Malwarek

http://www.commoncraft.com/video/computer-viruses-and-threats-hu

Az angol **malware** kifejezés az angol **mal**icious soft**ware** (*rosszindulatú szoftver*) összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit). A számítógépes kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el. Az ellenük való védekezés a köznyelvben víruskereső programnak nevezett szoftverekkel történik.

Trójai programok

Olyan program, ami látszólag hasznosat vagy érdekeset csinál, de káros program(ok) számára „kaput” nyit az általunk használt eszközön. Nevét az Odüsszeia eposzból ismert trójai faló után kapta. A trójai programok nem szaporodnak és önmagukban (szándékosan) ártalmatlanok, hogy a víruskereső programok ne találják meg őket.

Programférgek

Egy **számítógépes féreg** *(worm)* egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. A férgek gyakran a számítógép-hálózatokat használják fel terjedésükhöz.

A Unix rendszerek biztonsági rését kihasználó programok. Céljuk általában az információszerzés (pl. jelszótáblák, tűzfal). Nem irtották őket, hanem javították az operációs rendszer hibáit így nem terjedtek el. A programféreg szaporodik, de nem igényel hordozót.

Az első férget 1978-ban készítette el a Xerox PARC két kutatója.

Vírushordozók

Vírushordozók, vagy vírustároló programok.

- Injektor, a "vírusgazda", ő maga nem beteg, de fertőz.
- Dropper, indítás után előállítja a vírust, majd szabadon engedi. A Dropper nem kártékony, róla nem készül másolat.

Vírusgenerátorok

Eredetileg az assembly kód módosítása. Csak a "termék" kártékony.

A **számítógépes vírus** olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Többnyire rosszindulatú, más állományokat használhatatlanná, sőt teljesen tönkre is tehet.

Ransomware (zsaroló vírusok)

Ezeknek a programoknak a célja az anyagi haszonszerzés. Az áldozat (victim) számítógépén található fájlokat titkosítják, majd pénzt kérnek azok feloldásáért, általában olyan lenyomozhatatlan módokon, mint pl.: Ukash utalványok.

Bankoló vírusok

A fertőzött gépeket egy botnetbe kapcsolják, és rögzítik a billentyűleütéseket és az egyéb internetes adatforgalmat. Céljuk a banki jelszavak és hitelkártyaadatok megszerzése. A lopott adatokat később a feketepiacon értékesítik. Ilyen pl.: a ZeuS vagy a Spy Eye botnet.

ANSI bombák

Az ANSI bombák nem szaporodnak. A víruskód szöveges állományban van, aktiválni egy batch fájl segítségével lehet.

A **spam** (ejtsd: *szpem*) a fogadók által nem kért, elektronikusan, például e-mailen keresztül tömegesen küldött hirdetés, felhívás vagy lánclevél.

Az így kapott információk a fogadók túlnyomó része szempontjából érdektelenek, így fölösleges sávszélességet, tárhelyet, szellemi ráfordítást igényelnek a fogadótól. Mivel a spameket a feladóik milliós nagyságrendben képesek rövid idő alatt kiküldeni, ez jelentős terhelést jelent az internet használói számára. A spamek egy része tudatosan megtévesztő, a fogadó kihasználására törekszik (olcsó, nagy nyereséget ígérő befektetésre csalogató, piramisjátékra csalogató, banki azonosítókat, személyes adatokat különféle indokokkal megkérő levelekkel).

Kémprogramnak (angolul spyware, ejtsd: szpájver) nevezzük az olyan, főleg az interneten terjedő számítógépes programok összességét, amelyek célja, hogy a felhasználó tudomása nélkül megszerezzék a megfertőzött számítógép felhasználójának személyazonosító, banki vagy más személyes adatait.

A megszerzett információkat általában bűncselekmények elkövetésére használják fel, mások nevében kötött szerződések és más kötelezettségek elvállalására, hamis személyazonosító okmányok készítésére, banki folyószámlák megcsapolására, szolgáltatások vagy üzleti kapcsolatok felmondására.

Adathalászatnak (eredetileg angolul *phishing*, kiejtése: fising, a *fishing*=halászat szóra hasonlít) azt az eljárást nevezzük, amikor egy internetes csaló oldal egy jól ismert cég hivatalos oldalának láttatja magát és megpróbál bizonyos személyes adatokat, például azonosítót, jelszót, bankkártyaszámot stb. illetéktelenül megszerezni.

A csaló általában e-mailt vagy azonnali üzenetet küld a címzettnek, amiben ráveszi az üzenetben szereplő hivatkozás követésére egy átalakított weblapra, ami külsőleg szinte teljesen megegyezik az eredetivel.

http://hu.wikipedia.org/wiki/Informatikai_biztons%C3%A1g

Hogyan kerül a gépünkre?

- Internet, weboldalak (látogatás, telepítés)
- Külső adathordozóról (USB stick, CD, DVD)
- Telepítési melléktermék
- Nem kerül a gépre→Elektromos „szmog” lopása

Jelszó

- Nem ismert kifejezés (név, születési dátum…)
- Hossz
- Változatos karakterek
- Rendszeres csere

Adattikosítás

- HDD-n
- Tömörítés

Védelmek

- Rezidens malware keresők
- Víruskereső, Spykereső
- Tűzfal
- Billentyűzet figyelő megakadályozó
- Biztonsági szabályok
- Faraday kalitka (Extrém – Állam Kincstár)