SZÁMÍTÓGÉP VÍRUSOK

A számítógépvírus olyan speciális, önmagát szaporítani képes program, amely más programokba beépülve különböző káros hatásokat idéz elő. Kezdetben a számítógépprogramok szerzői védelmét biztosították velük, ma azonban károkozásért készítetik őket.

A legősibb vírusok a DOS-világban jelentek meg. Először a *.com kiterjesztésű programoknál, amelyekhez hozzákapcsolódva jöttek, láttak, és megfertőzték az egész világot. Később a lemez indítórekordját (boot-sector), majd később a partíciós tábla programját vették célba, így akár üres lemez segítségével is terjedni tudtak. Így jelent meg egy új iparág: megszülettek azok a vállalkozások, amelyek a vírusirtásra alapozták jövőjüket. Ezekből a cégekből nőtt ki jó pár ma világhírű, milliárdos forgalmú multinacionális vállalkozás: Symantec, McAffee Network Associates, Kaspersky Laboratórium.

Vírus részei:

- Fertőző rész: a vírust a gazdaprogramba másolja,
- Romboló rész: a károsító hatást fejti ki.

Károkozás szempontyából három fő csoportba oszthatjuk a vírusokat:

1. Ártalmatlan vírusok:
   olyan vírusok, amelyekbe a készítőjük nem tett semmilyen károkozó funkciót. Az ilyen vírusok csak saját maguk terjesztésével, és az antivírus szoftverek kijátszásával foglalkoznak, a felhasználó munkáját semmiben nem akadályozzák. Céljuk, hogy az egész világon elterjednek, bizonyítva a programozó ügyességét. A felismerés után egy megfelelő vírusirtóval távolítsuk el a vírust, mert könnyen előfordulhat, hogy jelentősen romlik a rendszertelsesítmény, egyes programok nem indulnak el, vagy lefagyasztják a számítógépet.
2. A felhasználót bosszantó, idegesítő vírusok;
   nem tesznek közvetlenül kárt a háttértárak tartalmában, de a felhasználót próbálják gátolni a normális munkavégzésben. A fertőzést követően néhány nappal, vagy egy előre meghatározott időpontban mindenféle zavaró funkciót aktivizálnak.Pl.:képernyőtartalom összekuszálása, esetleges lefagyasztás, vagy ilyesztő üzenetek küldése.
3. Kifejezetten rosszindulatú, káros vírusok.
   veszélyes vírusok, amelyek komoly anyagi károkat is okozhatnak a rosszul védett számítógápes rendszerekben.Ezek leggyakrabban a merevlemezen található állományokat törlik, módosítják, vagy csonkolják.legfőbb céljuk nem a károkozás, hanem az, hogy minél több számítógépet tudjanak megfertőzni. A víruskészítő inkább a hatékony önreprodukálásra és a vírusirrtok megtévesztésére fordítják a legtöbb energiát.Azárt hogy legyen idejük elterjedni, soha ne rögtön a számítógépre kezeléskor kezdik el romboló tevékenységüket. Bizonyos ideig önmaguk szaporítását végzik, majd valamilyen esemény bekövetkezésekor végrehajtják az előre beléjük programozott feladatot.

Különböző víruscsoportok, fajták:

- **Állományokat fertőző vírus:**
  Ezek program állományokat fertőznek meg. Ezután ha ezeket a programokat futatjuk, akkor a fertőzés továbbterjed. Az ilyen vírusok közül sokmemoria-rezidens, vagyis a memoriába tárolja magát. Ez ezzel jár, hogy a memória megfertőzése után minden végrehajtott program fertőzővé válik.Pl.: OneHalf, Getto.2000
- **Boot szektor vírusok:**
  Ezek a merevlemez vagy a ploppy boot szektorába veszik be magukat. Ezzel minden indításkor avírus végrehajtódik és szinte mindig memória-rezidensek, vagyis minden ezután használt lemezt megfertőznek. Legalábbis DOS alatt terjednek. A boot vírusok általában azután már nem fertőznek, ha a gép elindult, és akkor tesszük be a fertőzött lemezt. Pl.: Cruel.
- **Master boot record vírusok:**
  A boot szektorvírusokhoz hasonlóan viselkednek és memória-rezidensek. A fontos különbség a kettő között, hogy hová írják be magukat. A MBR (master boot record) vírusokat eredeti MBR-t átmásolják valahová máshova, így gépindításkor először a vírus maga hajtódik végre, majd ő mga ad hozzáférést az eredeti MBR-t. PL.: OneHalf
- **Többrétű (multi-partile,polypartite) vírusok**:
  Boot record-ot és progam állományokat is fertőznek. Ezekkel kicsit nehezebb elbánni, mert ha csak az egyik oldalt tisztítod ki, akkor az a másik oldalról simán visszafertőződik.
- **Makró vírusok:**
  Ezek adat állományokatfertőznek meg. Ezek egyre többen lesznek, ráadásul ha a program nem csak saját magán belül képes operálni, akkor nagyon hatékonyak is tudnak lenni, mert már nem csak másik

dokumentumot tudnak megfertőzni, hanem gyakorlatilag bármit tudnak csinálni. Ezek a vírusok a programok belső nyelvét használják ki, amik eredetileg arra készültek, hogy a programon belül működjenek.

- **Trójai faló (trojan horse):**
  külsőleg alkalmazói program a háttérben viszont „aknamunkát" folytat. Nem tartoznak szigorúan a vírusok közé, de mindenképpen ártalmasak. Mint a nevük is mutatja, általában valami másnak álcázva érkeznek hozzánk, gyakran E-mail-ben, vagy az Internetről letöltve. Gyakran valamilyen jópofajátéknak vagy animációnak álcázzák magukat. Ha elindítjuk, akkor az vagy a vírusttelepíti a számítógépre, vagy valamilyen közvetlen módon rongálya a háttértárak tartalmát. Azért nem nevezhető vírusnak, mert nem foglalkozik direkt módon önmaga terjesztésével és a felhasználók önkénttelepítik azt a számítógépünkre.
- **Féreg (worm):**
  olyan programok, amik rendszerről rendszerre terjednek, anélkül, hogy egy file-t használnának a terjesztéséhez, a vírusokkal ellentétben, amik leginkább file-okban terjednek. A férgek is file-okban vannak természetesen elrejtve, de azt másképpen használják ki, mint a vírusok. A féreg általában úgy utazik egy-egy file-ban, hogy a file maga a féreg.
- **Hátsó kapu (backdoor) :**
  olyan vírusok, amik a rendszeren egy részt nyitnak, ahol a támadások bejöhetnek, illetve amin keresztül az adatok szabadon áramolhatnak a tudtod nélkül.
- **Retrovírus:**
  olyan vírusfajta, amikkifejezetten a vírusvédelmi programokat támadják meg, és teszik használhatatlanná.
- **Hoaxvírus**:
  olyan üzenetek, amik e-mailben „ terjednek", és az ember az átvevő közeg sajnos.

  Ha ilyesmit látsz egy üzenet címsorában:

  1. Ha olyan levelet kapsz, aminek a címsora az, hogy [ide jön az aktuális név], akkor ne nyisd ki!
  2. Töröld azonnal!
  3. Tartalmazza a [ide jön a név] vírust!
  4. Mindent letöröl a merevlemezről és [ide jön még valami, ami nagyon súlyosan hangzik].
  5. Ezt a vírust ma (tegnap) jelentette be a [megbízható szervezet neve].
  6. Küld el mindenkinek hogy figyelmeztesd őket is!

Akkor nagy a valószínűsége , hogy egy hoax-szal van dolgod. Mielőtt egy ilyen üzenetet jóhiszeműen továbbküldenél, mindig ellenőrizd, hogy igaz-e? Ha rákeresel a neten, akkor biztosan találsz pontosabb információkat róla.
Ha ilyen levelet kapsz, és megbizonyosodtál róla, hogy az abban leírtak nem igazak, akkor udvariasan hívd fel annak a figyelmét erre, aki neked küldte, hogy legközelebb ő se ugorjon be olyan könnyen neki.

Legismertebb víruskeresők:
F-PROT,SCAN,TBAV,F-MACRO,NORTON AV, MCAFFEE AV

Védekezés a vírusok ellen:

- **Megelőzés:** csak jogtiszta programot használjunk,
- **Korai felismerés:** figyeljünk a gyanús jeleket a számítógép működése során (pl.: a gép lelassul, a programok nem úgy működnek, ahogy megszoktuk őket stb.)
- **Védelem:** használjunk vírusfigyelő, memória rezidens programot
- **Gyógyítás:** víruskereső és ártalmatlanító programmal próbáljuk felderíteni, majd törölni a vírust.

Nem vírusok:
Sokan sokmindenre egyből rámondják, hogy vírus, pedig ez nem mindig igaz. Egyszerűen csak könnyebb a vírusokat hibáztatni, főleg akkor, ha fogalmad sincs, mitől rossz a géped.
A következők nagy valószínűség szerint nem vírus okozta gondok:

- Hardvergondok. Egyenlőre nincs olyan vírus (Vagy talán mégis? Mintha lenne ilyen, hogy CIH, ami a BIOS flash-t felülírhatta), ami a számítógép hardver részét tönkretehetné. Monitor-vírus kifejezetten nincs.
- A számítógép bekapcsolásakor csipog és a képernyőn nem látszik semmi. Ez hardver gondokat jelent a boot folyamán. Meg kell nézned az alaplapod kézikönyvében, hogy a különböző hangjelek mit jelentenek.
- A számítógép 640 KB memóriát nem használ. Ez lehet vírus, de nem minden esetben. Néhány hardver meghajtó(monitor, SCSI kártya) használhatja ezt a memóriát. A hardver kézikönyvében kellene utánanézned.
- Két vírusirtó program van a gépeden és a egyik vírust jelent. Ez szintén lehet vírus, de az is lehet, hogy az egyik vírusirtó érzékeli a másik jelét a memóriában, és a memória rezidens a vírusnak azonosítja. Egyszerre, egy időben csak egyet használj, ha lehet.

- MS Office-t használva a program jelez, hogy a dokumentum makrót tartalmaz. Ez nem azt jelenti automatikusan, hogy ez makró vírus lenne, lehet rendes,, mindennapi makró is.
- Nem tudsz megnyitni egy dokumentumot. Ilyenkor próbálj meg megnyitni egy másik dokumentumot. Ha azt meg tudod nyitni, akkor a másik dokumentum talán sikerült, talán egy másik program tartja zárolva (lock).
- Merevlemez címkéje megváltozott. Minden lemeznek (így a merevlemeznek is) lehet egy címkéje. Ezt a címkét gyakorlatilag bármilyen program meg tudja változtatni a céljainak megfelelően, ehhez nem kell vírusnak lennie.
- Néha ha olyan program fut, ami erősen használja a merevlemezt (pl.: ScanDisk), akkor a víruskereső vírusszerű tevékenységet jelenthetnek. Ez attól van, hogy a víruskeresők nagy része nem csak a vírusok jellegzetes mintáira figyel, hanem olyan dolgokra is, amik vírust jelenthetnek (masszív lemezre írás, memória-rezidens programok, stb.).

Mi a biztonságos számítástechnika?

Minden hozzánk kerülő e-mailben, programban, vagy dokumentumban lehet vírus. Viszont ahelyett, hogy most bepánikolnánk, és mostantól nem fogadnánk el senkitől semmit, azután egy hónap múlva elfelejtenénk az egészet, tehetünk pár megelőző lépést.

A környezetedben mindenkinek hívd fel a figyelmét a vírusokra, de nem kell misztifikálni, lehet ellenünk nagyon egyszerűen védekezni.

Általános előkészületek:

- Ne hagyjál floppyt a gépben, mikor a gépet újraindítod, vagy kikapcsolod.
- A floppykat tedd írásvédetté, ha befejezted a munkát velük.
- Legyél elővigyázatos az e-mail attachment-ekkel, ha ismeretlen helyről kapod. Ismerős helyről kapott e-mailnél sem árt az óvatosság.
- Ellenőrizd, hogy valóban attól kaptál levelet, aki a fejléc szerint küldte azt.
- Ne állítsd be az e-mail programodat, hogy automatikusan futtassák a attachmeneket.
- Ha kijön valamilyen frissítés az operációs rendszeredhez (főleg ha az biztonsági), akkor töltsd le, és telepítsd.
- A fontos adatairól időnként csinálj biztonsági mentést úgy, hogy azt ne tudja felülírni, vagy megváltoztatni semmi a tudtod nélkül. Fontos a biztonsági másolatok készítése, aminél az sem árt, ha van benne valami rendszer. Minden mentés előtte persze víruskeresést kell végezni. Egy CD-tés azt a kis munkát megéri, hogy egy esetleges fertőzés után is megvannak a fontos állományaid.
- Ha használsz vírusirtó vagy kereső programot, akkor annak az adatbázisát folyamatosan frissítsd, hogy mindig felismerje a legújabb vírusokat is. Ez minimum havonkénti, de leginkább heti ellenőrzést és frissítést jelent.
- Ha van on-access scannered (olyan program , ami a file-hoz hozzáféréskor vizsgálja a vírusokat, általában a legtöbb vírusirtó programhoz jár), akkor kapcsold be.
- Ha valami új programot kapsz valakitől, vagy letöltesz valahonnan, akkor mindig elindítás előtt vizsgáld meg, nem vírus e. Ez CD-kre is vonatkozik, mert azon is lehetnek vírusos állományok.
- E-mail attachmenteket óvatosan nyissál meg. Ha lehet, akkor minden esetben először mentsd el a kérdéses állományt (semmiképpen ne nyisd meg!) és ellenőrizd a víruskereséddel. A legtöbb vírusirtó program tartalmaz email-scennert is, ami megnézi, hogy érkezzen vírus ezen keresztül. Ilyen is biztonságosabb, ha először elmented, és megvizsgálod az attachmenetet.