**Vírusok csoportosítása, fajtái**

**Egyebek**

* Trójai programok: Hasznos alkalmazásnak álcázza magát, miközben kártékony hatású. Hatásukat csak elindításuk után fejtik ki. A trójai programok annyiban hasonlítanak a vírusokra, hogy szükségük van valamilyen hordozó programra. A szaporító rész azonban hiányzik belőlük, így a terjedésüket csak a hordozó programnak köszönhetik.
* Lopakodók: Az antivírus programot, az operációs rendszert megkerülve a gép memóriájába maradva, a fájl méreteit, az operációs rendszer jellemzőit és a könyvtár struktúráját megváltoztatják.
* Retrók: A víruskereső alkalmazásokat nemcsak kijátszani, hanem hatástalanítani igyekeznek.
* Poliformok: Bármely vírus lehet poliform, hogy nehezebben lehessen elcsípni azokat, minden fertőzéskor megváltoznak.

**Számítógépes vírusok fajtái, csoportosítása**

A számítógépes vírusokat több szempont szerint csoportosíthatjuk. Ilyen szempont lehet az, hogy milyen állományokat fertőznek meg, azaz milyen állományokkal terjednek. Másik csoportosítási szempont lehet, hogy a vírus mennyire károkozó.
Terjedésük szerint lehetnek:

* Boot vírusok
* Alkalmazásvírusok
* Makrovírusok
* Férgek

Károkozás szerint lehetnek:

* Rosszindulatú vírusok
* Ártalmatlan vírusok

Bootvírusok

A boot vírusok az első vírusok közé tartoznak. Leggyakrabban akkor terjednek, ha fertőzött lemezzel indítjuk el a rendszert. Ebben az esetben a vírus a merevlemez boot szektorába ágyazódik be, így még az operációs rendszer betöltése előtt aktiválódik. Ennek hatására a fertőzött merevlemez az összes meghajtóba helyezett lemezt megfertőzi. A boot vírusok napjainkban a kevésbé elterjedt vírusfajták közé tartoznak.

Alkalmazásvírusok

Az alkalmazás- vagy más néven programvírusok a futtatható kódot tartalmazó (COM, EXE kiterjesztésű) állományokat fertőzik meg. A megfertőzött állományokba beírják a saját kódjukat.Két fajtáját különböztetjük meg: hozzáfűződő (append) és felülíró (replace) vírusokat. A hozzáfűződő vírusok az alkalmazások végéhez fűződnek, elhelyeznek azonban a program elején egy kódot, hogy az alkalmazás indulásakor előbb ők töltődjenek be, a program csak később. A felülíró vírusok az alkalmazások elejét írják felül saját kódjukkal, így a fertőzött állomány adatot veszít, és az eredeti állapot nem állítható helyre. Amennyiben egy programvírussal fertőzött fájlt elindítunk, a vírus betöltődik a memóriába és megfertőzi az összes többi elindított programot.

Makrovírusok

Elsősorban olyan dokumentumszerkesztő programokat támadnak meg a makrovírusok, melyek elég fejlettek, hogy bizonyos lépéssorozatokat képesek legyenek makrókkal automatizálni. Általában Word és Excel által készített dokumentumokat (DOC, DOT, XLS) állományokat fertőznek meg. Terjedéséhez elegendő egy fertőzött állomány megnyitása, és a vírus már be is töltődik a memóriába, mely a későbbiekben megnyitott dokumentumokat megfertőzi. A fertőzést általában már csak akkor vesszük észre, amikor már késő.
A makrovírusok csoportjába tartoznak a levelező vírusok is, melyek elsősorban e-mail útján terjednek. A csatolt fertőzött fájlok megnyitásakor aktivizálják magukat és általában a levelezési listában szereplő partnereknek írnak levelet, melyhez saját maguk másolatát is hozzáfűzik. Ha a levelezési címlistában nagyon sok partner van, akkor olyan mennyiségű levéláradat indulhat, amely megbénítja egy nagyvállalat levelezőrendszerét is.

Férgek

Terjedésük szempontjából a féreg vírusok furcsák, mivel nem hagyományos értelemben fejtik ki károkozó hatásukat, hiszen nem tesznek kárt állományainkban. Elsősorban interneten, hálózaton terjednek. Megbújnak a számítógépen, és információt gyűjtenek róla, majd az összegyűjtött információkat tárolják. Ha ismét csatlakozunk az internetre, hálózatra, akkor ezeket a tárolt információkat a megadott címre továbbítják.

Spyware

A spyware vagy más néven kémprogramok célja, hogy adatokat gyűjtsenek személyekről vagy szervezetekről azok tudta nélkül a számítógép-hálózatokon. Az információszerzés célja lehet például reklámanyagok eljuttatása a kikémlelt címekre, de akár ellophatják jelszavainkat, számlaszámainkat vagy más személyes adatainkat rosszindulatú akciók céljából is. A vírusokhoz hasonlóan lehet őket „beszerezni”.