Kártevők, vírusvédelem

Számítógépes vírusok fogalma, meghatározása és jellegzetes tulajdonságaik:
Tágabb értelemben számítógépes **vírusnak tekinthető** minden olyan program, melyet készítője ártó szándékkal hozott létre (a munka zavarása, ellehetetlenítése; adataink megszerzése, megsemmisítése, stb.).
A **szűkebb értelemben** vett **vírusok** az alábbi három **tulajdonsággal** bírnak:

- végrehajthatóak, vagyis működőképesek (executable)
- önmagukat másolva képesek terjedni
- képesek hozzáépülni más végrehajtható állományokhoz

Vírusok közös jellemzői:

- A vírust tartalmazó, fertőzött program futásakor a vírusprogram is lefut. Ekkor reprodukálja, megsokszorozza önmagát, és minden új példánya egy további fájlt fertőzhet meg.
- Valamilyen közvetlenül vagy közvetve futtatható bináris programfájlhoz vagy makróhoz, forráskódú szkripthez csatolja magát, miközben módosítja annak kódját úgy, hogy futtatásakor az ő saját kódja is lefusson.
- A vírusprogram futásakor valamilyen feltétel igaz vagy hamis voltát is figyeli. Ennek logikai értékétől függően aktivizálhatja az objektív rutinját. Azt a programrészt, amely törölheti a lemezes állományokat, formázhatja a merevlemezeket, vagy csak játékos üzeneteket, reklámszövegeket jelenít meg a képernyőn.

Vírust kaphatunk megbízhatatlan forrásból származó hajlékonylemezekről, CD-ről, flash-memóriákból, de email-hez csatolva is.

A számítógép működésében bekövetkező változások, amelyek alapján vírustámadásra lehet gyanakodni:

- Fájlok mérete indokolatlanul növekszik
- Megnövekszik indokolatlanul a háttértárakról felhasznált terület (maga a vírus-fájl kicsi, 10-20 bájtos is lehet)
- Idegen állományok jönnek létre a háttértárakon.
- Nagyon sok merevlemez használat
- „belassul" a gép

A programok működésében zavarok jelentkezhetnek

- A hálózatkezelés lelassul hibát jelez pl. lefagyások jelentkeznek
- A perifériák rendellenesen működnek.
- A gép feldolgozási sebessége csökken, a memóriák túlterheltek

A vírusok történeti fejlődésének néhány példája:

1986: Két pakisztáni PC-kereskedő rájött, hogy a floppy lemez boot szektorának programja felülírható, ezért megváltoztatták a kódot úgy, hogy az önmagát másolja floppyról floppyra. Az első (egyébként ártalmatlan) IBM PC vírust elnevezték **ŠBrain**-nek. Még ugyanebben az évben egy programozó, Ralf Burger, megoldotta azt, hogy a vírus a végrehajtható .COM kiterjesztésű állományokba ágyazódjon, és bennük terjedjen.
1987: Franz Swoboda közzé teszi a titokzatos eredetű **Charlie** vírust. Az első kártékony vírus újraindította vagy lefagyasztotta a számítógépet. A **Jerusalem** az első időzített vírus: minden péntek 13-án törli a végrehajtható állományokat. A **Stoned** nevű vírus, az első tömeges fertőzést okozó vírus. Még ma is vadon élő vírus. Minden nyolcadik bootoláskor üzenetet ír ki ("Your PC is now stoned").
1991: A sokasodó víruskereső szoftverek fejlesztői bajban vannak. A DOS operációs rendszer 640 kilobájtos memóriája nem tud megbirkózni a csaknem 1500 vírus definíciójával, nem beszélve az ellenőrzés lassúságáról.
1992: Egy amerikai víruskereső-kereskedő bejelenti, hogy március 6-án 5 millió számítógép fog leállni a **Michelangelo** vírus miatt. A cég meggazdagodott az eladott szoftverekből, miközben legfeljebb 10.000 számítógép fertőződött meg.
1995: A víruskereső szoftverek fejlesztői aggódnak, hogy a Windows 95 megjelenésével fölöslegessé válnak, hiszen a legelterjedtebb boot-vírusok nem szaporodnak az új operációs rendszer alatt. Ezzel szemben új kihívásokkal kell szembenézni, mivel megjelennek az első makró vírusok.
1998: Az első Java vírus megjelenése.
2000: Az ILoveYou minden idők "legsikeresebb" vírusa. Négy óra alatt körbejárja a világot. Ma már a vírus terjedése sokkal inkább az emberi, mint a technikai tényezőkön múlik.
Általánosságban elmondható, míg régen az unatkozó, zsenge programozózsenik írtak 1-1 világméretű fertőzést okozó vírust (pl. ILoveYou) és kerültek be aztán horrorfizetésekkel cégekhez, addig manapság nem az ilyen "hangos", médiavisszhangot is kiváltó globális fertőzések a "menők". Bűnözői csoportok célzottan írnak jól rejtőzködő szoftvereket, mert hiszen amit nem látsz, az ellen nehezen védekezhetsz.

A vírusok fajtái, kifejtett hatásuk:

- **Fájl-vírus:** Ez a legrégebbi vírusforma, mely futtatható (exe, com, dll) állományokhoz épül hozzá. A vírussal fertőzött program jelenléte a háttértáron önmagában még nem vezet károkozáshoz. A vírus kódja csak akkor tud lefutni (aktivizálódni), ha futtatjuk a vírus által fertőzött programot. Ekkor a gazdaprogrammal együtt a vírus is a memóriába töltődik, s ott is marad a számítógép kikapcsolásáig. Ez idő alatt a háttérben végzi nem éppen áldásos tevékenységét: hozzáépül az elindított programokhoz (fertőz), és eközben vagy egy bizonyos idő elteltével illetve dátum elérkezésekor végrehajtja a belékódolt destruktív feladatot.
- **BOOT-vírus*:*** A mágneslemez/merevlemez BOOT szektorába írja be magát, így ahányszor a lemez használatban van, annyiszor fertőz. Különösen veszélyes típus az un. **MBR** vírus, amely a rendszerlemez BOOT szektorát támadja meg, így induláskor beíródik a memóriába. Innentől kezdve egyetlen állomány sincs biztonságban, amely a memóriába kerül.
- **Makróvírus*:*** A makrók megjelenésével dokumentumaink is potenciális vírushordozóvá váltak A makró irodai programokban a felhasználó által létrehozott „parancslista”, mely a dokumentumban gyakran elvégezendő gépies feladatok automatizálására használatos. A makróvírus e lehetőséggel él vissza: dokumentumainkhoz épülve, annak megnyitásakor fut le kártékony kódja. A vírusok ezen válfaja az internetes adatforgalom fellendülésével indult rohamos terjedésnek.
- **Trójai program*:*** A mondabeli trójai falóhoz hasonlóan valójában mást kap a felhasználó, mint amit a program „ígér”. Ez a vírus a jól működő program álcája mögé bújik: hasznos programnak látszik, esetleg valamely ismert program preparált változata. Nem sokszorosítja magát, inkább időzített bombaként viselkedik: egy darabig jól ellát valamilyen feladatot, aztán egyszer csak nekilát, és végzetes károkat okoz. Némely trójai programok e-mail-ek mellékleteként érkeznek: a levél szerint biztonsági frissítések, valójában viszont olyan vírusok, amelyek megpróbálják leállítani a víruskereső és tűzfalprogramokat.
- **Féreg:** Általában a felhasználók közreműködése nélkül terjed, és teljes (lehetőleg módosított) másolatokat terjeszt magáról a hálózaton át. A férgek felemészthetik a memóriát és a sávszélességet, ami miatt a számítógép a továbbiakban nem tud válaszolni. A férgek legnagyobb veszélye az a képességük, hogy nagy számban képesek magukat sokszorozni: képesek például elküldeni magukat az e-mail címjegyzékben szereplő összes címre, és a címzettek számítógépein szintén megteszik ugyanezt, dominóhatást hozva így létre, ami megnöveli a hálózati forgalmat, és emiatt lelassítja az üzleti célú hálózatot és az internetet. Hírhedt példa az Internet 1988-as féregfertőzése (az **Internet Worm**).
- **Kémprogramok (Spyware):** Céljuk adatokat gyűjteni személyekről vagy szervezetekről azok tudta nélkül a számítógép-hálózatokon. Az információszerzés célja lehet békésebb (például reklámanyagok eljuttatása a kikémlelt címekre), de ellophatják számlaszámainkat, jelszavainkat vagy más személyes adatainkat rosszindulatú akciók céljából is. A többi vírusfajtához hasonlóan más programokhoz kapcsolódva tehet rájuk szert a nem eléggé óvatos felhasználó.

Ezen kívül a vírusokat csoportosíthatjuk a károkozás jellege (csak ijesztget vagy ténylegesen töröl illetve módosít) illetve az aktivizálódás időpontja szerint is (fertőzés esetén rögtön , adott idő elteltével vagy bizonyos dátum bekövetkezésekor).

Vírusok elleni védekezési módszerek és eszközök:

A fertőzés megelőzése: Egy eredendően „tiszta” számítógépre csakis külső forrásból érkezhetnek vírusok (hacsak az adott gép felhasználója maga nem készít ilyet). Mivel a számítógép teljes elszigetelése, a lehetséges adatcsatornák (cserélhető adathordozók, hálózat, telefonos kapcsolat) lezárása erősen korlátozza a használhatóságot, a bejövő adatforgalom minél szigorúbb **ellenőrzése** jelenthet megoldást:

- a **bizonytalan eredetű, illegális** szoftvertermékek használatának kerülése,
- a cserélhető **adathordozókon** érkező adatok **vírusellenőrzése** (ld. később),
- **vírusvédelmi szoftver** használata: olyan vírusellenes program alkalmazása, mely az operációs rendszer betöltődésekor bekerül a memóriába, és a gép működése során végig aktív marad (memóriarezidens). Működése során figyeli a boot-szektort, figyelemmel kíséri a futtatható állományokat (pl. azok méretét) és a háttérben futó alkalmazások tevékenységét. Gyanús esetben értesíti a felhasználót az általa rendellenesnek ítélt folyamatról.
- **tűzfal** használata: Olyan hálózatvédelmi szoftver alkalmazása, amely figyeli és korlátozza az internetes adatforgalmat. Így például visszautasítja az olyan IP-címekről érkező küldeményeket, amely címekről a felhasználó részéről adatkérés nem történt (pl. férgek kiszűrése). Megakadályozza továbbá, hogy a felhasználó nem publikus (nem megosztott) adatait pl. valamely trójai „hátsóajtó” program idegen címre továbbítsa.
- **Legyen naprakész az operációs rendszerünk!** Sok sebezhetőséget utólag javítanak ki egy-egy rendszerben, ezért fontos például, hogy a Windows, Android stb.. rendszeresen frissítse magát. (Vírusok nem csak számítógépre készülnek, hanem mobiltelefonokra, tabletekre, okos eszközökre is!)

A **fertőzés megszüntetése**: A vírus számítógépen való jelenlétének sokféle tünete lehet, ezek közül néhány jellegzetes példa:

- a **gép lefagy** vagy váratlanul **újraindul**,
- szokatlan jelenségek a **képernyőn**,
- a futtatható **fájlok mérete növekszik** (fájlvírus épült hozzájuk),
- fájlok tűnnek el vagy **ismeretlen fájlok jelennek meg**,
- a **háttértárak** szabad **kapacitása** hirtelen **lecsökken**,
- a **gép lelassul**, működése nehézkessé válik, stb.

A fenti jelenségek egy részét persze okozhatják hibás szoftverbeállítások, nem megfelelő hardverillesztő programok, vagy hardverhibák is.
A mai víruskereső és vírusmentesítő programok folyamatosan bővülő adatbázisokat tartanak karban a más ismert vírusok felismeréséhez. A célfájlokat átolvasva olya kódsorozatot keresnek, amelyek a vírusokra jellemzőek. Ha fertőzött fájlt találnak, a felhasználó választásától függően vagy eltávolítják a vírust, vagy törlik a fertőzött fájlt a vírussal együtt, vagy „elzárják”, megakadályozva a megnyitását. A keresést **minta- vagy szignatúrakeresésnek** nevezik. A módszer előnye, hogy ha találatot ad, akkor az biztos. Előnye még a relatív gyorsaság is. Hátránya, hogy a víruskereső programnak ismernie kell azt, amit keres. A károkozók fejlődése igen dinamikus. Nemcsak újabb károkozók megjelenése bonyolítja a helyzetet, de sok károkozó „tudatosan" változtatva alakját nehezíti ennek a taktikának az alkalmazását. (A polimorf, sokalakú vírusok vagy az úgynevezett kódolt vírusok aktivizálódás előtt egyedi kulccsal kibontják magukat.) Ma már célszerű napi gyakorisággal frissiteni a vírusellenes programok adatbázisát. Azon kis idő alatt, ami egy új károkozó felbukkanása és az általunk használt vírusellenes program adatbázisának következő frissítése között eltelik, védtelenek vagyunk a kérdéses károkozóval szemben (ez a nagyon gyakori frissítés indoka).
A **heurisztikus módszer** nem keres vírusmintákat, hanem a lehetséges célfájlokhoz olyan szituációkat teremt, hogy a vírus aktivizálja magát, és a rá jellemző műveletek felismerhetőek legyenek. Nagy előnye, hogy azokat a vírusokat is felismeri, amelyekről még nem tudnak a keresőprogramok. Hátránya a relatív lassúság és a téves riasztás lehetősége, amivel elbizonytalaníthatja a felhasználót.
A víruskeresők **mindkét taktikát** alkalmazzák.

A vírus eltávolítása csak akkor sikerülhet, ha a vírus nem aktív, azaz nincs működő példánya a memóriában. Ha a vírus a rendszerlemez bootszektorát fertőzte meg, vagy olyan futtatható állományt, amely az operációs rendszer betöltődésekor végrehajtódik, akkor az aktivizálódás csakis a gépnek egy „tiszta” rendszerlemezről történő bootolásával (indításával) kerülhető meg.

A mai vírusellenes programoktól többféle integrált szolgáltatást is elvárhatunk:

- A rendszer indításakor végezze el a memória, a merevlemezek boot-szektorainak és a rendszerfájlok ellenőrzését.
- Az operációs rendszer betöltődésekor automatikusan induljon el egy, a háttérben futó, önvédelmi alkalmazás (víruspajzs), amely figyeli a megnyitott állományokat. Ezenkívül beépülhet az általunk használt web-böngészőbe is, megakadályozva a scriptvírusok aktivizálódását.
- Természetesen tartalmaznia kell egy víruskeresőt is, amelyet a felhasználó bármikor elindíthat vagy ütemezhet (pl. hetenkénti automatikus futtatást).
- Ellenőrizze a beérkező e-mail-eket, megakadályozva az e-mail vírusok aktivizálódását

Néhány hírhedt vírus kártevő hatásának ismerete:
Chameleon:

- 1990
- Első polimorf vírus
- Minden fertőzés
- Alkalmával változott a kód, így megnehezült a vírusmintákon alapuló keresés

Michelangelo:

- 1992
- Első komolyabb károkat okozó vírus
- Rendszerfájlok, boot rekordok, FAT (MS-DOS) sérülése
- A lemez használhatatlanná tétele

ILOVEYOU(LoveLetter):

- 2000 májusában fertőzött
- E-mailben terjedt
- 45 millió felhasználó érintett
- Feltételezett programozóját letartóztatták, de bizonyíték hiányában felmentették

Példák a víruskereső és vírusirtó programokra:
Norton Antivirus, NOD32, Bitdefender (ingyenes), Panda Antivirus, VirusScan, F-Secure F-Prot, Kaspersky, Avast, AVG.
Víruspajzs: egy memóira-rezidens (gép indulásakor memóriába töltődő, kikapcsolásig működő, háttértevékenységet folytató program) figyeli a fájlokkal kapcsolatos műveleteket pl. ha megváltozik egy futtatható fájl mérete (valószínűsíthető vírus), figyeli az internetes adatforgalmat, a lemezek boot-szektorait stb.
Vírusdefiníciós adatbázis: egy adott vírusirtó folyamatosan frissülő adatbázisa, amelyből felismeri az adott vírusokat (a célfájlokat átolvasva olya kódsorozatot keres, amely a vírusokra jellemző), így hatékony védelmet
nyújt és képes a vírus kiirtására. Ha egy vírusirtó adatbázisában nincsen bent az adott vírus szignatúrája (mintája), akkor a vírusirtó legfeljebb heurisztikusan tud védekezni ellene. Ezért fontos a folyamatos frissítés, vagy egy új próbaverzió letöltése

Vírusirtó program használatának ismerete:
A vírusvédelmi rendszerek (szoftverek) összetett védelmi rendszerrel rendelkeznek pl.: kéretlen alkalmazások futtatásának tiltása, valós idejű ellenőrzés, választható ellenőrzés (meghajtóra, mappára stb.). Az alapbeállítások a telepítéskor érvényesülnek, melyeket utólag lehet személyre szabni. Mivel összetett szolgáltatásrendszerrel rendelkeznek ezek a szoftverek, a különböző egyedi beállításokat csak tapasztalt felhasználók, vagy rendszergazdák tudják megfelelően elvégezni.

Vírusellenőrzés a háttértárakon és a memóriában:
A háttértárakon ellenőrzése általában külön víruskeresési parancsra történik, illetve a memória és lapozó-fájl tartalma állandó ellenőrzés alatt lehet. Háttértároló ellenőrzésekor a víruskeresési idő

csökkenthető szűrési paraméterekkel pl.: csak az *.exe, *.doc, *.xls kiterjesztésű állományokat vizsgáljuk, vagy csak egy adott könyvtár tartalmát.

A vírusvédelem gyenge pontjai, hiányosságai (pl. emberi tényező):
A vírusok gyakran építenek az emberek tudatlanságára, és figyelmetlenségére pl. elhitetik a felhasználóval, hogy fertőzött a gépe és ha elindítja a programot (valójában a vírust), ami valójában megfertőzi a gépet. Ez ellen a vírusirtók kevésbé tudnak védekezni.
Mára a legnagyobb esély a gép megfertőződésére az emberi tényezőn alapul.
A vírusvédelmi adatbázis frissítésének elmulasztása lehetőséget biztosít az új vírusoknak, hogy észrevétlenek maradjanak.