VÉDD MAGAD!

avagy
hogyan védekezzünk a számítógépes vírusok ellen?

Párzsa László
számítástechnikai vállalkozó

MI IS AZ A SZÁMÍTÓGÉP VÍRUS?

- A számítógépes vírus nem más, mint egy számítógép program. Ez a program képes önmagát sokszorosítani, "szaporítani", káros tevékenységet folytatni.
- A vírusprogram erkölcs és érzelem nélküli mesterséges intelligencia.
- A vírusfunkciók:
  - saját kódját másolja;
  - rejtőzködik, hogy felfedezése előtt legyen módja a terjedésre;
  - be programozott jelre, vagy egy adott feltétel teljesülésére vár;
  - valamilyen káros mellékhatást produkál.

HONNAN JÖNNEK, ÉS SZÁRMAZHATNAK A VÍRUSOK?

- **Egyetemi kutatólaborok.**

  Az első vírusokat programozó matematikusok fejlesztették ki, kifejezetten kutatási célból.

- **Katonai kutatólaboratóriumok.**

  Bár hivatalosan tagadják, hogy a katonai fejlesztő műhelyekben az ellenséges számítógépek megbénítására szánt számítógép vírusokat fejlesztettek.

- **Terrorista szervezetek programfejlesztői.**

  Az egyik legelső, széles körben elterjedt vírus a JERUSALEM (PÉNTEK 13) volt. Ez valamely palesztin állam titkos laboratóriumában készült.

- **Anarchista programozok, klubok.**

  A 80-as évek vége felé nagy divat volt a víruscserélő hálózatok üzemeltetése.

- **Másolásvédelmek melléktermékе.**

  Egyes másolás ellen védett szoftverbe építettek be olyan büntető rutinokat, amelyek ha nem találják a megfelelő azonosító kódot, vírust eresztettek szabadon (lásd a VENTURA kiadványszerkesztő korai változata potyogtató vírust helyezett a gépre).

- **Munkakörülményeikkel elégedetlen programozók.**

  Egyes elbocsátott programozók a felmondási idő alatt vírusfejlesztéssel és telepítéssel igyekeztek megkeseríteni egykori munkáltatójuk életét.

- **Felelőtlen programozók.**

  Sok programozó az elfogott vírus kódját visszafejti, majd átírja.

- **Az amatőrök.**

  Akik képzett szakembereknek vélik magukat nem is gondolnak arra, hogy kiszabadulhat kezükből az átírt vírusprogram.

- **Napjaink veszélyforrása az INTERNET.**

  - Az Internet gyors fejlődésével a vírusok terjedése is gyorsan áthelyeződött erre az új kommunikációs lehetőségre.
  - Ma az ismert vírusok száma közelít a százezerhez (Norton Antivírus 2005.01.29.-én 68948-at ismer), és naponta több száz új vírust hoznak létre.
  - Különböző felmérések alapján állíthatjuk, hogy kellő védekezés híján húsz percen belül az egész világot meg lehet fertőzni egy új vírussal.

VÍRUS DEFINÍCIÓK, VÍRUS FAJTÁK.

- **Fájl vírusok.**

  Úgy tudnak szaporodni, hogy a végrehajtható program állományokba (EXE, COM) másolják be magukat. Léteznek felülíró (owerwrite) és hozzáíró (append) vírusok.

  - A felülíró (owerwrite) vírusok a megfertőzött programokat használhatatlanná teszik.
  - A hozzáíró (append) vírusokkal fertőzött programok nagy része megfelelő vírus irtó programmal helyre állítható.

- **Boot vírusok.**

  A vírusok egy csoportja a floppy vagy a merevlemez boot területébe írja be magát. A boot vírusok akkor fertőznek, ha a fertőzött lemezről indul a gép.

- **Mutáló, öntitkosító, polimorf vírusok.**

  Megjelentek a saját kódjukat módosítani képes vírusok. Az ilyen vírusoknak minden fertőzéskor saját programkódjuk megváltozik.

- **Többlaki vírusok.**

  A többlaki vírusok a COM és az EXE fájlokon kívül a partíciós táblát is megfertőzik. Ha egy fertőzött floppyról bejut a memóriába, a merevlemez megfertőzése után eltávolítja saját magát a floppyról.

- **Dropperek.**

  A vírusok egy olyan csoportját nevezzük droppereknek, amelyek önmaguk működő programok, csak mellékesen vírusokat engednek ki magukból.

- **Vírusgyártó automaták.**

  Ezek olyam programok, programcsomagok, amelyekkel több-kevesebb programozói tudással ezerszámra lehet új vírusokat létrehozni.

- **Trójai programok.**

  A trójai program a tőle várt hatások mellet (ie. történelem, trójai faló esete) váratlan, káros melléktevékenységet folytat. A közönséges vírusoktól csupán abban különböznek, hogy nem tartalmaznak önszaporító rutinokat.

- **Férgek.**

  A vírusoknak olyan alfaja, amely azzal okoz kárt, hogy addig másolja önmagát a fertőzött állományokba, amíg azok végül futtathatatlanul hosszúak lesznek, vagy be nem telik a lemez.

- **Időzített bombák.**

  Valami feltétel teljesülésére vár. Előfordult, hogy egy programozó „biztonsági rutinokat” épített be az általa fejlesztett programba. Ezek a rutinok figyelték, hogy Ő szerepel-e a fizetési listán. Mindaddig amíg a programozó szerepelt, semmi baj nem történt.

- **Tréfás programok.**

  Láthattunk olyat, hogy egy program a képernyőt "fejre” állította. A tréfás programok is vezethetnek komoly károkhoz, elég ha a felhasználó pánikba esik.

- **Új típusú vírusok.**
  - Létezik olyan vírus is ami a PC biost (flas bios) teszi tönkre.
  - Viszonylag újjak a MACRO vírusok, mely az Office dokumentumokat fertőzi.
  - Az E-mail-en terjedő kártevők okoznak manapság a legtöbb gondot. Naponta akár több száz kéretlen levelet (spam) kaphatunk, nem egy közülük vírussal fertőzött.

VÍRUSJENSÉGEK

- Előfordul, hogy időnként nem várt jelenségekkel találkozunk. Ezeknek egy része természetes, vagy szoftver hibákra, illetve vírus jelenlétére utalnak!
- Melyek ezek a jelenségek?
  - a korábban elegendő memória egyszerre csak "kevés lesz";
  - a floppy vagy a merevlemezen a vártnál gyorsabban fogy el a szabad terület;
  - látszólag ok nélküli, megmagyarázhatatlan programhibákkal találkozunk;
  - egyes programok működése lelassul, vagy teljesen leáll;
  - Fura, szokatlan üzenetek jelennek meg;
  - időnként szokatlan hangeffektusokat produkál a számítógép;
  - a képernyőn nem a begépelt szöveg jelenik meg, a billentyűzet úgy működik, mintha átprogramozták volna;
  - a merevlemez és a floppy adatforgalmát jelző lámpa (LED), minden ok nélkül aktivitást jeleznek;
  - a csak olvasási jogkörrel rendelkező programok, futtatható programállományok átírásával próbálkoznak;

- akkor is követeli számítógépünk az írásvédelem nélküli floppylemez behelyezését a meghajtóba, ha mi csak olvasást kértünk a lemezről (GETTO 2000 vírus, miután már megfertőzte az összes végrehajtható programot a merevlemezen);
- fájlok, könyvtárak "tűnnek el" vagy ellenkezőleg, jönnek létre minden ok nélkül;
- váratlanul újraindul a számítógépünk;
- megmagyarázhatatlan adatvesztések jelentkeznek;
- a hozzáférés-védelmi rendszerünk nem engedélyezett lemezre írási kísérleteket jelez;
- az önellenőrző, vagy másolásvédett szoftverek nem hajlandók elindulni, és azt jelzik, hogy valami a program kódjukat módosította (például a VIRSTOP.EXE vírusfigyelő program);
- a fájlok ellenőrzése során nem sikerült a megfelelő eredeti ellenőrző összegeket megkapni;
- a háttérben futó vírus ellenőrző szoftver vírust jelez;
- a rendszeres vagy alkalmi vírus ellenőrzés során a kereső program vírus jelenlétét jelzi;

A MEGELŐZÉS LEHETŐSÉGEI

- A vírus elleni védelemnek legjobb módszere (akárcsak az életben), a megelőzés.
  - Talán a legfontosabb szabálya, hogy csak a jogtiszta programot használjunk.
  - Ne alkalmazzunk hardveres vagy szoftveres "másolás elleni" védelemmel ellátott programokat.
  - Ne fogadjunk el ismerősöktől programot, lemezeket minden előzetes ellenőrzés nélkül.
  - Mielőtt telepítenénk a programot, végezzünk vírus ellenőrzést.
  - Rendszeresen végezzünk vírus ellenőrzést, legalább hetente egyszer.
  - Rendszeresen végezzünk biztonsági mentéseket.

- Használjunk memóriában állandóan figyelő vírus ellenőrző programrendszert úgy a hálózaton, mint a PC-inkben (netshield, vshield, virstop, Norton Antivírus, stb.).
- Legalább két különböző gyártótól származó vírus ellenőrző programot használjunk, így fokozhatjuk a biztonságot (F-prot, Norton Antivírus, stb).
- Feltétlen éljünk a megelőzés lehetőségével, állítsunk be vírusfigyelő, ellenőrző programunkat megfelelően, gondoskodjunk a vírus ellenőrző kódok frissítéséről.
- Ha rendelkezünk valamilyen INTERNET összeköttetéssel, különösen ajánlott az E-mail figyelése, szűrése, a kéretlen reklám levelek törlése (spamok) tiltása.
- Ha a PC-ink BIOS-a lehetővé teszi, kapcsoljuk be a BIOS-szintű vírus védelmet.
- Oktatással foglalkozó intézményeknél különösen gondot okoz az otthonról behozott programok, (játékok) csere-beréje.

MI A TEENDŐ?

- **Ne essünk pánikba!**
  - A pánikba esett felhasználók azonnal kikapcsolják a gépet, ezzel okozva igen nehezen belátható problémákat.
  - A pánikba esett felhasználók fertőzés észlelése után a nem merik használni a gépet, mert nincsenek tisztában azzal mit tehetnek, és mit nem.
- **Mit tegyünk?**
  - Fontos, hogy fertőződés észlelésekor szabályosan befejezzük a munkánkat.
  - Kapcsoljuk ki a gépet, és gyűjtsünk minél több információt az észlelt jelenségről, vírusról.
  - Bátran kérjük ki a nálunk tapasztaltabb kollegák véleményét.
  - A beszerzett információk birtokában indítsuk el számítógépünket, és garantáltan vírusmentes vírus irtó programmal végezzük el a vírus ellenőrzést, irtást.
  - Abban az esetben, ha a vírust nem tudjuk a fájlból eltávolítani /fájl vírusok /, vagy a fájl az eltávolítás után sérült lesz, akkor töröljük le a fertőzött fájlt.
  - Ne titkolódzunk! Hívjuk fel azoknak a kollegáinknak a fegyelmét akik esetleg a mi gépünk fertőzöttsége miatt szintén megfertőződhettek. A titkolózás oda vezethet, hogy ismét megfertőződünk.

A KÖVETKEZŐ KÉT (MA MÁR RÉGI) VÍRUS SAJÁT GYAKORLATOMBAN KOMOLY, FEJFÁJÁST OKOZOTT:

Vírus neve	: **Getto 2000**
Vírus hossza	: 2000 byte
Eredete	: Magyarország
Fertőzési hely	: COM és EXE fájl-ok
Típusa	: Rezidens, polimorf, lopakodó
Romboló hatás	: Rendszer állományok törlése

Ez a vírus egyike a leggyilkosabb vírusoknak. A COM és EXE fájlokat fertőzi meg. A fertőzött fájl indításakor a vírus dekódolja önmagát. A vírusutasítások fizikai helye változik a fertőzött programban.
A romboló hatást éjjel 0 és 1 órakor végzi, ekkor törli a két MS-DOS rendszer fájlt és a config.sys-t.

Saját tapasztalatom:
A tantermemben (20 gép) megfertőzte az összes számítógépet. Miután minden végrehajtható programot a merevlemezen és a NOVELL hálózaton a vírus megfertőzte, még akkor is követelte a floppylemez írásvédelem feloldását, ha mi nem akartunk a floppyra írni, csak tartalomjegyzéket kértünk.

Mivel nem állt rendelkezésemre a **G2000K.EXE** vírusirtó, az összes gépen az egész rendszert újra kellett telepítenem (a NOVELL hálózattal együtt)!

Vírus neve : **One Half**
Vírus hossza : 3544 byte
Eredete : Szlovákia
Fertőzési hely : Merevlemez MBR, COM és EXE fájl-ok
Típusa : Rezidens, polimorf, lopakodó
Romboló hatás: Szöveg megjelenítés, merevlemez elkódolása

Talán ez a vírus a leggyilkosabb vírus amivel eddig találkoztam. Ha egy fertőzött fájlt indítunk el, akkor a vírus azonnal észrevétel nélkül megfertőzi az első merevlemez Master Boot Record-ját. A vírus a következő indításkor rezidenssé válik, és elkódol 2-2 sávot a merevlemezen. Az elkódolás az első hét sáv kivételével az egész merevlemezre kiterjed. Amíg a vírus a memóriában van az egész elkódolásból semmit nem lehet észrevenni, mivel a merevlemez olvasásakor a beolvasott adatokat a vírus dekódolja. Ha a vírus a merevlemez felét már elkódolta, megjelenhet a következő üzenet:

Dis is one half.
Press any key to continue ...

Saját tapasztalatom:
Ha a vírus a teljes merevlemezt már elkódolta, saját magát letörli a winchesterről, a következő gépindításkor már nem lesz ami a tartalmat a memóriában visszakódolja, így az egész winchester használhatatlanná, olvashatatlanná válik. Egy alacsonyszintű formázás és a rendszer újratelepítése volt a gyógyír a problémára.