

13. Vírusok és egyéb szoftveres károkozók (3.1)

Definiálja a vírus fogalmát!

Ismertesse a vírusok közös jellemzőit!

Jellemezze a vírusok főbb osztályait!

Milyen jelei vannak a vírusfertőzésnek, hogy ismerhető fel?

Hogyan tud védekezni a vírusok ellen?

Hogyan csoportosítjuk az antivírus programokat?

Manapság naponta keletkeznek új vírusok, amelyek egyre nagyobb károkat okoznak, és egyre ügyesebben rejtik el magukat a **víruskereső programok** elől. Az internet és a számítógépes hálózatok elterjedésével határok nélkül, egyre nagyobb területeken támadnak.

Számítógépes vírus: Olyan speciális, önmagát szaporítani képes program, amely más programokba beépülve különböző káros hatásokat idéz elő.

Részei:

- fertőző rész: a vírust a gazdaprogramba másolja,
- romboló rész: a károsító hatást fejt ki.

Vírusok leginkább négyféle módon kerülnek a számítógépekre

- a webböngészőn keresztül, böngészés közben,
- spameken keresztül (spamekben érkeznek)
- letöltött fájlokkal
- és fertőzött adathordozókkal.

A vírusok általános jellemzői

- Rosszindulatú szoftver
- Általában ártó szándékkal készítették őket;
- Zavaróak, túlterhelhetik a gép erőforrásait
- Szaporodik és fertőz
- Információt továbbíthatnak a gépünkről (spyware)
- Nagyon kis méret;
- Futtatható állományokat képesek megfertőzni;
- Gyakran akár válogatva, időzítve tönkretesznek más fájlokat;
- Rejtetten működnek, esetleg akkor fedik fel magukat, ha feladatukat elvégezték;
- Egyre fejlettebb intelligenciával rendelkeznek, pl. változtathatják saját kódjukat és aktivitásukat

Boot vírusok

A bootszektor-fertőző vírusok a számítógépeknek azt a részét használják ki, hogy az operációs rendszer is lemezről töltődik be. A vírusok arra a lemezterületre írják magukat, ahol normális esetben az operációs rendszert indító rész van, tehát amikor a gép (BIOS) megpróbálja betölteni a rendszert, helyette a vírust fogja elindítani. A vírus utána elindítja a rendszert is, de ekkor már a memóriában van.

Programvírusok (Állomány, fájl)

A **fájl-fertőző** vírusok futtatható programokat fertőznek meg (.EXE, .COM, .SYS, stb. kiterjesztésűeket). Ha egy fertőzött program elindul, a vírus kódja bekerül a memóriába, aktivizálódik és elkezdhet más programokra áttérni. Fertőzéskor a vírus mindig olyan programokat keres, amiket még nem fertőzött meg, így növelve másolatainak a számát.

Féreg

A féregvírus olyan számítógépes kód, amely a felhasználó beavatkozása nélkül terjed. A legtöbb féreg e-mail mellékletként születik meg, amely megnyitásakor megfertőzi a számítógépet. A féreg a fertőzött számítógépen olyan fájlokat keres, mint a címjegyzékek vagy ideiglenes weblapok, amelyek e-mail címeket tartalmaznak. A féreg arra használja a címeket, hogy fertőzött e-maileket küldjön, és gyakran lemásolja (vagy meghamisítja) a „Feladó” címét az e-mailekben, így úgy tűnhet, mintha a fertőzött levél ismerőstől érkezne. Ezután a férgek automatikusan terjednek e-maileken, hálózatokon vagy az operációs rendszerek résein keresztül, gyakran még azelőtt ellepve a rendszereket, mielőtt észlelni lehetne őket. A féregvírusok nem minden esetben pusztító

jellegűek a számítógépre nézve, de általában problémát okoznak a számítógép és a hálózat teljesítményében és stabilitásában.

Trójai programok

A **trójai programok** olyan ártalmatlannak tűnő önálló alkalmazások, amelyek első pillantásra hasznos alkalmazásnak tűnnek, miközben kártékony kódot tartalmaznak, esetleg vírust tartalmazó programok (pl. játék vagy animáció), amiket a gyanútlan felhasználó elindít, s feltelepíti a vírust.

Nem igazi vírusok, mert **nem tartalmaz szaporító részt**, a felhasználó által jóvá nem hagyott műveleteket hajtanak végre a fertőzött gépeken: pl. törlik a merevlemezen található adatokat, lefagyasztják a rendszert vagy bizalmas információkat lopnak és küldenek el egy harmadik személynek. **Nem fertőznek programokat vagy adatokat, és nem önállóan hatolnak be a számítógépbe**, hanem rosszindulatú felhasználók, mint „hasznos” szoftvert terjesztik, vagy elektronikus levélben érkeznek. Hatásukat **csak az elindításuk után fejtik ki**.

Levélszemét, átverés, kémprogramok

Nem vírusok ugyan, de terjedésük hasonló a vírusokéhoz. A felhasználók terjesztik az interneten a jópofa szövegeket, láncleveleket, rémhíreket, kacskákat, átveréseket (**hoax**). Levélszemét (**spam**) a kéréstlen reklámot tartalmazó cégek által küldött levél is.

A **kémprogramok** bizalmas adatainkat (jelszavak, IP cím, email címek, számlaszám!, stb.) fürkészik ki. Kémprogramok (**Spyware**): Célja, hogy adatokat gyűjtsenek személyekről, vagy szervezetekről azok **tudta nélkül a számítógép-hálózatokon**. Az információszerzés célja lehet békésebb, például **reklámanyagok eljuttatása** a kiemelt címekre, de **elophatják a számlaszámainkat, jelszavainkat, vagy más személyes adatainkat**.

Vírusfertőzés felismerése, jelei

- Csökkent memóriaméret, megnövekedett memóriahasználat.
- Hirtelen, esetenként nagymértékben lelassult számítógép műveletek.
- Késlekedés egy program elindulásakor.
- Indokolatlan és/vagy megmagyarázhatatlan változások program vagy más állományok tartalmában, módosulásának időpontjában.
- Rendellenes “Write protection error” (írásvédelem hiba) üzenet.
- A lemez meghajtók hibásan kezdenek el működni: tévesztene, nem találják, rosszul olvassák be a kért tételt.
- Windows indulásakor hibák, esetleg indulásképtelenség, ciklikus bootolás.

Aktív időszakban már jóval egyértelműbb a helyzet, (de akkor már nagyobb problémák lehetnek):

- A számítógép nem indul el.
- A vírus egy észlelhető üzenettel, hangjelenséggel vagy képernyőábrával veteti észre magát.
- Megváltoznak az információk.
- Bizonyos állományokat nem lehet betölteni vagy elindítani.
- Állományok eltűnnek.
- A merevlemez formattálódik.

Védekezési lehetőségek

- Víruskereső program telepítése. A vírusok felderítésére, illetve elpusztítására valamilyen víruskereső, illetve vírusirtó programot használunk. Általában a keresést és az irtást egy programmal el tudjuk végezni.
- Soha ne nyissuk meg a gyanús fájlokat. Nem szabad megnyitni, hanem törölni kell az ismeretlen, gyanús vagy nem megbízható forrásból származó e-mailekhez csatolt fájlokat; illetve érdemes a víruskereső programmal ellenőriztetni a CD-ről, DVD-ről, pendrive-ről, floppyról származó idegen fájlokat.
- Adatainkról rendszeresen és gyakran készítsünk biztonsági mentést;
- legyen tiszta és írásvédett rendszerlemezünk (fertőzés esetén erről indíthatjuk a gépet);
- fontos adatok írásvédetté tétele;
- a beérkező levelek, lemezen szállított adatok használat előtti ellenőrzésével;
- internetes támadások elleni használjunk tűzfalat. **Tűzfal (firewall)**: szoftveres vagy hardveres architektúra. Célja: biztosítani, a hálózaton keresztül egy adott számítógépbe ne történhessen illetéktelen behatolás.

Antivírus termékek

A vírusirtó vagy antivírus program szoftveres vagy hardveres architektúra, **célja** annak biztosítása, hogy:

- a hálózatba vagy egy adott számítógépbe ne juthasson be olyan állomány, mely:
 - károkozást,
 - illetéktelen adatgyűjtést vagy
 - bármely, a felhasználó által nem engedélyezett műveletet hajt végre.

A vírusok felfedezését a **vírusaláírások** teszik lehetővé, amelyek egy vírusra jellemző kódsorozatok. Ezeket, a vírusaláírásokat, tartalmazó fájlokat folyamatosan kell frissíteni. Nem elég egyszer telepíteni, hanem folyamatosan meg kell újítani.

Vannak **polimorf vírusok**, vagyis működés közben átalakulnak, felkutatásukra a **heurisztikus keresés** javasolt. Ebben az esetben a vírusirtó a beépített analizáló algoritmusok (mesterséges intelligencia) segítségével azonosítja a vírusokat.

A **modern vírusirtók** kombinálják tehát a hagyományos (vírusdefiníciós adatbázison alapuló) védelmet a modern heurisztikus védelemmel, és így nagyobb biztonságot adnak a felhasználóknak.

A védekezés legjobb módszere, ha **víruspajzsot** használunk. Bármilyen műveletet végzünk állandóan, figyel, és ha felismer egy vírust, akkor megszakítja a műveletet, s jelez számunkra, ez nagyon **hasznos**, viszont hátránya, hogy nagyon **lelassítja a számítógépet**. Fontos megjegyezni, hogy **tökéletes vírusvédelem nincs**. Nem létezik olyan program, amely minden vírust ismerne.

Víruskereső szoftverek ellenőrzik a bejövő e-mailek tartalmát (és a számítógépen lévő fájlokat), és azokban vírusokra utaló jeleket keres. **Ha vírust talál, törli vagy karanténba helyezi azt**. Mivel minden hónapban több száz új vírus jelenik meg, minden víruskereső szoftvert **rendszeresen frissíteni** kell a legújabb vírusdefiníciókkal, hogy a szoftver a legújabb vírusokat is megtalálja. Olyan szoftver kell, amely **automatikusan letölti a legújabb definíciókat és programfrissítéseket az internetről**.

A legismertebb vírusirtó programok közé tartozik a **Virus Buster, a Norton AntiVirus, NOD 32 Antivirus System, Panda Antivirus**.

Az AV termékek működés szerinti típusai

1. **Víruskereső:** olyan program, melyet elindítva az ellenőrzi a memóriát majd a háttértárakat, és kijelzi, ha vírust talált.
2. **Vírusirtó:** az a termék, amelyet külön elindítva azt, a felfedezett fertőzést eltávolítja a gépről.
3. **Integrált víruskereső és irtó:** a két folyamatot egy program végzi.
4. **Vírusfigyelő:** Végül vírusfigyelő az a program, mely a memóriában maradva folyamatosan végzi munkáját.