Számítógépes vírusok

A számítógépes vírus fogalmának meghatározása a szakirodalomban nem egyöntetű, több egymást részben átfedő definíciót is használnak. A legtágabb értelemben az olyan alkalmazások (futó programok) tekinthetők vírusnak, melyek működése felett felhasználójuk nem rendelkezik teljes mértékben, azaz működését nem tudja ellenőrizni, irányítani. Az alábbi táblázatban a felhasználói és vírus programokat hasonlítjuk össze a működésük feletti rendelkezés szempontjából:

Felhasználói program	*vírus program*
működésének módja és célja dokumentált (így dönthetem el, hogy akarom-e használni)	nem dokumentált
a program valóban csak a dokumentációban megadott funkciókra képes	rejtett funkciók
a használat előtt a számítógépen kívül, ismert helyen tárolom (pl. a fiókomban egy CD-n)	ismeretlen a forrás
általam meghatározott időben telepíthetem	fertőzve terjed
ismert helyen tárolódik a háttértáron és ott is marad	rejtett állomány, helyet változtat, megsokszorozza magát
az allokációs táblában bejegyzés készül a telepítési helyről és időről (így bármikor lekérdezhetem a létezésének tényét)	hamis bejegyzések
általam meghatározott időben futtathatom vagy nem	ismeretlen aktivitás
bármikor törölhetem a gépről	nehezen vagy nem törölhető

A fenti, legtágabb értelmű definíció szerint szinte minden program vírusnak tekinthető, kivéve az amit maga a felhasználó ír saját magának. Kevésbé tág értelemben számítógépes vírusnak tekinthető minden olyan program, melyet készítője ártó szándékkal hozott létre (a munka zavarása, ellehetetlenítése, adataink megszerzése, megsemmisítése stb.) Ebben a szűkebb értelemben vett megfogalmazásban a vírusok a következő három tulajdonsággal jellemezhetők: szaporodási képesség, (azaz a saját kód megsokszorozásának képessége), rejtőzködés, károkozás. A felsorolt ismérvek alapján kitűnik, nem véletlen a „névrokonság" a számítógépen futó kártékony programok és a biológiai élősködők között.

A vírusok eredete két okra vezethető vissza:

1.) 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”. A szoftvercégek ilyenfajta programvédelmét aztán hamarosan betiltották, hiszen előfordult, hogy emiatt a jogos felhasználó is kárt szenvedett, továbbá nem megengedhető, hogy jogellenes magatartást ugyancsak jogellenes módszerekkel toroljanak meg.

2.) 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 haditechnika az ellenség kezére jutna. Nagy felháborodást váltott ki pl. szakmai körökben a Pentagon 1990-ben megjelent pályázata, melyben 50 ezer dollárt ígért annak a programozónak, aki hadi célokra alkalmas vírust fejleszt.

A vírusokat több csoportba sorolhatjuk:

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 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.

Makró vírus: A makrók megjelenésével dokumentumaink is potenciális vírushordozóvá válhatnak. A makró az irodai programokban a felhasználó által létrehozott „parancslista”, mely a dokumentumban gyakran elvégezendő gépies feladatok automatizálására használatos. A makró vírus e lehetőséggel él vissza, dokumentumainkhoz épülve, annak megnyitásakor fut le kártékony kódja. A vírusok e 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 féreg fertőzése (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. A többi vírusfajtához hasonlóan más programokhoz kapcsolódva tehet rájuk szert a nem eléggé óvatos felhasználó.

Védekezés a vírusok ellen.

Legfontosabb a tudatos számítógép-használat: a vírusok ellen védelmet jelenthet, ha a számítógépünkre *víruspajzs program*ot telepítünk, amely állandóan figyeli a rendszert (letöltött és indított programokat, e-maileket, az operatív memória váratlan lefoglalását). A pajzs gondoskodik arról, hogy a vírushordozóként azonosított fájl ne induljon el, tehát amikor a vírusriasztást megkapjuk, akkor a vírus még nem aktiválódott, a pajzs ebben megakadályozta. Emiatt a riasztás nem a megfertőzöttség tényét, hanem csak a fertőzés lehetőségét hordozó fájl felbukkanását jelzi. A fertőzőnek jelzett fájlt ne indítsuk el újra, a vírusosnak jelzett honlapot ne nyissuk meg újra, csökkentendő a fölösleges kockázatot. A merevlemeznek a víruspajzshoz tartozó víruskereső programmal időnként történő teljes átvizsgáltatása is lényeges védelmi elem. A kártékony programok másik fajtája, a spyware-ek ellen külön erre a célra készített *antispyware keresőszoftver*ek segítenek. Használhatunk *tűzfal*at is, melynek célja, hogy a hálózaton keresztül a számítógépbe ne történhessen illetéktelen behatolás. Bár ez a program nem védi a gépet a vírusfertőzés ellen, nem jelzi a fertőzött fájlokkal való találkozást, viszont az általa védett hálózat gépei között a háttérben észrevétlenül, nem dedikált módon közlekedni próbáló programok mozgását, behatolását megakadályozhatja.