FIATAL MŰSZAKIAK TUDOMÁNYOS ÜLÉSSZAKA

Kolozsvár, 2003. március 21-22.

SZÁMÍTÓGÉPES VÍRUSOK

Garaguly Kálmán, Tomka Ildikó

Mi is a vírus?

Olyan program, ami

- engedély nélkül hatol be a rendszerbe
- szaporodik
- kárt okoz(hat)

Részei:

- reprodukciós rutin
 - o polimorf vírus: állandóan változtatja az alakját
 - o permutációs vírus: a program részei változó sorrendben jelennek meg
- aktiválási mechanizmus
 - o egy bizonyos feltétel teljesülése esetén
 - péntek 13-a van
 - az operációs rendszer Windows 98
 - nincs telepítve egy javítás
- romboló egység
 - o beférkőzés a rendszerbe
 - o rendszerinformációk megszerzése és továbbküldése
 - o fájlok megfertőzése, törlése, tartalmuk felülírása, kiterjesztésük átírása
 - o bizalmas adatok (pl. jelszavak) továbbküldése e-mailben
 - o csak közvetve okoz kárt (annyi példányban küldi tovább magát e-mailben, hogy az internet forgalma lelassul)

Vírustípusok

Rendszervírus

A rendszervírusok megfertőzik az MBR-t (Master Boot Record) és/vagy a FAT-táblát (File Allocation Table).

Előbbi a merevlemez azon része, ami a gép indításakor elsőként töltődik be. Rendszerinformációkat tartalmaz (mint például az operációs rendszerre vonatkozó utasítások), és mivel ezek az információk képezik a gép működésének alapját, ezt a vírust valamivel nehezebb kiirtani, mint a többi. Mivel minden vírusirtó program a rendszer elindulása után indul, a legtöbb feltételezi, hogy az MBR-nak semmi baja, - hiszen anélkül ő sem működne -, így nem is ellenőrzi. Egyes rendszervírusok úgy változtatják meg az MBR-t, hogy az fdisk-mbr utasítás (ami normális esetben törölné az MBR-t) a merevlemez tönkremenetelét okozza.

A FAT-táblában szerepel minden, a merevlemezen található fájl neve és holléte. Ha egy vírus megtelepszik a merevlemez egy szektorában, átírhatja a FAT-táblát, hogy minden név órá mutasson; vagy a fájlneveket nem változtatja meg, épp csak felülírja a tartalmukat, mint a HalfLife vírus.

Programvírus

Más programokhoz kapcsolatosan érkezik, vagy csak egymagában. Ha egyszer aktivizálódott, szinte bármit megtehet - fájlműveletek, jelszavak feltörése és elküldése e-mailben, fájlok megfertőzése és egy e-mail csatolt fájlaként való továbbküldése.

Ha egy programvírus lopakodó üzemmódba vált, viselkedhet egyszerű lopakodóként - ránézésre a fertőzött fájl mérete nem változott, de megnyitáskor már észrevehető a különbség -, vagy teljesen lopakodóként - nem lehet észrevenni a fájl méret változását.

A Magistr.b vírus példának okáért megsemmisíti az összes helyi és hálózati meghajtón található fájlt, elrontja a CMOS memóriában és a FLASH BIOS mikrochip-ben tárolt adatokat, még az operációs rendszert betöltő WIN.COM-ot és NTLDR-t is felülírja oly módon, hogy bizonyos körülmények teljesülése mellett, a számítógép következő indításakor, a helyi és a hálózati meghajtókon tárolt összes adatot letörli. Miközben a vírus olyan fájlok után kutat, amiket megfertőzhet, megsemmisíti a .NTZ kiterjesztésűeket. Ha a Magistr.b a "ZoneAlarm" személyi tűzfal szoftvert aktívknak találja a memóriában, azt automatikusan kikapcsolja.

Makróvírus

A makró egy névvel rendelkező, ismételhető utasítássorozat, hasonló a batch (.bat) fájlokhoz. A leggyakrabban a Microsoft Word és Excel használja. A makróvírusok működését némiképp nehezíti, hogy egyes utasítások csak az adott nyelven (angol, magyar,...) értelmezhetőek.

Makrókat csak sablon tartalmazhat (.dot), de mivel a Word felismeri dokumentum-kiterjesztéssel is (.doc), ez ritkán jelent akadályt. Egy szövegfájlra senki sem gyanakodna, így viszonylag könnyen terjed.

Elsődleges célpontja általában a Normál.dot (a Word indulásakor automatikusan betöltődő sablon). Ezután - bár viszonylag korlátozott utasításkészletből kell megélnie - képes átdefiniálni bizonyos utasításokat (pl. *FileSave*), alkalmazásokat hívhat vagy szüntethet meg, fájl műveleteket végezhet; akár saját magát is meghívhatja a parancssorból (*winword/<rnakrónév>*), valamennyire beleszólhat a rendszer működésébe (törölhet automatikus rutinokat).

Ha csak programon belül garázdálkodik, megváltoztat néhány szót, jelszóval látja el a dokumentumokat (ami zavaró lehet, ha épp nincs olyan valaki a közelben, aki fel tudja törni), esetleg nyomtat.

A W97M.Thus nevű makróvírus saját makróit másolja a fertőzött dokumentumba, ráadásként december 13-án törli a c: meghajtóról az összes állományt.

Egyéb kártékony programok

Trójai programok

Hasznosat is tesznek, de nem várt „mellékhatásaik” is vannak (megfelelő körülmények közt szabadon engednek egy vírust; miközben kiirtanak egy vírust, átírnak egy rendszerfájlt).

Vírushordozók és -generátorok

- injektor: fertőz, bár ő maga nem fertőzött
- germ: normális úton nem terjedőképes vírusokhoz
- dropper: indításakor vírust generál, majd szabadon ereszti; ő maga ártalmatlan

Programférgek

Szaporodnak, kárt okoznak, de mindezt hordozóprogram nélkül.

A Slapper (Ütő) egy Linux hálózati környezetben terjedő féreg, amely egy 2002. augusztusában felfedezett OpenSSL könyvtárbeli hibát használ ki. A férget először 2002. szeptember 13-án, pénteken

Kelet-Európában észlelték. A féreg azokat a gépeket veszélyezteti, melyeken Apache web server fut OpenSSL támogatással. Ez elég sok gépet érinthet, nagyjából a nyilvános Internetes webszerverek 60%-át. Ha egy gép megfertőződik, a féreg elkezd terjedni további gépekre. Ezenfelül a féreg kódja megvalósít egy peer-to-peer hálózati támadást is, ahol a fertőzött gépeket távolról lehet DDoS (Distributed Denial of Service) típusú támadásra kihasználni.

„Viccés” programok

Ártalmatlan programok, nem titkolt céljuk a felhasználó halálra rémítése. Egy jellemző példa rá a Jep/Russ nevű program, ami - miután úgy tett, mintha megkérdezte volna a felhasználót, hogy akarja-e - úgy tesz, mintha letörölné a Windows rendszerkönyvtárát.

Védekezés

1. Megnehezíteni a vírusok számára a behatolást

- Folyamatosan figyelő vírusellenőrző program
- Tűzfal
- A vírusellenőrző program adatbázisának gyakori frissítése
- Ismeretlen, megbízhatatlan forrásból származó állományok elkerülése (messzire)
- Szükségtelen alkalmazások használatát kerülni
- Frissítések, j avítások telepítése

2. Megnehezíteni a vírusok elterjedését

Ha egy elszánt vírus szabadul be egy megfelelő védelem nélküli gépre, és letöröl mindent, csak az segíthet, ha van biztonsági másolat.

A Windows és a Unix között a nagy különbség a jogosultságok szabályozásában és a biztonsági rések számában van.

Míg egy Windows-felhasználót könnyen megfertőzte az ILOVEYOU vírus (az e-mail program automatikusan futtatta a csatolt állományban levő .vbs kiterjesztésű fájlt), a Unixot használókat ez nem érintette, hiszen az ő levelezőprogramukban nincs ilyen lehetőség, éppen az efféle fertőzések elkerülése érdekében.

A felhasználói jogosultságok pontos behatárolása szintén sok vírus számára akadályozza meg a továbbfertőzést - ha egy átlagos felhasználó fertőzött alkalmazást indít el, az nem tud átmenni más

felhasználókhöz, hiszen a program futtatójának jogait örökölte, márpedig egy átlagos felhasználónak csak a saját könyvtárához van joga.

A Unix gyenge pontja a rendszergazdai jogosultsággal rendelkező felhasználó - azaz a rendszergazda. Ha ő indít el egy fertőzött programot, az.az.ő (mindenható) jogosultságait kapja, így bárkit megfertőzhet azon a gépen, vagy más, távoli gépeket is, ha azok megbíznak a fertőzött gépben.

Egy jelszó sokat érhet a vírusok elleni harcban - minél nehezebb megfejteni, annál jobb. Ha legalább 12 karakter hosszú, részenként sem értelmes kis és NAGY betűkből, számokból és speciális karakterekből (/ % & #) áll, nagyon nehéz megfejteni, tehát azok a vírusok, amelyek netán ezt szeretnék tenni, nem tudnak vele mit kezdeni.

3. Tökéletes biztonság nincs

Legfeljebb egy soha be nem kapcsolt gép lehet teljes biztonságban, de mivel ennek nincs értelme, igyekezni kell a lehető legbiztonságosabbá tenni a gépeket a fent felsorolt módszerekkel.

Bár a Windows a legtöbb (sikeres) támadás célpontja, és Japánban a Linux-klónokon kívül leginkább Windowst használnak, ott mégsem akkora probléma a vírustámadás, mint másutt - merthogy rendszeresen telepítik a javításokat, és kellően óvatosak.

A vírusirtó cégek legtöbbször egy-két órával, legkésőbb egy nappal a vírus megjelenése után már közlésezik a vírusirtó frissítését, a vírus kiirtására vonatkozó tanácsokkal együtt, a helyzet tehát nem reménytelen.

Felhasznált irodalom:

- www.index.hu
- www.virushirado.hu
- Kaspersky Labs/www.viruslist.com

vissaiifgthotmail.com, kalmv@netposta.net