EGY KIS VIROLÓGIA

Vírusfajták

Nem árt tudni, melyik, mire képes. Így a felismerésük is könnyebb.

Féregvírusok

A féreg egy olyan aprócska szoftver, amely a számítógépes hálózatok biztonságai réseit használja ki a terjedéshez. Miután bejutott a gépbe olyan számítógépeket kezd keresni, amelyeken szintén megvan a biztonsági hiba. Ezután ezekbe a gépekbe is behatol, és tovább másolja önmagát.

Hoaxok és lánclevelek

Ebben az esetben sohasem létezett vírusokról szóló lánclevelekről van szó, amelyek képtelen állításokat tartalmaznak (kikapcsolt gépet is megfertőző vírus és egyebek). A rémült alkalmazottak lelkesen küldözgetik fűnek-fának a figyelmeztetést, ami tényleg kivégezheti a levelezőszervert.

Trojan Horse

A trójai ló egy olyan program, amely az ismertető alapján nagyon hasznosnak tűnik, az ember letölti, de a beígért dolog helyett teljesen mást csinál – például letörli a merevlemez tartalmát. Valójában nem vírus, hiszen nem szaporodik, és a felhasználó megtévesztésével fejti ki romboló hatását.

Makrovírusok

MS Office programcsomag automatikusan betöltődő és elindúló makrói által használt Visual Basic for Applications programnyelven írt, platformfüggetlen vírusok.

Boot- és fájlvírusok

A fájl vírusok a végrehajtódó állományokat fertőzik meg, miközben a boot-vírusok a floppy vagy a merevlemez boot-szektorába írják be magukat. Emiatt minden indításnál garantáltan betöltődnek a memóriába. Az alaplapon bekapcsolható vírusvédelem miatt ma már nem képesek komoly károkozásra, egykor azonban futótűzként terjedtek.

E-mail vírusok

Az e-mail vírusok nevüknek megfelelően e-mailben terjednek – a fertőzött gép (MS Outlook) címlistáján szereplő címekre küldik el önmaguk másolatait.

Antivírus Centrum

Egy hely, ahol az elméleti tudnivalók mellett a védekezéshez is megtalálunk mindent, amire csak szükség lehet. Ideális kiindulópont.

www.virusinfo.hu

Email vírusok sajátosságai

Az E-mail üzenetekben terjedő (mass mailer) vírusok napjainkban egyre gyakrabban fordulnak elő. Jellemző rájuk, hogy igen rövid idő alatt képesek akár az egész világon elterjedni és az adott vírusra jellemző, változatos módszerekkel különböző károkat okozni. Jó példa erre, hogy a SirCam internetes féreg, amely mindössze hat nappal a 2001. július 18-i felfedezése után már az egész világon elterjedt és bizonyítottan a leggyakoribb károkozó programmá vált. A technikai ügyfélszolgálatok mostanáig már több tizezer bejelentést kaptak SirCam fertőzéses esetekről az USA, Franciaország, Kanada, Kína, Oroszország, Spanyolország, India, Nagy-Britannia, Németország, Lengyelország, Olaszország, Törökország, Argentína és sok más ország felhasználóitól.

A levelezéssel terjedő vírusokat általában Visual Basic nyelven készítik, a nagy méretük miatt esetleg pedig általában valamilyen .EXE tömörítővel (pl. UPX) zsugorítják őket.

A levelek szövege is igyekszik eloszlatni a felhasználók gyanakvását azzal, hogy az több előre megírt lehetséges variációból kerül kiválasztásra. A levelek mellékleteiben is ilyen sokféle változattalanságot tapasztalhatunkval találkozhatunk, de az is előfordul gyakori például, hogy a felhasználók kíváncsiságára (Kournikova, Britney Spears képeknek álcázott vírusok vagy barátiag ajánlott képernyővédőknek álcázott vírusok) vagy jóhiszeműségére építenek (az I-Worm-Gibe vírus egy Microsoft javítócsomagnak álcázott vírusza magát). építenek.

A vírusok levelezésen keresztüli terjedése a levelezéssel természetesen nem látható az Elküldött elemek (Sent items) mappában. Általában a regisztrációs adatbázisból kiolvasott SMTP levéltovábbító szerveren keresztül próbálják a ezeket magukat továbbítani, de olyan vírus is létezik, amelynek a saját SMTP rutinjait használja fel a terjedéshez (pl. I-Worm. Klez. E).

A működéshez szükséges átmeneti állományok neveit is igyekeznek valamilyen hasznosnak látszó vagy a Windows operációs rendszerhez tartozó névvel létrehozni, ezzel is segítve az álcázást.

Sokszor az MIRCmIRC-et használókat is felhasználják a terjesztéshez azzal, hogy módosítják az annak beállításait tartalmazó .INI állo-

A legújabb 5 Vírus

A W32/Gibe egy e-mailben terjedő féregvírus. A levél 'Internet Security update' tárggyal jön, és több oldalon taglalja angolul, hogy milyen hibákat javít ki a levélben csatolt **Q126309.EXE** fájl. A fájl teljesen úgy viselkedik mintha valóban egy biztonsági frissítést futtatnánk, még arra is figyeltek hogy ha többször akarjuk frissíteni, szól hogy az már megtörtént. A vírus maga nem tesz vagy okoz kárt, csak szaporodik és sajátmaga tovább küldésével lassítja Internetes kapcsolatunkat.

A VBS/Chick egy féregvírus ami képes terjedni e-mailben és IRC-n is. Megoróbálja azzal becsapni a felhasználót, hogy a csatolt fájlban egy híres popénekes képe van. A csatolt fájl egy 10 622 byte méretű .HTML (**BRITNEY.CHM**), és a levél tárgya 'RE: Britney Pics'. A csatolt állomány futtatásakor ActiveX installálást kér, és ha igent nyomunk a vírus elkezdi keresni a MIRC.INI, SCRIPT.INI fájlokat és ezeken keresztül tud terjeszkedni az IRC-n is.

A VBS/Numgame egy féreg, ami e-mailben terjed a fertőzött gép címlistája alapján. A vírus romboló része törli a hálózati meghajtók bizonyos könyvtárait, Registry bejegyzéseket és meghatározott kiterjesztésű fájlokat! A levél tárgya 'Are you **a cimzett neve** my valentine?', a csatolt fájlok: **GUESSGAME.HTML** vagy **GUESSGAME.VBE**. Futtatáskor egy játék indul el, miközben a háttérben megkezdődik a törlés.

A W32/Maldal, egy e-mailben terjedő féregvírus. A tárgy sokféle lehet és a csatolt állomány neve is véletlen generált .PIF kiterjesztésű fájl. Futtatáskor egy kis fekete alapú ablak jön fel, amin ha Exit-et nyomunk a vírus bemásolja magát a Windows/System könyvtárba **HYDE.PIF** és **ZACKER.PIF** néven és beleír a Registrybe. Kis idő elteltével a 'ZaCKer Is N YoUr MaCHiNe' felirat jelenik meg.

A W32/Yarner szintén egy féregvírus, de eltérően a többi hasonló féregtől nem használ Outlook alkalmazást, csak saját magát használja a terjedéshez. A levél feladója *'Trojaner-Info webmaster@trojaner-info.de'* a tárgy pedig 'Trojaner-Info Newsletter **aktuális dátum**'. A rendszer címlistájában lévő címekre kiküldi önmagát és az összes .php, .htm, shtm és .cgi kiterjesztésű fájlt amit talál, majd a vírus romboló része kitörli a C: meghajtón lévő összes éppen nem használt fájlt. A vírus a NOTEPAD.EXE fájlt átnevezi NOTEDPAD.EXE fájlra majd létrehoz egy vírusos NOTEPAD.EXE fájlt, és módosítja a Registry-t is.

mányt, és így a féreg elküldi magát minden olyan IRC csatornára, amelybe az adott felhasználó be van jelentkezve.

Majdnem mindegyikük létrehoz egy új kulcsot is a regisztrációs adatbázisban, melynek az a feladata, hogy minden rendszerindításkor a vírust futtassa., esetleg az Autoexec.bat vagy win.ini állományokba is beleírnak.

Egyre gyakrabban fordul elő, hogy támadást intéznek a gépen futó víruskeresők ellen is, megpróbálva azok futását leállítani (pl. I-Worm. Goner).

Az alkalmazott büntető rutinok is igen különbözőek legalább ilyen változatosak lehetnek: a levelek továbbküldésétől kezdve egészen a Windows könyvtár, vagy akár az összes meghajtó állományainak törléséig vagy roszszabb esetben szeméttel való felülírásáig (pl. I-Worm. Klez. E, VBS/Loveletter).

Mit tehetünk ellenük?

Az a tény, hogy SirCam ilyen gyorsasággal volt képes elterjedni, bizonyítja, hogy sok számítógép-felhasználó semmit sem tanult a korábbi világméretű számítógépvírus-járványokból. Nem ismerték fel a víruskereső szoftverek rendszeres frissítésének szükségességét és a levélmellékletek óvatos kezelésének fontosságát.

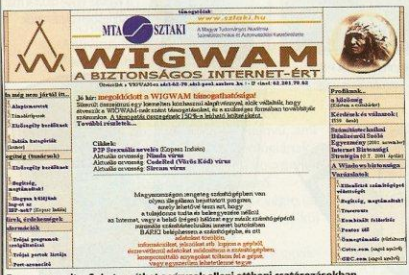
1. Ne nyissuk meg az ismeretlen feladótól, ismeretlen nyelven érkezett leveleket, hanem töröljük le azokat.
2. Legyünk gyanakvóak és figyelmesek akkor is, ha ismert feladótól érkezik mellékletet tartalmazó küldemény.
3. Ha Outlook Express levezőt használunk, akkor rendszeresen futtassuk le a szükséges javító állományokat, melyek a vírusok által kihasznált biztonsági réseket befoltozzák.
4. Mindenképpen használjunk valamilyen víruskereső programot és annak vírusismereti adatállományát naponta, de legalább hetente egyszer frissítsük.
5. Ha valamilyen levélben érkező programot mégis futtatni akarunk, azt előtte mentsük ki fájlba, ne közvetlenül a levélből indítsuk el.
6. Fontos állományainkról rendszeresen készítsünk mentést egy külön adathordozóra.

Csizmazia István
support@2f.hu (x)

A PANDA ACTIVESCAN ÁLTAL MEGTALÁLT VÍRUSOK RANGLISTÁJA FEBRUÁRBAN

Virus neve	Xxxxxxxx
W32/Badtrans.b	21,31%
W32/Klez.f	19,29%
W32/Sircam	6,19%
W32/Nimda	5,37%
W32/Disemboweler	4,55%
W32/MY PARTY	4,11%
W32/Hybris	3,83%
W32/Hai	2,52%
Magistr. B	2,30%
VBS/Help	1,81%

Az adatok természetesen időközben frissülhettek...



Egy magyar site. Sokat segíthet a vírusok elleni otthoni csatározásokban.

szítőinek nagy része középiskolás vagy egyetemista leendő programozó, aki pusztán a szórakozás kedvéért, vagy képessége csillogtatására készít vírusokat. Vannak olyanok, akiket az izgalom vonz – készíteni valamit, ami aztán elterjed, és jó (rossz) esetben bekerül a világ vezető hírei közé. Másokat a kihívás motivál – tehetséges, kiválóan képzett programozókról van szó, akik ellenállhatatlan szellemi próbatételnek tartják a vírusírást. Vannak olyanok is, akik a biztonsági résekre akarják felhívni a figyelmet. Az okok tehát szerteágazók, egy dolog azonban biztos: bár a vírusok valóban komoly veszélyt jelentenek, a vírusirtókat készítő cégeket sem kell félteni. Egy-egy járvány kitörésekor általában dollármilliárdokban mérhető károkkal riogatják az ügyfeleket, aztán rendszerint kiderül, hogy kissé túlbecsülték a dolgot.. **PCF**