Számítógépes vírusok

1 Vázlat

A vírusok fogalma: 1
Eredetetük 1
Csoportosításuk egy lehetséges módja: 2
Lánclevél (hoax) 2
Adathalászat (datafishing) 2
Kémprogram (malware) 2
Trójai (trojan) 3
Féreg (Worm) 3
Exploitok (Kihasználó vírusok) 3
Vírus megelőzés módja 3
Vírusölő programok 3
Tűzfal 3
MSN messenger, Skype, Email 4
Windows frissítések 4
Vírusfertőzés módja: 4
Vírusfertőzés jele: 4
MIÉRT ÍRNAK VÍRUSOKAT? 2

2 A vírusok fogalma:

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

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

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

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

3 Eredetetük

1. *A szoftverek másolásvédelme*: A 70-es években a szoftveripar fellendülésével együtt felbukkant az illegális szoftvermásolás problémája. A programkészítő cégek ennek a jogellenes tevékenységnek úgy akarták elejét venni, hogy szoftvereikhez másolást „büntető” programrészeket építettek. Ezek másolás esetén akcióba léptek: jobb esetben csak a védelmük alatt álló programot tették működésképtelenné, nem ritkán azonban a felhasználó többi állományát is károsították „büntetésül” (akárcsak a mai vírusok). *A szoftvercégek ilyenfajta programvédelmét hamarosan betiltották, hiszen előfordult, hogy emiatt a jogos felhasználó is kárt szenvedett, továbbá nem megengedhető, hogy jogellenes magatartást ugyancsak törvénytelen módszerekkel toroljanak meg.*
2. *A hadviselés*: A hadiiparban régóta használják a vírusokat: egyrészt az ellenfél számítógépes rendszerébe bejuttatva annak teljes tönkretételét célozva meg, másrészt a saját rendszerüket pillanatok alatt teljesen elpusztító vírusokat is „kifejlesztettek”, arra az esetre, ha a kifejlesztett haditechnika az ellenség kezére jutna.

Nagy felháborodást váltott ki szakmai körökben a Pentagon 1990-ben megjelent pályázata, melyben 50 ezer dollárt ígért annak a programozónak, aki hadi célokra alkalmas vírust fejleszt ki.

3. *Bosszúra szomjas szakemberek vagy programozók magamutogatásból* készítenek (írnak) vírusokat Az esetek nagy részében közvetlen anyagi haszon nem származik a vírusok írásából. (Legfeljebb, ha az illető vírusvédelmi szakember is.)

3.1 MIÉRT ÍRNAK VÍRUSOKAT?

A számítógépről a **vírus** készítői hasznos **információkat szerezhetnek meg**. Például email címeket, melyeket **spamküldés** céljára felhasználhatnak, illetve akár a saját gépünk válik spamküldő állomássá.

Egy fertőzött gépről és sok ezer társáról **DDOS támadás (Distributed Denial of Service) is indítható**, mellyel a kiszemelt célszámítógép szolgáltatásai teljesen elérhetetlenné válnak. A DDOS támadásnak a célja elsősorban nagy intézmények, bankok szervereinek megbénítása, vagy annyira lelassítása, hogy használatuk gyakorlatilag lehetetlenné váljon.

Esetenként egy-egy **vírusos gépről** olyan információk is nyerhetők, melyek segítségével **védettebb rendszerek** pl.: Bankok, hitelintézetek is **feltörhetők**, abban az esetben, ha a vírusos gépet használónak hozzáférése van egy ilyen zárt rendszerhez.

Hasznos adatok szerezhetők meg a saját **gépünkről is**. Ilyenek pl.: **Bankkártya adatok**, **Internetezési szokások**, **Felhasználó nevek** és **jelszavak**, **email címek**, stb...

4 Csoportosításuk egy lehetséges módja:

4.1 Lánclevél (hoax)

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

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

4.2 Adathalászat (datafishing)

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

Védekezés: Tisztában kell lennie azzal, hogy bankok és egyéb hivatalos szervek **soha nem küldenek** üzenetet ügyfeleinek azzal a céllal, **hogy megkérjék, jelentkezzenek be** és adják meg személyes adataikat! Ha bizonytalan inkább hívjuk fel a bank, vagy szervezet ügyfélszolgálatát a teendőkkel kapcsolatban. Győződjünk meg a kapott **hivatkozás helyességéről!** Ha a domain név (pl.: www.mkb.hu) nem egyezik, akkor semmiképpen ne adja ki adatait! A megfelelő Internet böngészők (pl.: Internet Explorer, Firefox) rendelkeznek **adathalász szűrővel**, így képesek figyelmeztetni Önt, hogy adathalász oldalra került. Érdemes ellenőrizni, hogy ez a funkció engedélyezett-e a böngészőben!

4.3 Kémprogram (malware)

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

Védekezés: Szerezzen be megbízható helyről malware vírusok felfedezésére és írtására alkalmas vírusírtó programot.

4.4 Trójai (trojan)

A **trójai vírus** nagyon találó nevet kapott. Ön is emlékszik még a történetre? A trójaiak elkövették a hibát, hogy a görögök ajándékát beengedték a városukba, majd lóban rejtőző katonák reggelre bevették a várost. A **trójai vírus** az esetek nagy részében **nem annak látszik, ami valójában**. Hasznos alkalmazásnak álcázva jut be számítógépébe, és képes az **irányítást** teljes egészében egy **külső irányító kezére játszani**. Sok esetben a trójai programok nem tartalmaznak rosszindulatú programkódot, viszont megtalálható bennük egy ún. **hátsó kapu** (backdoor) melyen keresztül a külső irányító **bejuthat gépünkre**. A hátsó ajtó nyitása és a külső irányítás természetesen Interneten keresztül történik.

4.5 Féreg (Worm)

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

Az önsokszorosításon kívül a **féreg** sokféle dologra beprogramozható, például **fájlok törlésére** a gazdarendszeren, vagy **önmaga elküldésére e-mailben**. Az újabban megfigyelt férgek több végrehajtható állományt is visznek magukkal. Még valódi ártó szándékú kód nélkül is **súlyos fennakadásokat okozhatnak** csupán azzal, hogy sokszorozódásuk kiugróan magas hálózati forgalmat generálhat.

4.6 Exploitok (Kihasználó vírusok)

Az **exploitok** olyan **kártékony alkalmazások**, melyek az Internet böngészők és a számítógépes rendszer gyenge pontjait, **biztonsági réseit használják ki**. Léteznek olyan weblapok, melyek az ingyenes letöltés lehetőségével vonzzák magukhoz a látogatót, ám letöltés helyett csak a weboldalban elhelyezett exploit települ számítógépére. Sajnos nagyon sok internetes oldal kódja feltörhető, és ebből kifolyólag biztonságos oldalakba is elhelyezhető exploit vírus. Windows környezetben a védekezést egy biztonságos Internet böngésző használatával érdemes kezdeni. Ilyen pl.: a**Mozilla Firefox**, **Opera**, vagy a **Google Chrome** is.

5 Vírus megelőzés módja

5.1 Vírusölő programok

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

A mai **vírusellenőrző programok** képesek az adatbázisukban szereplő vírusfajták azonosítására és hatástalanítására. Ez utóbbi azonban csak akkor sikerülhet, ha a vírus nem aktív, azaz nincs működő példánya a memóriában. Ha a vírus a rendszerlemez bootszektorát fertőzte meg, vagy olyan futtatható állományt, amely az operációs rendszer betöltődésekor végrehajtódik, akkor az aktivizálódás csakis a gépnek egy „tiszta” rendszerlemezről történő boo-tolásával kerülhető meg.

A vírusírtó legyen:

- gyors, hatékony ésegyszerűen kezelhető
- elindított programokat a háttérben mindig ellenőrzze, és csak abban az esetben hagyja azokat futni számítógépén, ha nem talált bennük vírust.

Internetre kapcsolt számítógép esetén elengedhetetlen a megfelelő írusölő alkalmazás használata, mivel használatuk nélkül képtelenség a vírusmentes Internetezés.

5.2 Tűzfal

Windows rendszer esetén mindenképpen szükséges egy **tűzfal program** használata. Segítségével **megvédhető számítógépe** az Internetről érkező **támadásokkal szemben**, továbbá figyelhető és korlátozható a ki- és bejövő adatforgalom. A tűzfal segítségével beállítható, hogy a számítógépre telepített programok közül melyek kapcsolódhatnak az Internetre és melyek nem. Ezáltal a **vírusoknak nehezebb dolga van**, hiszen ha kapcsolódni szeretnének, akkor a tűzfal blokkolja őket.

Tévhitek a tűzfalakkal kapcsolatban:

- A tűzfal helyettesíti a vírusölőt. Nem igaz, csak kiegészítő védelmet nyújt.
- Ajánlott több tűzfal egyidejű használata. Nem igaz, csak egy tűzfal programot szabad használni, mivel összeakadhatnak egymással és kapcsolódási hibákat okozhatnak.
- A Windows beépített tűzfala rossz. Véleményünk szerint ez sem igaz. Léteznek komolyabb és akár nagyobb biztonságot nyújtó tűzfal megoldások, ám használatuk a kezdő felhasználók számára túlságosan bonyolult. Egy hibásan beállított tűzfal pedig sokkal rosszabb, mint a Windows gyári tűzfal megoldása.

5.3 MSN messenger, Skype, Email

Sok **vírus terjed** a különböző **beszélgető (chat) programokon** és email útján. Az egyik széles körben használt trükk, hogy **ismeretlen felhasználóktól** olyan fájlokat kapunk, melyek **vírust tartalmaznak**.

Néhány kerülendő példa:

- Ne fogadjunk ismeretlentől állományokat (pl.: Barbie89-től myPhotos.exe-t és hasonlókat)
- Ismerőseinktől érkező állományokkal szemben is **legyünk gyanakvóak!** Előfordul, hogy barátunk számítógépén lévő vírus küld üzenetet nekünk. Ezek főként angol nyelvűek így könnyen felismerhetőek. Ha ismerőstől olyan állományt kapunk, amelynél felmerül, hogy nem tőle származik, akkor megnyitás előtt érdemes egyeztetni vele valóban ő küldte-e.
- Ne látogassunk meg **gyanús üzenetben** közölt hivatkozásokat. Ezek is tartalmazhatnak vírusokat.

5.4 Windows frissítések

A **biztonsági rések** felszámolásával **számítógépünk biztonságosabbá válik**, ezért **engedélyezze Ön is** számítógépe **automatikus frissítését**, hogy minél hamarabb hozzájusson a **biztonsági javításokhoz**. Az automatikus frissítés beállításait a vezérlőpulton találja. Windows XP esetén automatikus frissítések, míg Vista esetén Windows frissítések néven. Ha nem kívánja az automatikus frissítést használni, akkor javasolt a manuális frissítő szolgáltatás használata. A kézzel indított frissítést érdemes **legalább havonta egyszer** lefuttatni a ***Microsoft Windows Update*** oldalon.

6 Vírusfertőzés módja:

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

7 Vírusfertőzés jele:

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

8 Forrás:

http://www.pcvilag.hu/szamitogep-virus-eltavolitas