VírusHíradó

Fokozódó szigor...

A számítástechnika rohamléptű fejlődése sajnos nem csak a gyorsabb processzorok, nagyobb tárolókapacitású merevlemezek és a fejlettebb szoftverek létrejöttében, hanem az egyre ravaszabb és kártékonyabb vírusok keletkezésében is megmutatkozik. 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-, videofájlok és egyéb adatállományok 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 büntetőrutinjának rövid leírását tesszük közzé.

I-Worm.Maldal
Névváltozatok: Keyluc, Zacker, CHRISTMAS.EXE, Reeezak

A féreg végigmegy minden helyi és hálózati meghajtón és hozzáfűzi a "DaLaL.htm" tartalmát minden egyes .HTM, .HTML és .ASP kiterjesztésű állományhoz. zek után a kártevő törli az alábbi kiterjesztésű álományokat: .LNK, .ZIP, .JPG, .JPEG, .MPG, .MPEG, .DOC, .XLS, .MDB, .TXT, .PPT, .PPS, .RAM, .RM, .MP3 AND .SWF.

Ezen művelet után a vírus lemásolja magát a törölt állományok nevén, de az eredeti névhez egy .VBS kiterjesztést fűz hozzá. égül, a kezdeti fertőzés után 30 perccel öt másodpercenként megkísérli a létező összes állomány törölését, megjelenít egy üzenet ablakot, majd bezárja a Windows-t.

I-Worm.Gigger
Névváltozatok: Gigger, Gigger.A@mm, IRC/Gigger.A@mm, JS/Gigger.A@mm

A féreg végigmegy az összes helyi és megosztott hálózati meghajtón, hozzáfűzve a víruskódot minden .HTM, .HTML és .ASP kiterjesztésű állományhoz.

Ha az adott könyvtár tartalmaz .INI vagy .HLP kiterjesztésű

fájlt, 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" állományt a vírus kódjával. Ezek után a féreg elküldi magát minden olyan IRC csatornára, amelybe a felhasználó be van jelentkezve.

Ha az aktuális dátum napjának értéke 1, 5, 10, 15 vagy 20, akkor a féreg az összes elérhető meghajtón az összes hozzáférhető állományt lecseréli egy nulla byte hosszúságú fájlra, így azok az eredeti tartalmukat elveszítik.

I-Worm.Klez.E
Névváltozatok: ElKern, Klaz, Kletz, I-Worm.Klez

A Klez vírus Magyarországon és világszerte is napjaink egyik leggyakoribb kártevője. A féreg minden páratlan hónap 6.-án az alábbi kiterjesztésű fájlokat semmisíti meg: TXT; .HTM; .HTML; .WAB; .DOC; .XLS; .JPG; .CPP; .C; .PAS; .MPG; .MPEG; .BAK; .MP3

A január és július hónapokban viszont (1, 7 hó) a teljes merevlemez minden fájlját véletlenszerű adatokkal írja felül. Ezek visszaállításra kizárólag csak mentésből van lehetőség!

I-Worm.Alcaul
Névváltozatok: Alcarys, W32/Alcarys@mm, W32.Alcarys@mm, Alcaul

Ennek a féregnek is igen veszélyes büntető rutinja van. Felülír minden .HTM, .HTML fájlt a rendszeren egy általa korábban létrehozott "c:dnserror1.html" állomány tartalmával.
Ezen kívül az összes .COM, .SCR, .WAV és .MP3 fájlt felülírja (kivétel a COMMAND.COM és a WIN.COM) saját magával. Az újonnan keletkezett .WAV és .MP3 állományokhoz .EXE kiterjesztést ad hozzá. Ezen felül a féreg megkísérli felülírni az alábbi nevezetes, vírusvédelmi programokhoz tartozó fájlokat:

- avpm.exe
- _avpm.exe
- avp32.exe
- _avp32.exe
- vshwin32.exe

I-Worm.MyLife.b
Névváltozatok: I-Worm.Mylife, Caric, Cari

A féreg tulajdonképpen egy PE EXE fájl, melyet Visual Basic-ben írtak. Programkódja ténylegesen 32 Kb hosszúságú, amely össze lett tömörítve az UPX program segítségével, így a féreg mérete 11 Kb.
A terjedési részében a féreg összegyűjti az összes levelezési

címet az Outlook könyvtárakból és a Windows címjegyzékből (Windows Address Book) és elküldi magát minden egyes címre.

Ha már sikerült megfertőznie a rendszert (a fertőzött gép újraindult), a féreg ellenőrzi az aktuális dátumot, és ha az órák száma egyenlő nyolccal, végrehajtja a büntető rutinját. Ez az alábbiakat törli:

- c:*.*
- d:*.*
- e:*.*
- f:*.*

Ezen felül törli a .SYS állományokat a Windows könyvtárból és a .VXD, .SYS, .OCX, .NLS fájlokat a Windows System alkönyvtárból, ezzel teljesen működésképtelenné téve a Windows-t.

Az F-Secure és Kaspersky Anti-Virus programok naprakész adatállományokkal minden itt ismertetett vírus jelenlétét felismerik.

Csizmazia István