Vírusok

Vázlat:

I. Vírusok fogalma, ismérvei

A **vírusok** károkozás céljára létrehozott (a munka zavarása, ellehetetlenítése; adataink megszerzése, megsemmisítése, stb.), önreprodukáló (szaporodni képes) és más programok megfertőzésére képes programok.

A szűkebb értelemben vett vírusok az alábbi három **tulajdonsággal** bírnak:

- végrehajthatóak, vagyis működőképesek ,
- önmagukat másolva képesek terjedni,
- képesek hozzáépülni más végrehajtható állományokhoz.

A felsorolt ismérvek alapján kitűnik, hogy nem véletlen a „névrokonság” a számítógépen futó kártékony programkódok és a biológiai élősködők között.

II. A vírusok eredete

1. *A szoftverek másolásvédelme*: A 70-es években a szoftveripar fellendülésével együtt felbukkant az illegális szoftvermásolás problémája. A programkészítő cégek ennek a jogellenes tevékenységnek úgy akarták elejét venni, hogy szoftvereikhez másolást „büntető” programrészeket építettek. Ezek másolás esetén akcióba léptek: jobb esetben csak a védelmük alatt álló programot tették működésképtelenné, nem ritkán azonban a felhasználó többi állományát is károsították „büntetésül” (akárcsak a mai vírusok). A szoftvercégek ilyenfajta programvédelmét hamarosan betiltották, hiszen előfordult, hogy emiatt a jogos felhasználó is kárt szenvedett, továbbá nem megengedhető, hogy jogellenes magatartást ugyancsak törvénytelen módszerekkel toroljanak meg.
2. *A hadviselés*: A hadiiparban régóta használják a vírusokat: egyrészt az ellenfél számítógépes rendszerébe bejuttatva annak teljes tönkretételét célozva meg, másrészt a saját rendszerüket pillanatok alatt teljesen elpusztító vírusokat is „kifejlesztettek”, arra az esetre, ha a kifejlesztett haditechnika az ellenség kezére jutna. Nagy felháborodást váltott ki szakmai körökben a Pentagon 1990-ben megjelent pályázata, melyben 50 ezer dollárt ígért annak a programozónak, aki hadi célokra alkalmas vírust fejleszt ki.
3. *Bosszúra szomjas szakemberek vagy programozók magamutogatásból* készítenek (írnak) vírusokat Az esetek nagy részében közvetlen anyagi haszon nem származik a vírusok írásából. (Legfeljebb, ha az illető vírusvédelmi szakember is.)

III. Vírusok csoportosítása

1. A régi idők vírusai

Fájl-vírus (állomány vírusok)

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 feladatot.
Terjedésük a floppy, később CD lemezek másolásával és futtatásával történt (ez viszonylag lassú folyamat volt), majd a modemek és az Internet térhódításával ez felgyorsult.

BOOT-vírusok
A számítógép alaprendszerét (winchesterek vagy floppyk ún. boot-szektorát vagy partíciós tábláját) támadják meg, s még azelőtt betöltődnek a memóriába, hogy bármilyen program elindult volna. A boot-vírusok aktiválódásuk után átveszik a hatalmat, és azonnal támadásba lendülnek. Szerencsére az újabb gyártású alaplapokon bekapcsolható, gyári vírusvédelem van, amely azonnal jelez, ha ilyen típusú vírus támadna. (Viszont nem ad védelmet a többi fajtával szemben !!!) Hajlékonylemezek esetében a fizikai írásvédelem bekapcsolása megakadályozza a fertőzést.

Lopakodó vírusok
Az azonnali, erőteljes károkozás helyett inkább a lopakodó taktika és a feltűnésmentes terjedés jellemzi. Pl: péntek 13. vírus (ami csak akkor aktiválta magát, ha az adott nap péntekre és 13-ára esett).

Poliform vírusok
Ezek a vírusok képesek arra, hogy megváltoztassák a saját kódjukat. A több millió kódváltozatot a víruskereső programok nehezen, csak speciális technikákkal tudják felismerni.

2. Makróvírusok
Az MS Office programcsomag (pl. Word, Excel) automatikusan betöltő és elinduló makrói (irodai programokban a felhasználó által létrehozott „parancslista”, mely a dokumentumban gyakran elvégezendő gépies feladatok automatizálására használatos) kiváló lehetőséget adnak vírusok írására (ezek futtatásához csupán a Word vagy az Excel program szükséges, az operációs rendszer bármely Windows változat lehet. A makrók kezdetben csak a dokumentumokban tettek kárt (pl. töröltek sorokat, beszúrtak szövegeket, nem engedték elmenteni a dokumentumot stb.), de később a teljes fájlrendszert veszélyeztették. Ez a fajta vírus a mai napig igen népszerű. A makróvírusok az internetes adatforgalom fellendülésével indult rohamos terjedésnek.

3. E-mail-ben terjedő vírusok
Az Internet terjedésével növekedett a böngésző és levelezőprogramok biztonsági (no meg a felhasználók figyelmetlenségét) kihasználó vírusok száma.
Az e-mail-ben terjedő vírusok legtöbbször az elektronikus levelekhez csatoltan érkeznek. A levél elolvasásával (csatolmány megnyitásával) aktiválódnak, majd beépülnek az operációs rendszerbe, szintén e-mail formájában (általában a felhasználó címjegyzékéből megszerzett címeken) tovább fertőznek.

IV. Egyéb károkozók
Férgek
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 féregfertõzése (az Internet Worm).

Trójai

A mondabeli trójai falóhoz hasonlóan valójában mást kap a felhasználó, mint amit a program „ígér”. Nem vírus, mert nem terjed, viszont nagyon veszélyes. Egy ártatlan programnak „álcázott” károkozóról van szó, mely 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 megpróbálják leállítani a víruskereső és tűzfalprogramokat.

Egy másik példa: egy ártatlannak tűnő képernyőkímélő vagy játékprogram lehetőséget adhat arra, hogy valaki átvegye az uralmat gépünk felett vagy ellopja adatainkat.

Hoaxok (kacsák)

Az emberi hiszékenységet használja ki. Pl: Kapunk egy levelet, melyben leírják, hogy mostantól 1 hétig ne kapcsoljuk be a gépet, mert vírusterjedés várható és tönkreteszi a gépünket. Persze ezt az üzenetet elküldjük gyorsan ismerőseinknek, hogy szóljunk, hogy baj van. És ezzel elindítjuk a lavinát.

(Persze ez igaz lehet, de manapság minden nap jelennek meg új vírusok, de ez nem jelenti azt, hogy ne használjuk a gépünket! Használjunk vírusirtó programot!)

V. Csoportosítás a károkozás szempontjából

1. **Ártalmatlan:** Lényegében semmit nem csinál „csak” szaporodik és közli, hogy a gépen van és fertőz.
2. **A felhasználó munkáját zavaró** A munka lassítása, apróbb bosszúságok, újrabootolás, egy kisegér megeszi a betűket, a képernyő tükörképét látjuk stb.
3. **Rosszindulatú**
   - A fájlok tartalmának megváltozása, törlése.
   - A winchesterek teljes tartalmának az elvesztése.
   - A jogosultságok megváltoztatása, védelmi rendszerek kiiktatása.
   - Adatok továbbítása az interneten böngészési szokásainkról, kedvenc oldalainkról.
   - Bizalmas dokumentumok szétszórása az interneten.

VI. Vírusfertőzés jelei:

- Ha az asztalon, a gyorsindítóban vagy a startmenüben ismeretlen új ikonnal találkozunk.
- Ha egy vagy több alkalmazás elindítás után azonnal leáll, vagy nem indul el.
- Ha aktív internetes kapcsolatunk van (fel vagyunk jelentkezve a hálózatra), nem kezdeményezünk semmiféle műveletet (letöltés, levélküldés vagy ellenőrzés) az internet felé, viszont mégis hosszan tartó, aktív forgalmunk van, akkor legyünk óvatosak, mert ez jelezhet sikeres vírustámadást.
- Ha hosszan tartó, indokolatlan winchester-aktivitást tapasztalunk (azaz „kerreg” a winchester, villog a kis piros HDD Led) olyankor, amikor nem dolgozunk a gépen.
- Ha félreérthetetlenül „bejelentkezik” a vírus, pl. kiír egy üzenetet a képernyőre, akkor biztosak lehetünk a sikeres vírustámadásban.
- Ha a gép lefagy vagy váratlanul újraindul.
- Szokatlan jelenségek a képernyőn.
- A futtatható fájlok mérete növekszik (fájlvírus épült hozzájuk).
- Ha fájlok tűnnek el vagy ismeretlen fájlok jelennek meg.
- A háttértárak szabad kapacitása drámaian lecsökken.
- A gép lelassul, használata nehézkessé válik, stb.

A fenti jelenségek egy részét persze okozhatják hibás szoftverbeállítások, nem megfelelő hardverillesztő programok, vagy hardverhibák is.

A mai **vírusellenőrző programok** képesek az adatbázisukban szereplő vírusfajták azonosítására és hatástalanítására. Ez utóbbi azonban 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 kerülhető meg.

VII. Vírusfertőzés 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 használatát mellőzzük.
- A cserélhető adathordozókon érkező adatokat ellenőrizzük vírusirtóval.
  A számítógép rendellenes működése esetén mindenek előtt a vírusmentességről kell meggyőződni.
  Gondoskodni kell arról, hogy az alkalmazott vírusellenes program legfrissebb változata fusson a számítógépen (egy három hónapos verzió már elavultnak számít).
  A rendszeres (pl. heti) vírusellenőrzés elejét veheti az esetlegesen a számítógépre került vírus elszaporodásának, továbbterjedésének, a komolyabb károkozásnak
- Kerüljük az ismeretlen helyről származó Word dokumentumok és az Excel táblák megnyitását. Mindig legyen bekapcsolva a Word és az Excel makrovédelme (ez az Office 97-től kezdve került beépítésre). Ez a funkció figyelmeztetni fog, ha olyan dokumentumot nyitottunk meg, amely makrókat tartalmaz. Csak akkor engedélyezzük a makró futását, ha biztosak vagyunk abban, hogy az nem ártó szándékú.
- Soha ne nyissunk meg e-mail-hez csatolt küldeményt (csatolt fájlt), he nem ismerjük annak funkcióját, még akkor sem, ha látszólag ismerőstől kaptuk a levelet. Néha pl. üdvözlőkártyák álcázzák a vírust, ilyen volt pl. a Happy99 féregvírus, amely újévi üdvözlet és látványos tűzijáték mellett fertőzte végig a fél világot.
- Azonnal, gondolkodás nélkül töröljünk minden olyan fájlt, levelet, amelynek nincs feladója, vagy ha a levél általunk ismert személytől érkezett, és nem a megszokott nyelven „szól hozzánk”. (pl. angolul vagy spanyolul)
- Csak akkor tanácsos megnyitni bármilyen e-mail mellékletet, ha annak érkezése nem váratlan, és tartalma pontosan ismert
- **víruspajzs 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.

VIII. Vírusellenőrző és vírusirtó programok

- 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.