Kinyílhatnak a hátsó ajtók

Nő az e-mailben érkező vírusok fenyegetése

Az e-mail-üzenetekben terjedő 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 károkat okozni.

A levelezéssel terjedő vírusokat legtöbbször valamilyen magas szintű nyelven, például Visual Basic vagy Visual C nyelven készítik, s nagy méretük miatt valamilyen .EXE tömörítővel zsugorítják össze. A vírust hordozó levél szövege, illetve a tárgy/subject mezője igyekszik eloszlatni a felhasználók gyanakvását azzal, hogy ezeket nagyszámú és változatos variációkból mindig véletlenszerűen választja ki. Ez építhet a felhasználó kíváncsiságára (Kurnyikova vagy Britney Spears-képek), ajánlhat képernyővédőt vagy valamilyen hasznos, esetleg vicces segédprogramot, de megtörtént, hogy a vírus látszólag a Microsoft nevében küldött „javítócsomagban" érkezett (I-Worm-Gibe) – állítja *Csizmazia István*, az IT-biztonsággal foglalkozó 2F 2000 Kft. szakembere.

Az is megtévesztően hathat, amikor a kártevő magát vírus elleni irtóprogramnak állítja be (I-Worm.Klez.H). Az ilyen vírusnál a levél szövegében a furfangos vírusíró még azt is leírja, hogy ne törődjünk vele, ha víruskeresőnk riasztana a mellékelt programra, ebben az esetben ez természetes, és hagyjuk figyelmen kívül a riasztást!

A vírusok levelezésen keresztüli terjedése nem látható az „Elküldött elemek/Sent items" mappában. Legtöbbször a regisztrációs adatbázisból kiolvasott úgynevezett SMTP levéltovábbító szerveren keresztül próbálják magukat továbbítani, de olyan vírus is létezik, amely a saját SMTP rutinjait használja fel a terjedéshez (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.

A vírusok sok esetben a csevegőszoftverek, például a mIRC használóit is célba veszik, úgy, hogy módosítják az annak beállításait tartalmazó .INI állományt, és így a féreg elküldi magát minden olyan IRC csatornára, amelybe az adott felhasználó bejelentkezett. Legtöbbször új kulcsokat hoznak létre a regisztrációs adatbázisban, melyeknek az a feladatuk, hogy minden rendszerindításkor lefusson a víruskód. Egyre gyakrabban fordul elő, hogy támadást intéznek a gépen futó víruskeresők ellen is, megpróbálva azokat hatástalanítani.

Az alkalmazott büntető rutinok legalább ilyen változatosak lehetnek: a károkozó fertőzött leveleket küldhet, a Windows könyvtár vagy akár az összes meghajtó állományait törölheti vagy rosszabb esetben bináris „szeméttel" felülírja (I-Worm.Klez.E, VBS/Loveletter). Ilyen esetben a sérült állományok semmilyen módon nem állíthatók helyre, csak a külön adathordozóra készült rendszeres mentésben bízhatunk.

Sok esetben egy adott időpontra időzítve történik a rombolás. A már említett Klez.E vírus például minden páratlan hónap 6-án a txt; htm; html; wab; doc; xls; jpg; cpp; c; pas; mpg; mpeg; bak; mp3 kiterjesztésű fájlokat semmisíti meg, míg januárban és júliusban a teljes merevlemez minden fájlját véletlenszerű adatokkal írja felül. A SirCam és a Klez.H vírus a fertőzött gép merevlemezén található dokumentumokat küldi tovább a vírussal együtt különböző címekre, így titkos vagy bizalmas információink kerülhetnek idegen kezekbe – figyelmeztet Csizmazia, aki szerint sűrűn előfordul, hogy a vírusok megpróbálnak egy hátsó ajtót nyitó (backdoor) programot telepíteni az áldozatok gépére, amelyen keresztül minden adatunk, winchesterünk tartalma kiszolgáltatottá válik a rosszindulatú vírusterjesztő számára.

(NAPI)

Automatikus archiválás

A vállalkozások többségénél, ahol a vállalati belső és külső kommunikáció alapját az elektronikus levelezés adja, megoldandó feladatot jelent az elektronikus kommunikáció révén felhalmozódott információtömeg tárolása. Erre nyújt megoldást az IBM által kidolgozott és a Synergon által is ajánlott Content Manager e-mail-archiváló rendszer. Ez a megoldás számos levelezési rendszerhez biztosít archiválási lehetőségeket. Üzeneteket, jegyzeteket, csatolt fájlokat és mappákat archivál hely- és költséghatékonyan, így több szempontból javul a vállalkozások belső információkezelése. A rendszer automatikusan archiválja a felhasználó által kategorizált állományokat a központi levelezési adatbázisba, mely a levelezési felületről is elérhető. A rendszer képes a csatolt állományok és a levelezési rendszeren alapuló alkalmazások kezelésére és archiválására is.