14. Vírusok

- **Mit nevezünk számítógépes kártevőnek, hogyan csoportosíthatjuk ezeket a kártevőket?**
- **Mi a vírus, jellemezze a vírusok főbb csoportjait!**
- **Hogyan juthat vírus (kártevő) a számítógépbe, milyen károkat okozhat, mit tehetünk ennek megakadályozására, illetve a fertőzés megszüntetéséért? Mi a tűzfal?**
- **Ismertesse az iskolai számítógépre telepített vírusellenőrző programot!**

Számítógépes kártevő

Azokat a programokat, amelyeket azért készítettek, hogy a számítógépek működését megzavarják, vagy éppen lehetetlenné tegyék, számítógépes kártevőknek nevezzük. A vírusok is kártevő, de nem mindegyik kártevő vírus.

Számítógépes kártevők fajtái

- A **vírus** olyan számítógépes kód (program), amely egy másik programhoz vagy fájlhoz csatolja magát, és így terjed át egyik számítógépről a másikra, ezzel megfertőzve a másik gépet is. Terjedéséhez általában valamilyen emberi közreműködés szükséges, például egy fájl megosztása vagy egy e-mail megnyitása.
- A **féreg** a vírusok egyik alosztálya, amely hasonlóan a vírushoz, számítógépről számítógépre másolja magát. Ezt azonban automatikusan, a felhasználók közreműködése nélkül is képes megtenni, átvéve az irányítást a számítógép fájl- és adatküldő szolgáltatásai felett. Például elküldi magát az e-mail címjegyzékben szereplő összes címre, és a címzettek számítógépein szintén megteszi ugyanezt, ami még a hálózati forgalmat is megnöveli, és emiatt lelassítja a helyi hálózatot és az Internetet. A férgek befurakodhatnak a rendszerbe, és lehetőséget adhatnak másoknak arra, hogy részben átvegyék az irányítást a számítógép fölött.
- A **trójai faló** olyan számítógépes program, amely hasznosnak tűnik, de valójában kártékony. Ahogy a mitológiában a trójai faló ajándéknak tűnt, de görög katonák rejtőztek a belsejében, akik aztán elfoglalták Trója városát, a trójai programok is hasznos programnak tűnnek. Ezek úgy terjednek, ha a részedett felhasználók megnyitják a programot, mert azt gondolják, hogy hivatalos forrásból származik. Pl. nemrég trójai falovak olyan e-mailek formájában érkeztek, amelyek melléklete a levél szerint Windows biztonsági frissítéseket tartalmazott, valójában viszont vírusokat. A trójai falovak ingyen letölthető szoftverek részei is lehetnek. Ezért nem szabad programot letölteni olyan forrásból, amely nem megbízható.
- **kémprogramok** A kémprogram olyan program, amely személyes adatokat gyűjt a felhasználóról tudta nélkül és anélkül, hogy eldönthetné, hogy ezt megengedi-e vagy sem. A kémprogram által összegyűjtött adatok sora terjedhet a meglátogatott webhelyek listájától egészen a felhasználónevekig és jelszavakig. Akkor válhat valaki kémprogramok célpontjává, ha zenéket tölt le fájlcserélő programokkal, vagy ingyenes játékokat olyan webhelyekről, amelyekben nem bízik meg, illetve ismeretlen forrásból származó programokat használ.

Hogyan terjednek a vírusok?

- **A vírusfertőzés frekventált helyei régen és ma:**
  - a winchester partíciós táblája
  - operációs rendszer
  - a winchester vagy a floppy lemez boot szektora
  - EXE, COM és más futtatható állományok-ok
  - Word és Excel állományok (makróvírusok)

- A vírusok többsége elsődlegesen e-mail mellékletekben - az e-mailekkel együtt küldött fájlokban - terjed. Az ismeretlen mellékletek megnyitása a legáltalánosabb módja annak, hogy valaki elkapja a veszélyes programokat. A mellékletek lehetnek fényképek, Microsoft Word dokumentumok, Excel táblázatok, stb. A felhasználókat gyakran csellel veszik rá a csatolt fájl megnyitására, néha az érdekesnek vagy valóságosnak hangzó tárgysor, néha az ismerős feladó miatt (ha a vírus hozzáfér a fertőzött rendszer címjegyzékéhez, és ily módon egy megbízható személytől érkező e-mailnek álcázza magát). A behatolók mesterei az álcázásnak. A Mydoom (magyarul: A végzetem) nevű féreg, amely 2004 februárjában bukkant fel, különösen ármányos módon vette rá a felhasználókat, hogy a mellékelt fájlt megnyissák. A féreg írója gondosan kifundált egy csomó valósnak tűnő e-mail hibaüzenetet, például "Levélküldő rendszer", "Ellenőrzés" vagy "A levelet nem sikerült elküldeni". Ilyen jellegű üzeneteket az emberek szinte naponta kapnak, amelyek arról tájékoztatják a felhasználót, hogy az elküldött levelek valamelyike nem jutott el a címzetthez. A vírus készítője ezek nyelvezetét utánozta, és ezzel képes volt rávenni több millió embert, hogy nyissák meg a mellékletet. A Mydoom újabb verziói az ijesztgetés technikáját választották, például olyan tartalmú leveleket küldtek, amelyek látszólag az internetszolgáltatótól jöttek, arra figyelmeztetve a felhasználót, hogy vírus van a számítógépén, és annak eltávolítására az egyetlen mód a melléklet megnyitása. Valójában a melléklet tartalmazta magát a férget.
- Egyes internetes oldalak meglátogatásával is vírust lehet "szerezni", mert a weblapokon az interaktivitás érdekében gyakorta alkalmazott sript-ek (apró programok) szintén lehetnek rosszindulatúak. Ez természetesen nem a cégek hivatalos honlapjainál, hanem jellemzően az illegális- és szexuális tartalmú weblapoknál fordul elő.
- A vírusok az internetről letöltött programok vagy barátoktól kölcsönkapott vírusfertőzött számítógépes lemezek útján is terjedhetnek, de ezek a terjedés kevésbé gyakori módjai.

A kártevők által okozott károkról

- Amellett, hogy saját maguktól terjednek, a vírusok, férgek általában úgy vannak programozva, hogy más műveleteket is elvégezzenek.
- Ahogy az emberre veszélyes vírusok súlyossága is eltérő, a számítógépes vírusok közt is van, amelyik csak kissé bosszantó, de vannak erősen pusztító hatásúak. A helyreállítás pedig igen költséges is lehet.
- Pár évvel ezelőtt az ún. makróvírusok uralták a toplistákat, melyek a Microsoft Office dokumentumokat támadták. Egy emlékezetes Excel-makróvírus néha, néhány tizedszázalékkal megváltoztatta az egyes cellák tartalmát, így pár hét, hónap után a kártevő gyakorlatilag teljesen megváltoztatta a táblázatokat.
- Vannak férgek, melyek zombikká változtatják a számítógépeket, hogy ez által spamek küldésére vagy távoli rendszerek megbénítására használhassák az igába hajtott PC-ket, a tulajdonos tudta nélkül. (Ilyen volt pl. a nemrégiben terjedő MyDoom féreg, melyet úgy terveztek, hogy a megfertőzött rendszereken hátsó ajtót nyisson, és webhelyek megtámadására használja fel azokat.)
- A vírusok a legnagyobb értéket, a gépeinken tárolt adatokat is megtámadják. A hosszú hetek, hónapok munkájával létrehozott dokumentumok, hang- és videofájlok válhatnak semmivé egy-egy vírus aktivizálódásának hatására.

Milyen jelei vannak a vírusfertőzésnek?

- A vírusfertőzés hatására a számítógép lelassulhat, lefagyhat, illetve pár percenként újraindulhat, a gépen lévő programok furcsán viselkedhetnek. Ezek a tünetek mind azt jelezhetik, hogy a számítógép fertőzött, de mindezen jelenségeket okozhatja hardver- vagy szoftverhiba is, amelynek semmi köze a vírusokhoz.
- Annak, hogy valaki megtudja, van-e vírus a számítógépén, csak egyetlen biztos módja van: ha naprakész víruskereső program van telepítve a számítógépre.

Hogyan lehet megelőzni a vírusfertőzést?

A vírusok ellen védekezni lehet és kell is. Semmi nem garantálja a számítógép 100%-os biztonságát, de az alábbiak betartásával minimálisra csökkenthető a veszély.

a) gyanús levelek mellékletét nem nyitjuk meg

Csak akkor nyissa meg az e-mailek mellékleteit, ha tökéletesen megbízik a levél küldőjében, mellékletet is várt tőle, és ha pontosan tudja, mit tartalmaz a fájl. A vírusok és a férgek képesek adatokat lopni az e-mail programokból, és elküldik önmagukat mindenkinek, aki az e-mail címjegyzékben szerepel. Így ha egy ismerőstől kap e-mail-mellékletet, akkor is jobb, ha megkérdezi tőle, hogy tényleg ő küldte-e azt.

Ha olyan e-mailt kap valakitől, amelyet nem ért, vagy olyan fájlt mellékletként, amelyet nem várt, mielőtt megnyitná, mindig lépjen kapcsolatba a feladóval, és kérdezze meg tőle, hogy mi a melléklet tartalma. Ha ilyen levelet kap egy ismeretlentől, a legbiztosabb azt törölni.

b) víruskereső program használata

Egyes számítógépekre már gyárilag van telepítve víruskereső program. Ennek ellenőrzésére a Start menü/Programok menüpont alatt keresse a víruskereső (vagy antivirus) szót, vagy a népszerű víruskeresőprogram-gyártók nevét, amilyen például a McAfee, a Norton, az eTrust, a Symantec vagy a Panda.

A víruskereső program csak akkor véd meg a vírusoktól, ha rendszeresen frissítik. Az új vírusok adatait tartalmazó naprakész vírusleírásokat általában egyszerűen a programkészítő cég webhelyéről tudja letölteni. A frissítések letöltéséhez érvényes előfizetéssel kell rendelkeznie a víruskereső programhoz. Mivel a vírusírók mindig kitalálnak valami újat, hogy meg tudják fertőzni a számítógépet, ajánlott hetente elvégezni a frissítést. A víruskereső program legutolsó frissítésének dátumát a program valamelyik menüpontja alatt kijelzi. A víruskereső programokat gyártó cégek többsége automatikus letöltőszolgáltatást is kínál, amely automatikusan frissíti a víruskereső programot, amikor csatlakozik az Internetre.

Ha nincs víruskereső program a számítógépére telepítve, vagy ha másik programot szeretne helyette telepíteni, a választás során vegye figyelembe a szoftver szolgáltatásait (pl. automatikus frissítés) és a gyártó hírnevét. A víruskereső programok gyártói többnyire lehetővé teszik a víruskereső programok ingyenes verziójának kipróbálását, hogy mielőtt megvenné, eldönthesse, megfelel-e Önnek.

Két víruskereső program nem jobb, mint egy. Ha már van valamilyen víruskereső programja, de ki szeretne próbálni egy másikat, az új program telepítése előtt mindig távolítsa el a régit. Ha több víruskereső programot is futtat egy időben, az súlyos programütközéseket okozhat.

A mai vírusmegelőző rendszerek (Win 95/98 alá) többféle elven gátolják a vírusok bejutását, elszaporodását, illetve az esetleges károkozást.

- figyelik a memóriát, nem bukkan-e föl benne valamilyen "körözött" program,
- figyelik a programok által kiadott parancsokat, nem készül-e merénylet a gép legsebezhetőbb pontjai ellen (pl. állomány nyilvántartás manipulációja)
- időszakonként teljes "razziát" ajánlanak fel az egész winchester átfésülésére,

esetleg figyelik a kritikus rendszer file-okat, nem sérültek-e, nem ragadt-e rájuk hívatlan vendég.

Tűzfal

A tűzfal olyan szoftveres és/vagy hardveres technika, amellyel az intézmények a helyi hálózatukat megvédhetik a külső hálózatról (jellemzően az Internetről) érkező betörések ellen, a bejövő és kimenő adatforgalom figyelésével, megszűrésével és korlátozásával. A számítógépre a vírusírtó mellett érdemes tűzfalat is telepíteni.