

Számítógépes vírusok

Számítógépes vírus

A **számítógépes vírus** olyan program, amely saját másolatait helyezi el más, végrehajtható programokban vagy dokumentumokban. Rossz indulatú főképp, más állományokat használhatatlanná, sőt teljesen tönkre is tehet. A számítógépes vírusok működése hasonlít az élővilágban megfigyelhető [vírus](#) viselkedéséhez, mely az élő sejtekbe hatol be, hogy önmaga másolatait előállíthassa. Ha egy számítógépes vírus kerül egy másik programba, akkor ezt *fertőződés*nek nevezzük.

A vírus csupán egyike a rosszindulatú szoftverek (*malware*) számos típusának. Ez megteveszthető lehet a számítógép felhasználók számára, mivel mára lecsökkent a szűkebb értelemben vett számítógépes vírusok gyakorisága, az egyéb rosszindulatú szoftverekhez, mint például a [férgékhez](#) képest.

Bár a számítógépes vírusok lehetnek kártékonyak (pl. adatokat semmisítve meg), a vírusok bizonyos fajtái azonban csupán zavaróak. Némely vírus késleltetve fejt csak ki hatását, például csak egy bizonyos számú gazdaprogram megfertőzése után. A vírusok domináns kártékony hatása az ellenőrizetlen reprodukciójuk, mely túlterhelheti a számítógépes erőforrásokat.

Napjainkban (2005), az internet térhódításával vírusok már valamivel kevésbé gyakoriak, mint a hálózaton terjedő férgek. Az antivírus szoftverek, melyeket eredetileg a számítógépes vírusok elleni védelemre fejlesztettek ki, mára már képesek a férgek és más veszélyes szoftverek, mint pl. a [kémprogramok](#) (*spyware*) elleni védelemre is.

Gyakori jellemzőik

A gazdaprogramok megfertőzése és az önsokszorosító viselkedés valamennyi vírusra jellemző. Ezenkívül gyakran rendelkeznek a következő tulajdonságokkal:

- nagyon kis méret;
- legtöbbjük a [Microsoft Windows operációs rendszereken](#) okoz gondokat;
- futtatható állományokat képesek megfertőzni;
- általában ártó szándékkal készítették őket;
- 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

Alaptípusaik

- Bootvírus
- Fájlvírus
- Makróvírusok

Legújabb fenyegetések

Céljuk nem a rombolás, hanem illegális javak, illetve személyes, titkos adatok megszerzése. Ennek megfelelően terjesztési módszerük is különbözik a korábbiaktól. 2005-ben az "izraeli eset" kapcsán jegyezték fel az első személyre szabott trójai programot alkalmazó csendes támadást.

Legújabb fenyegetések típusai

- Személyre szabott támadás

- Csendes támadás

A lánclevél tartalma

A levél tartalma lehet:

- érzelmekre ható üzenet
- pénzszerzéssel kecsegtető
- életvezetési tanácsokat adó
- vírusriasztást közlő
- segítségkérő
- stb.

Lánclevél az [Internet](#) kora előtt is létezett, a postaládába bedobott bélyeg- vagy akár boríték-nélküli, fénymásolt kiviteleről lehet megismerni.

Az Internet és az [e-mail](#) elterjedésével a lánclevelek gyakoribbak lettek, gyorsabban terjednek és nagyobb tömegeket érnek el.

A lánclevél többnyire egy személyes ismerősünktől érkezik, ez azonban nem jelenti azt, hogy a levél tartalmához neki bármi köze lenne. A bizalom következtében azonban a kapott levelet könnyebben továbbküldjük, mintha egy ismeretlentől kaptuk volna.

A lánclevelek nagy része ártatlan tréfa de vannak olyanok is, amik kárt okozhatnak azoknak, akik elhiszik a levél tartalmát. Előfordulhat például olyan, vírusriasztásról szóló levél, ami egy vírus elhárítására bizonyos fájlok törlésére szólít fel, és ha ezt meg tesszük, a gépünk a következő bekapcsoláskor nem indul el.

Spam

Ugrás: [<small>NAVIGÁCIÓ</small>](#), [<small>KERESÉS</small>](#)

A **spam** a fogadó által nem kért, elektronikusan, pl. [e-mailen](#) keresztül tömegesen küldött hirdetés, felhívás.

Az így kapott információk a fogadók túlnyomó része szempontjából érdektelenek, így fölösleges [sávszélességet](#), [tárhelyet](#), szellemi ráfordítást igényelnek a fogadótól. Mivel a spameket a feladók milliós nagyságrendben képesek rövid idő alatt kiküldeni, ez jelentős terhelést jelent az internet használói számára. A spamek egy része tudatosan megtévesztő, a fogadó kihasználására törekszik.

Védekezés

A fentiek miatt sokféle védekezési mód alakult ki a spammal szemben:

- olvasás nélküli törölgetés (fennáll a fontos levél véletlen törlésének esélye)
- a web oldalakon feltüntetett e-mail címek álcázása a begyűjtés ellen
- a nyitott mail-továbbító szerverek korlátozása
- spam azonosító program telepítése a felhasználó gépére
- szűrő alkalmazása a levélkezelő felületen
- kulcsszavak alapján való szűrés
- öntanuló Bayes-szűrő használata
- a valós küldő címének blokkolása

- a küldő cégek jogi perlése
- hamis hibaüzent visszaküldése spam érkezésekor
- a spam-ben feltüntetett hirdetési felület, csatorna leterhelése
- SPAM szűrő szervereken keresztüli levélfogadás.

Az elnevezés eredete

Az angol szó eredete egy angol konzervként forgalmazott hústermék (*Spiced Pork And Ham*), mely egy angol komikus filmjelenet (*Monty Python's Flying Circus* egyik epizódja) alapján lett a „ránkeröltetett valami” jelölője.