzen 2002. decemberének vírusstatisztikája, mivel lapzártánkkor a januári adatok még nem álltak rendelkezésünkre.

A százalék oszlopban az előfordulás gyakorisága látható. A Top 20 táblában látható, hogy újra az I-Worm.Klez család vezeti a mezőnyt. A statisztika a Kaspersky Lab 2002. december havi adataiból készült. További információ a weben a www.kaspersky.com és a www.viruslist.com címen található, az aktuális vírusokra figyelmeztető friss hírek pedig a www.2f.hu címen olvashatók.

Ki áll nyerésre?

A bűnözés kapcsán szokták emlegetni, hogy az elkövetők mindig egy lépéssel a bűnüldözők előtt járnak. Sajnos ez többnyire igaz a vírusok elleni védekezésre is. Megjelenik egy-egy vírus – mi pedig várjuk a mihamarabbi ellenszert.

Csizmazia István

Egy neves elemzőcég felmérése szerint a Slammer/Sapphire vírussal megfertőződött SQL szerverek 90%-a a járvány első 10 percében esett áldozatul. Az általuk publikált jelentés szerint a Slammer féreg közvetlenül a megjelenése után már minden 8,5 másodpercben megkétszerezte a fertőzött gépek számát, és három percen belül elérte aktivitása csúcspontját, amikor is másodpercenként 55 millió adatcsomagot küldött szét az interneten. A Slammer terjedése két nagyságrenddel (!) gyorsabb volt a 2001 nyarán megjelent CodeRed vírusénál, amely átlagosan 37 percenként duplázta meg a fertőzött gépek számát.

Kimmo Alkio, az F-Secure Corporation alelnöke szerint még veszélyesebb és nehezebben detektálható vírusok fognak megjelenni. A vírusok Linux/Unix rendszereken történő terjedése, a nyílt forráskódot kihasználó támadások, az otthoni számítógépekbe való betörések egyre gyakoribbá válása, és az ázsiai vírusírók fokozódó aktivitása rengeteg munkát adott és ad az adatbiztonsággal foglalkozó cégeknek.

Eugene Kaspersky számítógépvírus-vadász, a Kaspersky Labs alapítója és vezető kutatója szintén pesszimista a várható helyzettel kapcsolatosan. Szerinte a vírushelyzet a rossztól a rosszabb felé tart. A jövőben több problémánk lesz a vírusokkal, de az informatika emiatt nem fog összeomlani.

Mit tehet a felhasználó?

Rengeteg számítógépen még mindig nem fut semmilyen vírusvédelmi program, és sok problémának pusztán ez az oka. A statisztikákat toronymagasan vezeti az elvileg könnyen detektálható Klez, de a figyelmetlen felhasználók miatt azóta is tömegesen terjed.

A Slammer/SQL vírus kapcsán az is nyilvánvalóvá vált, hogy sok cégnél nincs még (jól beállított) tűzfal – ott a tűzfalprogram naplófile-ja helyett már csak a hatásából, a net lassulásából vették észre a Slammer által okozott problémát.

Sor.	Szúrások	Érték	Vírusnév
1.		16.68	I-Worm.Klez
2.		8.75	I-Worm.Lexbin
3.		6.57	I-Worm.Sobig
4.		6.55	I-Worm.Aveton
5.		5.17	Macro.Word97.Thus
6.		3.13	I-Worm.Hybris
7.		2.46	I-Worm.Rbot.gen
8.		1.92	I-Worm.Tanatos
9.		1.25	Backdoor.NetDevil
10.		1.17	Macro.Word97.Saver
11.		0.95	I-Worm.Magistr
12.		0.85	Macro.Word97.Marker
13.		0.79	Worm.Win32.Opaserf
14.		0.76	I-Worm.KWorm
15.		0.72	Win95.CIH
16.		0.71	Trojan.Spy.SCKeyLog
17.		0.67	Backdoor.Death
18.		0.66	VBS.Redlof
19.		0.66	Win32.Elkern
20.		0.65	Win32.FunLove

2003. januári vírusstatisztika *(Forrás: Kaspersky Lab)*

A megfelelő védelmet a naprakész vírusvédelmi rendszer, valamint az operációs rendszerek és az alkalmazások gyártói által kiadott biztonsági frissítések telepítése, naprakészen tartása, a tűzfalak használata és megfelelő konfigurálása jelenti.

Emellett – különösen ha állandó netkapcsolatunk van – célszerű automatizálni és rövid intervallumot (60 perc) meghatározni a vírusismereti adatfile-ok frissítésére, így az új vírusismeret megjelenésekor az adatbázis azonnal frissül a számítógépünkön.

Aktuális havi kártevő: Lovgate

Névváltozatok: I-Worm.Supnot. Ez az új, hátsóajtó-komponenssel is felszerelt féreg Kínából indult pusztító útjára. Február 24-én megjelent legutóbbi, Lovgate.C nevű változata gyorsan terjed egész Ázsiában. A Lovgate féreg fertőzött e-mailekkel és a belső hálózatokon keresztül, a Windows megosztott mappáiban is terjed sokféle néven (Fun.exe, humor.exe, docs.exe, s3msong.exe, midsong.exe, billgt.exe, Card.EXE, SETUP.EXE, searchURL.exe, tamagotxi.exe, hamster.exe, news_doc.exe, PsPGame.exe, joke.exe, images.exe, pics.exe). A fertőzött levelek különféle témájúak lehetnek.

A Windows rendszerkönyvtárába is betelepszik WinGate.exe, WinRpcsrv.exe, syshelp.exe, winprc.exe és rpcsrv.exe néven – ezek futtatásáról különböző registrybejegyzésekkel gondoskodik. Emiatt a fertőzött gépen a féreg bármely szöveges file megtekintésekor lefut, bár ezt a felhasználó többnyire nem veszi észre, hiszen a Lovgate a Notepad alkalmazást hívja a TXT file-ok megjelenítéséhez.

Ezek után a féreg a Windows rendszerkönyvtárába menti károkozó rutinját, amelyet az alábbi file-ok hordoznak: ily.dll, task.dll és reg.dll. Ezek a programrészletek képesek a billentyűzeten begépelt adatok mentésére (keylogger funkció), file-okban is kutatnak jelszavak után. Az így összegyűjtött adatokat a féreg a win32pwd.sys és a win32add.sys file-ban tárolja, majd elektronikus levelezés (SMTP) vagy trójai program üzemmódban eljuttatja a féreg írójának, a hello _dll@163.com vagy a hacker117@163.com címre. A trójai üzemmód portszáma 10168 TCP, míg a féreg saját e-mailküldő rutinja által használt levelezőszerver címe smtp.163.com. Ez a mailserver egy hírhedt kínai spamküldő (kéretlen reklámlevél) portálhoz tartozik.

Végül a Lovgate féreg megkísérel fertőzött üzenet küldésével válaszolni minden beérkező levélre. Ehhez az Outlookot használja fel, de az ezzel kapcsolatos féregkódrészlet hibásnak tűnik, nem minden esetben hajtódik végre. A féreg átnézi még a hypertext formátumú (.HT* névkiterjesztésű) file-okat is, további levélcímeket keresve.

Az F-Secure és a Kaspersky Anti-Virus a 2003. február 24-i adatfile-okkal már képes detektálni.

További információ a weben a www.kaspersky.com és a www.viruslist.com címen érhető el. Aktuális vírusokra figyelmeztető friss hírek a www.2f.hu és www.virushirado.hu címen olvashatók.

A jó jelszó titka

Az aktuális kártevőként bemutatott Deloder féreg egyik jellegzetessége, hogy a hiányzó vagy fantáziátlan – „admin", „password", „123456" stb. – jelszavú számítógépeken egyszerű próbálgatásos módszerrel belépve megszerzi a rendszergazdai jogosultságokat.

Csizmazia István

Ennek kapcsán érdemes röviden megemlíteni néhány idevágó gondolatot a célszerűen megválasztott jelszavakról. A jelszavak alapvető célja, hogy kizárólag az adott jelszó birtokosa férjen hozzá, illetve gyakoroljon ellenőrzést valami felett. A nem megfelelően megválasztott és karbantartott jelszó veszélyforrás, míg a helyesen kiválasztott jelszó megakadályozza, de legalábbis erősen megnehezíti a jogtalan behatolást.

Helyes, ha a jelszó kiválasztásakor nem engedjük a felhasználó nevének, rokonai nevének, illetve egyéb személyi adatainak használatát – születési évszám, kutya neve stb. Ez túlságosan könnyen kitalálható lenne nemcsak a környezet számára, de az idegen próbálkozók is a névvariációkkal szokták kezdeni. A minimális hosszt is célszerű meghatározni, például a kiválasztott jelszó 6 vagy 10 karakternél ne lehessen rövidebb. A jelszófeltörő alkalmazások dolga a jelszó hosszúságával jelentősen nehezedik, exponenciálisan nő a feltöréséhez szükséges idő. Jó ötlet, ha a jelszóban vegyesen szerepelnek kis- és nagybetűk, valamint számok és más megengedett szimbólumok.

Helyes megközelítés, ha legalább a védendő értékek arányában fordítunk energiát a megfelelő jelszó kiválasztására, és biztosítunk erőforrást annak kezeléséhez. A kezelés itt nemcsak a választható jelszavak felügyeletét, hanem meghatározott időközönkénti rendszeres kicserélését, és a korábbi jelszavak esetleges újraválasztásának korlátozását is jelenti.

Bár ez nem szigorúan technikai kérdés, egy magára valamit is adó cég biztonsági szabályzatában a jelszavak kezelésének emberi támadhatóságát is alaposan körüljárják. Ebbe beleértendő nemcsak az, hogy jelszót nem szabad egyszerű sárga cetlire írva a monitor sarkára felragasztani, de az is, hogy ne engedjük, hogy a jelszó beírásakor bárki a hátunk mögül figyeljen. Fontos szempont továbbá, hogy a munkahelyről kilépő dolgozók hozzáférési

Sor.	Százalék	Érték	Vírusnév
1.		29.67	I-Worm.Klez
2.		9.91	I-Worm.Gobig
3.		7.04	I-Worm.Lentin
4.		3.12	Macro.Word97.Thus
5.		3.00	I-Worm.Aeron
6.		2.87	I-Worm.Ronon
7.		2.49	I-Worm.Hybris
8.		1.30	I-Worm.Tanatos
9.		0.90	Macro.Word97.Flap
10.		0.79	Macro.Word97.Saver
11.		0.71	Win95.CIH
12.		0.69	Worm.Win32.Opaserf
13.		0.76	Win95.Spaces
14.		0.59	Backdoor.Mniovck
15.		0.57	Backdoor.Antilam
16.		0.53	VBS.Redorf
17.		0.53	I-Worm.Blator
18.		0.52	Macro.Word97.Melissa
19.		0.51	Backdoor.Cqbk.Pro
20.		0.50	Macro.Word97.VMPC

2003. februári vírusstatisztika *(forrás: Kaspersky Lab)*

kódjait a legrövidebb idő alatt szüntessük meg, illetve az általa ismert jelszavakat haladéktalanul változtassuk meg, ezzel is elejét véve egy volt dolgozó esetleges kémkedésének vagy bosszúállásának.

A „social engineering" révén sok esetben meglepően könnyen ér el a hacker gyors eredményt. Tucatnyi érdekes tanpéldát olvashatunk a témakörben Kevin Mitnick nemrég megjelent The Art of Deception, azaz a Megtévesztés művészete című könyvében is.

Murphy egyik törvényével – mintegy összefoglalásként – jól jellemezhetjük a kérdést. Eszerint kifejezetten hasznos, ha van bennünk némi egészséges kételkedés: „Bízz embertársaidban, de azért emeld meg a kártyapaklit..."

Deloder

Névváltozata: W32.HLLW.Deloder.

A Deloder féreg olyan windowsos hálózati gépeket képes megfertőzni, amelyeknél az adminisztrátori account jelszó nélküli, vagy könnyen kitalálható a jelszava.

Kéretlenül telepíti a VNC nevű távfelügyeleti alkalmazást, megnyitva így a gépet a külvilág számára. Véletlenszerű IP címeket vizsgálva próbál nyitott 445-ös porttal rendelkező windowsos gépeket találni. A 445-ös port (Microsoft SMB megosztás TCP/IP segítségével) engedélyezi a kívülállóknak, hogy windowsos megosztásokat érhessenek el.

A legtöbb vállalati számítógépen központilag vagy helyben telepített tűzfallal védekeznek, amely képes lezárni ezt a portot. Ám a felhasználók zöme láthatónak hagyja meg a portot, és ezzel sebezhetővé válik, ha a helyi adminisztrátori jelszó nem megfelelően erős.

Ha a féreg alkalmas gépet talál, megpróbál helyi adminisztrátorként belépni, ehhez ötven könnyen kitalálható, sajnálatosan gyakori jelszóvariációt használ. Ha a bejelentkezés sikeres, a féreg különböző indítómappákba másolja be magát (rendszerint INST.EXE néven), és létrehoz egy registry-kulcsot, amellyel a DVLDR32.EXE file-t (ez szintén a féreg másolata) minden rendszerindításkor lefuttatja.

A gép újraindítása után a féreg további megfertőzhető gépek után kezd kutatni.

A fertőzés mellékhatásaként az is előfordulhat, hogy a korábban megosztott könyvtárakat nem tudjuk többé megosztani.

Az F-Secure és a Kaspersky Anti-Virus programok a 2003. március 9-i adatfileokkal már képesek detektálni.

●

Végezetül következzen a 2003. február havi vírusstatisztika. A százalék oszlopban az előfordulás gyakorisága olvasható. Továbbra is az I-Worm.Klez család vezeti a mezőnyt, a többieknek csak a „futottak még" kategória maradt. További információ a weben a www.kaspersky.com és a www.viruslist.com címen érhető el.

Az aktuális vírusokra figyelmeztető friss hírek a 2F honlapján rendszeresen olvashatók az alábbi címen: www.2f.hu és www.virushirado.hu.

Social Engineering

A social engineering érzékeny adatok megszerzésére irányuló olyan kísérlet, amelynek során a hiszékenységre építve, az emberek megtévesztésével, hazugság révén, vagy hamis személyazonosság felhasználásával manipulálják az adatok közelében dolgozókat.