A számítógépes vírusokról...

Tartalmi forrás: https://www.pcvilag.hu/szamitogep-virus-eltavolitas

A számítógépes vírusokról általában

- A PC-k terjedésével az 1980-as évektől világszerte sokféle vírus pusztított már a számítógépekben, célszerű megismerkedni velük és az ellenük való védekezéssel
- A vírus előbb-utóbb kárt okoz a háttértáron lévő állományokban, könyvtárakban vagy zavarja a számítógépes rendszer használatát
- Leggyakrabban magukat kiváló programozónak tartó fiatalemberek írnak vírusokat, amelyekkel feltűnést akarnak kelteni
- A vírusok károkozásuk miatt felhasználásra kerülhetnek (és esetenként kerülnek is) az üzleti és a katonai életben

Mik azok a vírusok?

- A **számítógépes vírus** olyan **önmagát sokszorosító** program, vagy programrészlet, mely képes saját magát más végrehajtható alkalmazásokban, vagy dokumentumokban elhelyezni és ezáltal **terjedni.**
- **„Feladatuk" a károkozás,** vagy legalábbis az **önmutogatás,** a saját maguk létére való figyelemfelhívás
- Általában a **számítógép memóriáját, illetve az internetet** használják **terjedésükhöz, szaporodásukhoz**
- Mindenféle közhiedelemmel ellentétben **nem terjednek tüsszentéssel**

Hogyan kerülhet vírus a gépemre?

- Internet **böngészőn keresztül**, weboldal megtekintés közben.
- **E-mail** formájában. Érkezhet akár ismerőstől, akár levélszemét (Spam) formájában
- Beszélgető **(Chat) programokon** keresztül (pl.: MSN, Skype, Facebook Messenger, stb…)
- Letöltött **fájlokkal**
- **Fertőzött adathordozó** használatával (pl.: winchester, pendrive, cd/dvd lemez)
- **Helyi hálózaton** keresztül, más fertőzött számítógépekről

A felsorolás nem teljes, és lehet, hogy holnap új típus is megjelenik…☹

A vírusok fajtái

- **Fájl vírusok**
- **Boot vírusok**
- **Makrovírusok**
- **Lánclevél (Hoax)**
- **Adathalászat (Datafishing)**
- **Kémprogramok (Malware)**
- **Trójaiak**
- **Számítógépes férgek (Worm)**
- **Kihasználó vírusok (Exploitok)**
- **Tárcsázó (Dialer)**
- **Zsaroló vírusok**

Fájl vírusok

- Többnyire más (futtatható) programokhoz fűzik magukat, ezzel biztosítva a víruskód lefutását
- A fertőzött végrehajtó (EXE, COM, DLL stb. kiterjesztésű) állomány gyakran használhatatlanná válik, vagy csak tovább fut, mintha mi sem történt volna, de közben fertőz
- A fertőzött állományok floppykon vagy hálózaton terjednek
- Figyelem! A különböző vírusok - így a fájl vírusok is - az Internet használatával is bekerülhetnek rendszerünkbe!

Boot szektor: a háttértárolók (pl. winchester, cd/dvd lemez) indító szektora.

Boot vírusok

- A számítógép háttértárolóin az ún. betöltő (boot) területekhez kapcsolódó fájl vírusok
- Általában fertőzött háttértár segítségével terjednek
- Az operációs rendszer „kiskapuit” kihasználva, a rendszer bekapcsolásakor - amikor a gép az operációs rendszert betölti a lemezről - automatikusan a memóriába kerülnek, és így tovább fertőznek

A makrók az Office dokumentumokban (is) használt - egyébként hasznos - programrészletek, leggyakrabban ismétlődő folyamatsorok végrehajtását könnyítik meg.

Makrovírusok

- **MS-Office állományokhoz kapcsolódnak,** kárt, illetve működésbeli zavart keltve
- 1997 óta számuk több, mint a hagyományos vírusoké

- Az **MS-Office jelenlegi változatai** már **beépített védelmet** tartalmaznak a makrovírusok ellen

Lánclevél (Hoax)

Ki ne ismerné az Interneten keringő számos olyan levelet, melyeknek egyetlen célja, hogy **minél több embernek továbbítsák** azokat. Miért jó ez bárkinek? Az ok nagyon egyszerű. A módszerrel **rengeteg élő és működő email címet** lehet összegyűjteni, melyekre később **kéretlen levél** (spam), vagy akár **vírusok** is küldhetőek. A lánclevelet egyszerű felismerni, hiszen mindegyik felhívja a figyelmet arra, hogy minél több barátnak, ismerősnek küldd tovább a levelet. **Néhány Hoax alaptípus, aminek nem szabad bedőlni:**

- Küldd tovább, pénzt kapsz valamelyik vállalattól pl.: AOL, INTEL, MICROSOFT
- Küldd tovább, Bill Gates felosztja vagyonát (sokszor vegyítve az előzővel…)
- Küldd tovább, rákos kislány utolsó kívánsága (legalább 10 éve rákos szegény kislány…)
- Küldd tovább, új vírus jelent meg (napi több 100 új vírus jelenik meg, ezért az ilyen levelek teljesen értelmetlenek…)
- Küldd tovább, notebookot nyersz (a legrégibb trükk, hogy valamit nyerni lehet…)

Adathalászat (Datafishing)

Az **adathalászat** egy olyan eljárás, melynek során egy **internetes csaló** egy jól ismert cég hivatalos oldaláról másolatot készít és megpróbál **személyes adatokat**, például **azonosítót, jelszót, bankkártya számot** stb. illetéktelenül megszerezni. A csaló **általában e-mailt** küld több ezer címzettnek, amiben ráveszi az üzenetben szereplő hivatkozás követésére egy átalakított weblapra, ami külsőleg szinte teljesen megegyezik az eredetivel.

- **Védekezés:** Tisztában kell lenni azzal, hogy bankok és egyéb hivatalos szervek **soha nem küldenek** üzenetet ügyfeleiknek azzal a céllal, **hogy megkérjék, jelentkezzenek be** és adják meg személyes adataikat!

Kémprogramok (Malware)

A számítógépén tárolt **adatok ellopására** specializálódott vírusfajta a **kémprogram**. Az ilyen kártékony szoftver a felhasználó tudta nélkül képes a számítógépén **tárolt adatokat**, vagy **felhasználói szokásokat** az Interneten keresztül készítője számára eljuttatni. Képesek akár minden egyes **leütött billentyűt összegyűjteni** és megadott időközönként elküldeni egy kívülálló személy számára, így jutva fontos adatokhoz, jelszavakhoz.

- **Védekezés: ”Anti-Malware”** alkalmazás telepítése kémprogramok eltávolításra.

Nevüket az eredeti ”trójai falóval” való hasonló viselkedésüknek köszönhetik

Trójaiak

A **trójai vírus** nagyon találó nevet kapott. Emlékszel még a történetre? A trójaiak elkövették a hibát, hogy a görögök ajándékát beengedték a városukba, majd lóban rejtőző katonák reggelre bevették a várost. A **trójai vírus** az esetek nagy részében **nem annak látszik, ami valójában**. Hasznos alkalmazásnak álcázva jut be számítógépbe, és képes az **irányítást** teljes egészében egy **külső irányító kezére játszani**.

- Jól használható programnak (pl. tömörítő programnak) álcázott rombolók
- Nem szaporodnak, hanem különböző funkciókat rendelnek a gazdaprogramhoz (programvédelem, hibás működés, rombolás)
- Előszeretettel alkalmazzák őket az üzleti életben

Számítógépes féreg (Worm)

A **Számítógépes féreg** a számítógépes vírushoz hasonló **önsokszorosító program**. Míg azonban a vírusok más végrehajtható programokhoz, dokumentumokhoz kapcsolódnak hozzá illetve válnak részeivé, addig a férgeknek **nincs szükségük gazdaprogramra**, önállóan fejtik ki működésüket.

Az önsokszorosításon kívül a **féreg** sokféle dologra beprogramozható, például **fájlok törlésére** a gazdarendszeren, vagy **önmaga elküldésére e-mailben**.

- Vigyázat! Feladatuk sokszor a levédett rendszerek jelszóinak megszerzése, a védelmi funkció kiiktatása is lehet!

Kihasználó vírusok (Exploitok)

Az **exploitok** olyan **kártékony alkalmazások**, melyek az Internet böngészők és a számítógépes rendszer gyenge pontjait, **biztonsági réseit használják ki**. Léteznek olyan weblapok, melyek az ingyenes letöltés lehetőségével vonzzák magukhoz a látogatót, ám letöltés helyett csak a weboldalban elhelyezett exploit települ számítógépre. Sajnos nagyon sok internetes oldal kódja feltörhető, és ebből kifolyólag biztonságos oldalakba is elhelyezhető exploit vírus.

Windows környezetben a **védekezést** egy biztonságos Internet böngésző használatával érdemes kezdeni. Ilyen pl.: a **Mozilla Firefox**, **Opera**, vagy a **Google Chrome** is. Ajánlott **Windows** rendszerünk **automatikus frissítésének engedélyezése**, így ha egy biztonsági rés javítása elkészül, akkor a frissítés automatikusan települhet gépre.

Tárcsázó (Dialer)

A **tárcsázó vírus** egy régi eszközt, a **modemet használja** fel **emeltdíjas telefonszámok** hívására. Ezzel közvetlen profitot termelve a vírus fejlesztőjének. A számítógépes modem használható internetezésre, faxküldésre, és ezáltal bármilyen hagyományos analóg telefonszám tárcsázására is.

- **Védekezés:** Amennyiben már szélessávú kapcsolatot használunk internetezésre (az esetek többségében ez a helyzet), akkor egyszerűen **távolítsuk el a telefon vezetéket** a modem "LineIn" bemenetéről. Ezzel gyakorlatilag lehetetlen modemen keresztül bármilyen tárcsázást kezdeményezni. Amennyiben a modemre egyáltalán nincs szükség érdemes lehet teljesen eltávolítani a rendszerből.

Zsaroló vírusok

- Saját fájljainkat támadja meg, például t**itkosítja dokumentumainkat, képeinket hangfelvételeinket**.
- A titkosítás visszafejtéséért **pénzt követel** tőlünk.
- Általában e-mail **csatolmányként**, vagy chatprogramokon keresztül juthat a gépünkre, van olyan fajtája, mely **minden csatolt meghajtón** (pendrive, hálózati meghajtó, felhő) **lévő állományainkat is titkosítja.**
- A legjobb védekezés ellenük a megelőzés (**nem nyitunk meg gyanús csatolmányokat**)!
- 2015-ben a Magyarországon is megjelent CTB-Locker **460-470 ezer forintnak megfelelő váltságdíjat követelt** a titkosítás feloldásáért.

A vírusfertőzés tünetei

- Szokatlan programműködés
- Programállományok mérete megnő, átneveződnek, esetleg egyes programok törlődnek, vagy nem indulnak
- A rendszer indokolatlanul lelassul
- Szokatlan üzenetek jelennek meg
- Furcsa jelenségek a képernyőn (pl. a betűk „lepotyognak”)
- Dokumentumaink, képeink, hangokat tartalmazó állományaink átneveződnek, titkosítódnak, maguktól törlődnek
- Ritkán, de megeshet a hardver meghibásodása is (régebben ez nem volt jellemző!!!)

Ha a fenti tüneteket (főleg, ha többet egyszerre) tapasztaljuk, legalább a vírusfertőzés gyanújának meg kell születnie bennünk!

Vírusfertőzés megelőzése

- **Biztonsági másolat** készítése fontos **állományainkról**
- Az **operációs rendszer** szoftver **telepítő készletének CD-DVD lemezen való tárolása** (egyéb szoftverek esetében ma már nem létfontosságú, mert az interneten biztonságos letöltő oldalakról, vagy a szoftvert fejlesztők oldaláról letölthetők a legfrissebb telepítők…)
- **Legális szoftverek** használata
- **Idegen lemez, program(ok), dokumentumok vizsgálata** az első használat előtt valamely friss adatbázisú vírusfigyelő programmal
- Tartózkodj **a bizonytalan eredetű e-mailek (különösen csatolmányaik)** megnyitásától!
- Kellő **körültekintéssel** használd az **internetet,** tartózkodj **bizonytalan „tulajdonú" honlapok** meglátogatásától!

Vírusfigyelés és vírusirtás

- A vírusfertőzés elhárításának eszköze a tiszta rendszerlemez, amelyen legalább egy jelző és/vagy tisztítóprogram is van.
- Tényleges fertőzés gyanúja esetén ezen rendszerlemez segítségével kell indítani a számítógépet, majd a vírusjelző, illetve irtó programot.
- A vírusirtó programot, és annak vírusadatbázisát állandóan frissíteni kell!

Vírusfigyelő és/vagy irtó programok

A **vírusölő programok** nagy része nem csak megvédi számítógépét a támadásoktól, hanem megakadályozza, hogy egy vírus átkerüljön családod és barátaid számítógépére e-mail küldés, vagy fájl megosztás során. Fontos megemlíteni, hogy mivel a vírusokat programozzák le először, illetve napi szinten rengeteg új fenyegetés jelenik meg, ezért tökéletes vírusölő sajnos nem létezik. Ezért a **vírusölő használata mellett is** rendkívül fontos a számítógép **körültekintő** használata.

- **Avira Personal Edition (Free)**
- **ESET NOD32**
- **AVG AntiVirus (Free)**
- **Avast! Home Edition (Free)**
- **Norton AntiVirus**
- **Kingsoft Antivirus (Free)**
- **stb...**

Természetesen a lista nem teljes!

A víruspajzsok

- A víruspajzsok a mai korszerű vírusfigyelő/irtó programoknak olyan vírusfigyelő moduljai, melyek a **rendszer indításakor a memóriába kerülnek.**
- Fertőzés, vagy annak gyanúja esetén **azonnal jeleznek.**
- **Folyamatosan figyelik**, hogy a használt meghajtók, állományok, csatolmányok fertőzöttek-e?
- Hátrányuk, hogy valamennyire lassítják a számítógép működését, ez a **hátrány azonban elenyésző** az általuk nyújtott (bár nem 100 %-os) **biztonsághoz mérten.**

Érdekességek

- Magyarországon az első vírus 1984-ben jelent meg. Terjesztője egy kisiparos, aki saját forgalmát akarta így növelni. (A vírus károkozásán segíteni csak a gépek szétszerelésével lehetett.)
- 1989-ben 30 ismert vírus volt, jelenleg a vírusfigyelő/irtó programok több milliós nagyságrendben ismerik fel a vírusokat.
- Az Öböl-háborúban az amerikai ügynökök részben vírusokkal bénították meg az iraki légelhárítás számítógéprendszerét.
- A mai vírusok képesek saját kódjuk módosítására, és a mutáns lecserélésére.
- Olyan vírusok is léteznek, amelyek álvírusokat hoznak létre, így a vírusirtó végzi a legnagyobb rombolást, amikor megpróbálja kiirtani az álvírust.

Ellenőrző kérdések

- Mi a vírus és hogyan terjed?
- Hogyan csoportosítjuk a vírusokat?
- Mi a teendő fertőzés esetén?
- Hogyan védekezzünk a fertőzés ellen?
- Mi a víruspajzs?

Feladatok

- Vizsgáld át a gépedet egy vírusfigyelő-írtó programmal!
- Vizsgálj meg egy csatlakoztatott meghajtót is! (CD-DVD, pendrive, hálózati meghajtó, stb…)