Vírusok, férgek, trójai falovak és egyéb programozott kórokozók

Az alábbiakban olyan programokkal, programkódokkal foglalkozunk, melyet ártó szándékkal (beleértve az illetéktelen elérést is) hoztak létre, vagy kísérletezésből, játékból születettek, de veszélyt jelentenek és kárt okozhatnak. Az ilyen kódokat 'vandalware' szóval is illetik, mely roppant találó, bár nem elterjedt. E programok sajátos csoportját alkotják a vírusok és a férgek (worms), melyek sajátsága, hogy aktivizálódva reprodukálódhatnak, s egy rendszerben vagy számítógépek közt terjedhetnek. Bár számos más csoport is idetartozik, ezek közül csak a trójai falovakat (Trojan Horses) tárgyaljuk. Említjük a bombákat (bombs) és a csapóajtókat (hátsó ajtó - trap door, back door), melyek, mint az előzőek 'alkatrészei' érdekesek.
Az egyéb csoportok jelentősége nem kicsiny, de nem a nyílt hálózatok (Internet, BBS[i]-ek) esetében, vagy túl speciális kérdés lenne tárgyalásuk. A vírusokban, férgekben és trójai falovakban még két közös vonás van, ami a közös tárgyalásukat indokolja:
- a hasonló károkozás;
- az ellenük történő védekezés hasonlósága, mely a terjesztés- és terjedésbeli rokon vonásokból fakad.

Vírusok

A vírusokra több definíció használatos. Szűkebb értelemben (mi mindig így használjuk) a vírus egy programkód, mely önállóan működésképtelen, melyet program vagy program információs file tartalmazhat, a program végrehajtásával aktivizálódik és replikálja magát, hozzáfűzi vagy beleírja magát más programokba.
A vírusokat rendszerint ártó szándékkal hozzák létre (bár kísérleti vagy játék célból is születtek). Általában az észrevétlen terjedés érdekében rejtettek, károkozásukon kívül nehezen vehetők észre (segédeszközök nélkül). Gyakran bombákat tartalmaznak, egyesek képesek más vírusokkal interakcióba lépni.
A vírusok nem hatásosak, ha nem kerülnek végrehajtásra. Ezért a másolás s minden más, végrehajtás nélküli tevékenység veszélytelen velük. Adatfile-t nyugodtan beolvashatunk rendszerünkbe (feltéve, ha nem tartalmaz program információt valamely végrehajtandó program számára). Léteznek vírusok ill. vírusszerű kreálmányok, melyek bootlemezről a bootkóddal aktivizálódhatnak, így fertőzött lemezről a bootolás veszélyes.
Hasznos tudnunk, hogy csak az egyfelhasználós rendszerek ellen bocsátottak szabadon vírusokat (PC-s DOS és Windows, Macintosh System, Amiga és Atari OS , ...). Unix-ra írtak, de csak kísérleti célból, VMS[ii]-re, mainframe-re nem ismeretes vírus (bár a szakirodalom említ ilyeneket, ezek nem vírusok a mi definíciónk értelmében). NetWare alatt futót soha senki nem írt, tudtommal. OS/2-re létezik. NT-re (szintén tudtommal) nincs. Olyan vírus sem ismeretes, amely több operációs rendszer alatt is működőképes lenne. Bár többfelhasználós rendszerekre lényegében nincsenek vírusok, ez nem zárja ki, hogy DOS vagy Windows emuláció alatt vírusok nem aktivizálódhatnak, replikálódhatnak, sőt akár károkat is okozhatnak - pl. a Word makró vírusok -, de ezek operációs rendszer szinten már nem veszélyesek.

Férgek

A férgek - ellentétben a vírusokkal - önálló programok. Máskülönben hasonlóak a vírusokhoz. Férget sokkal kevesebbet írtak mint vírust, s mivel ezek hálózaton át terjednek elsősorban, ezért a többfelhasználós rendszerek az elsődleges célpontjaik. Híres példa az Internet 1988-as féregfertőzése (az Internet Worm). Az első férgeket kísérleti jelleggel, hasznos célra hozták létre. Céljuk az akkor szűkösen elérhető számítógépes erőforrások feltárása és kihasználása lett volna. A gondolat azóta is kísért, bár nem erőforrás, inkább információgyűjtés (pl. WWW-n - vigyázat a WWWWorm nem féreg!), hibaelhárítás és hálózatmenedzsment célból. Számos DOS-os féreg van, amit rendszerint vírusként emlegetnek.
A férgek potenciálisan nagyobb veszélyt jelentenek. Az ismert vírusok elterjedése hamar korlátokba ütközik, s a terjedési sebesség is kisebb annál, hogy ne lehetne hatékony riasztást és védelmet alkotni. Persze elvben egy féreg terjeszthet vírust is, s így már egy vírus is kemény dió lehet, de ezt az ötletet a vírusírók még nem használták ki. Mindazonáltal a mondottak a jelen pillanatban érvényesek, s nem elvi korlátok. Meglepő lehet, hogy az 1988-as Internet Worm eset óta nem következett be súlyos féregfertőzés az Interneten. Ez részben az 1988-as intézkedéseknek köszönhető, részben a szerencsének. Talán az Internet globális biztonsága lépést tart a támadókkal.

A trójai falovak

A trójai falovak olyan kódok, programok, melyeket más programba rejtettek. Ilyen értelemben a vírusok is trójai falovak, de a trójai falovak nem feltétlenül vírusok. A trójai falovon inkább olyan programot szokás érteni, mely hasznos programnak látszik, vagy valamely más hasznos/ismert program preparált változata. Sokkal könnyebb trójai programot készíteni, mint vírust vagy férget, sokkal jobban is lehet álcázni, inkább a terjesztése nehézkes.

Bombák

A bomba egy programkód, melyet valamely más program tartalmaz, s valamely feltétel (idő, esemény, vagy ezek kombinációja) hatására, vagy távvezérléssel 'robbannak', 'robbanthatók'. A fenti programozott kórokozók sokszor tartalmaznak ilyeneket, emellett szoftver másolásvédelemben, (shareware, bérelt stb.) szoftver hatástalanítására alkalmazzák. Ez utóbbi bombák csak az aktuális szoftver hatástalanítására szolgálnak.

Csapóajtók

A angol nyelvű biztonsági irodalom a 'trap door' és a 'back door' kifejezéseket használja rejtett kiskapuk meghagyására, létrehozására, melyen az illegális behatoló bejuthat vagy újra visszatérhet a rendszerbe. Az angol 'trap door' egyik hétköznapi magyar megfelelője a 'csapóajtó', a 'back door'-é pedig a 'hátsó ajtó'. (Utóbbi félrevezető lehet, a 'hátsó ajtó' kifejezést a magyar nem ismeri. Talán a 'kiskapu' jó lenne, de ez érzelmi töltéssel bír. Így jobb híján maradunk itt is a csapóajtónál).

Csapóajtót hagyhat maga után a korábban legális eléréssel rendelkező felhasználó, egyszer illegálisan hozzáférést szerző személy, de csapóajtók telepíthetők trójai falovakkal, férgekkel és más módokon is. Sőt, programhiba, konfigurálási hiba folytán rendszerünkön eleve lehet csapóajtó. Értelemszerűen a rendszerek ellenőrzésének ki kell terjedni az esetleges csapóajtók feltárására is. Ilyen célra számos szoftvert írtak, de kényszerű okokból ezek operációs rendszer és alkalmazás specifikusak, valamint használatuk szakértelmet igényel.

Védekezés

Az alábbiakban csak a vírusok elleni védekezéssel foglalkozunk, de nem azért mert a vírusok általunk kitüntettek lennének, hanem mert a védekezés más jószágok ellen is nagyban hasonló. Sőt, a vírusok a legártalmatlanabbak a fent említett lények közül. A mai napig nem írtak jelentős veszélyt jelentő vírusokat (a vírusírás messze elmarad a technikai lehetőségek mögött - nincs számítógépes megfelelője az AIDS-nek, az Ebolának és az influenzának). Mindemellett könnyen átláthatók és kivitelezhetők a védekezés módjai.

A védekezés alapja, hogy tudnunk kell, mi ellen védekezünk, milyen veszélyekkel nézünk szembe. A vírusnak valamely módon be kell kerülnie rendszerünkbe, így az izoláció teljes védelmet jelent, persze ilyen árat nem akarunk fizetni a hatásos védelemért.

A következőkben a vírusvédelem legfontosabb teendőit pontokba szedtük. Először az egyéni (pl. otthoni) gépek, majd a helyi hálózatok felhasználóinak védelmével foglalkozunk. Megjegyezzük: tökéletes védelem nincs, de hatásos igen.

(Helyi) hálózatba nem kapcsolt gépek esete

1. A vírusok adatvesztést, ill. a szoftver károsodását okozhatják. A szoftver károsodása is kellemetlen, hiszen sok esetben újra kell installálni rendszerünket, s ez pl. floppy-ról bosszantóan időigényes lehet, vagy önerőből nem is tudjuk végrehajtani. Adatainkat nagy baj nem érheti, ha rendszeresen mentettünk, s mentésünk nem vírusfertőzött. Elvben (volt rá példa a gyakorlatban is) vírus hardver károsodást is okozhat, de ennek veszélye rendkívül csekély. A szoftvereink visszatelepítése újrafertőzés nélkül lehetséges, hiszen installáló lemezeink írásvédettek (bár az írásvédelem esetleges hardver hiba miatt nem garantált). Adataink vírusmentességét az biztosíthatja, hogy végrehajtható kód kell a vírusfertőzéshez, s ha ilyen nincs a lemezünkön, akkor fertőzöttek sem lehetnek adatállományaink. A kritikus adatállományainkat tartalmazó floppy lemezeinket - pl. egy Unixos gépen - átmásolva érintetlen lemezekre, azok vírusmentessége már garantált (igaz, hogy ez esetleg önerőből nem megy).
2. Víruskereső szoftverrel rendszeresen ellenőrizzük állományainkat, a kapott új állományokat is. A víruskereső szoftver legyen naprakész. Esetleg használhatunk ún. rendszerintegritást ellenőrző szoftvereket, de ez nem kötelező.
3. Legyünk óvatosak, ellenőrzött és ismert helyről szerezzünk be szoftvert (persze a kereskedelmi forgalmazás nem garancia).
4. Fogadjuk fenntartással, ha valaki pénzes vírusvédelmet, vírusvédelmi kártyát akar ránk sózni. Ezek önmagukban nemigen hatásosak, valamint vakriasztásokat okozhatnak.
5. Az OS/2 HPFS vagy az NT file-rendszer meglehetősen védett, Unix, VMS, NetWare ellen még nem került forgalomba vírus. Természetesen DOS-os (Mac stb.) vírusok előfordulhatnak ilyen file-rendszerekben is, csak nem képesek aktivizálódni a számukra idegen operációs rendszer alatt.
6. Ismételt vírusfertőzéseket a lemezeinken elfekvő vírusok okozhatnak.

7. Ha megtehetjük, a lemezeknél hatékonyabb mentő/archiváló berendezést szerezzünk be.

Védekezés helyi hálózatokon

Helyi hálózatokon a fentiek közül minden eszközt alkalmaznunk kell, de ezeknél többet is, valamint a lehetőségeink is szélesebbek. Itt a fő cél a vírusbekerülés potenciális útjainak ellenőrzése, valamint a központi ellenőrzés.

A tennivalók és lehetőségek:

1. Legyen vírusvédelmi politika, kapjanak vírusvédelmi útmutatást a felhasználók. Valósuljon meg együttműködés az érintettek között a vírusvédelemben (riasztás, tájékoztatás stb.).
2. Korlátozzuk a fertőzés útjait. Egyes helyekről kiszerelhetjük a floppy meghajtókat, sőt remote boottal diszknélküli üzemmódot használhatunk.
3. Szerverekről futtassuk alkalmazásainkat.
4. Használjunk központi file-szervereket és központi mentést, a mentéseket és a file-szerverek állományait ellenőrizzük, a file-szerverre másolt vagy módosított program azonnal kerüljön ellenőrzésre.
5. Ne DOS/Windows környezetet alkalmazzunk, ha lehetőségünk van másra. Ha a fentiek alapján megfelelő gondossággal járunk el, a vírusfertőzéseket gyakorlatilag kiküszöböljük. Ha nincsenek kritikus alkalmazásaink (nem lehet munkaidő kiesés), akkor a helyi hálózatokon annyi baj sem lehet, mint az otthoni felhasználóknál, hiszen a visszaállítás a file-szerverekről pillanatok műve. (Persze rosszul menedzselt rendszerekre ez nem áll!!!).

A tapasztalat azt mutatja, hogy az áttérés a helyi hálózatra az egyedi PC felhasználásról, lényegesen csökkentheti a vírusfertőzések számát. Ez annak köszönhető, hogy nem fekszenek el vírusok hajlékonylemezeken, az ellenőrzés kiterjed a felhasználók állományaira, a file-ok nagy része megfordul a központi file-szervereken, a vírusvédelmi szoftver szétosztása és frissítése gyorsabb és szélesebb körű, a szoftverek telepítése tiszta forrásból történik. Bár a hálózat bevezetése számos új biztonsági probléma forrása, itt egy példa arra, hogy a biztonsági problémák megoldásában is lehet szerepe.

BBS-ek és anonymous FTP helyek

Mind az üzemeltetők, mind a felhasználók számára sok biztonsági problémát vetnek fel a szabad (nyilvános) elérésű archívumok, mint pl. BBS-ek és anonymous FTP helyek. A gondok nagy része csak az üzemeltetőket érinti közvetlenül, ezekkel itt nem foglalkozunk.

A problémák egyik fő forrása, hogy e helyek vírusok és más programozott kórokozók terjesztői lehetnek. A nevesebb FTP helyek archívumai, cégek support FTP helyei nagyon jól ellenőrzöttek, gondosan megválogatják, hogy honnan kerülhetnek ide programok, valamint az üzemeltetők minden tőlük telhetőt megtesznek az ellenőrzésre. Tökéletes védelem azonban nincs, a vírusok ellen a szigorú ellenőrzés még csak hatásos, de trójai falovak időnként felbukkannak.

A felhasználó részéről a védekezés a következő lehet:

- nem tölt le programot;
- a programokat izolált környezetben teszteli (karantén);
- gondosan tesztel vírus azonosító szoftverekkel;
- szoftvert csak hivatalos disztribúciós helyéről vagy ennek hivatalos (vagy más szempontok miatt biztonságosnak tekintett) tükör (mirror[iii]) helyeiről tölt le.

Látható, hogy csak az utolsó pont az, amit igazán követhetünk. Megjegyezzük, hogy a vírusellenőrzést nevesebb archívumok, disztribúciós helyek esetén nem tartjuk elengedhetetlennek. A vírusfertőzések elenyésző töredéke vezethető vissza anonymous FTP-ről letöltött file-okra.

A nyilvános elérésű helyekhez hasonló a helyzet a különféle helyi archívumokkal. Sajnos általános útmutatót nem lehet adni arra, hogy mely archívumok tekinthetők biztonságosnak, s melyek nem.

Egyes archívumokba bárki tölthet fel file-okat. Ha ezek az állományok azonnal nyilvánosan elérhetők, akkor ezek biztonsága kétes (a beérkező file-on legfeljebb azonnali automatikus vírusellenőrzés futtatható).

---

[i] **BBS** (Bulletin Board System): elektronikus faliújság, ahol közérdekû információk helyezhetõk el, illetve olvashatók; szûkebb értelemben a telefonhálózaton elérhetõ - jórészt amatõr üzemeltetésû, PC-ken mûködõ - számítógépes szolgáltatás (file-archívum és kommunikációs fórum)

[ii] **VMS** (Virtual Machine System) virtuális gép használatát biztosító operációs rendszer elsõsor-ban a Digital Equipment VAX és MicroVAX gépein

[iii] **mirror** valamely népszerû Internet információforrásról készített (és rendszeresen frissített) teljes másolat egy (általában földrajzilag távol levõ) másik szerveren; a tükrözéssel csökkenthetõ az eredeti szerver és az interkontinentális vonalak terhelése, ha a felhasználók a hozzájuk legközelebb esõ mirrort használják