VírusHíradó

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 károkat okozni.

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 károkat okozni. Jó példa erre a SirCam internetes féreg, 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 több tízezer 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, nagy méretük miatt pedig általában valamilyen .EXE tömörítővel (pl. UPX) zsugorítják őket. A levek szövege igyekszik eloszlatni a felhasználók gyanakvását azzal, hogy az több előre megírt lehetséges variációból kerül kiválasztásra. A levél mellékletben is sokféle változattal találkozhatunk, gyakori például, hogy a felhasználók kíváncsiságára (Kournikova, Britney Spears képek vagy barátilag ajánlott képernyővédőknek álcázott vírusok) vagy jóhiszeműségére építenek (az I-Worm-Gibe vírus Microsoft javítócsomagnak álcázza magát).

A vírusok levelezésen keresztüli terjedése természetesen nem látható az Elküldött elemek (Sent items) mappában. Általában a regisztrációs adatbázisból kiolvasott SMTP levéltovábbító szerveren keresztül próbálják magukat továbbítani, de olyan

vírus is létezik, amely 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 a mIRC-et használókat is felhasználják a terjesztéshez azzal, hogy módosítják az annak beállításait tartalmazó .INI állományt, 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 legalább ilyen változatosak lehetnek: a levelek továbbküldésétől kezdve egészen a Windows könyvtár, vagy akár az összes meghajtó állományainak törléséig vagy rosszabb esetben szeméttel való felülírásáig (pl. I-Worm.Klez.E, VBS/Loveletter).

A már korábban említett SirCam vírus a fertőzött gép merevlemezén található véletlenszerűen kiválasztott dokumentumunkat küldi tovább a vírussal együtt különböző címekre. Még belegondolni is rossz, hogy ilymódon titkos vagy bizalmas információnk kerülhetnek idegen kezekbe. Végül, de nem utolsó sorban az is szinte gyakorlattá vált, hogy a vírusok megpróbálnak egy hátsó ajtót nyitó (backdoor) programot telepíteni az áldozatok gépére, melyen keresztül minden adatunk, winchesterünk tartalma kiszolgáltatottá válik a rosszindulatú vírusterjesztő számára.

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.

- Ne nyissuk meg az ismeretlen feladótól, ismeretlen nyelven érkezett leveleket, hanem töröljük le azokat.
- Legyünk gyanakvóak és figyelmesek akkor is, ha ismert feladótól érkezik mellékletet tartalmazó küldemény.
- Ha Outlook Express levezőt használunk, akkor rendszeresen futtassuk le a szükséges javító állományokat, melyek a vírusok által kihasznált

biztonsági réseket befoltozzák.
- Mindenképpen használjunk valamilyen víruskereső programot és annak vírusismereti adatállományát naponta, de legalább hetente egyszer frissítsük.
- Ha valamilyen levélben érkező programot mégis futtatni akarunk, azt előtte mentsük ki fájlba, ne közvetlenül a levélből indítsuk el.
- Fontos állományainkról rendszeresen készítsünk mentést egy külön adathordozóra.

Csizmazia István