

(4) Számítógépes kártevők

A számítógépes kártevőknek sokféle fajtája létezik. Definíció szerint ezek olyan programok, amelyek nem hasznos tevékenységet folytatnak. Az angol elnevezésük malware, ami rosszindulatú programot jelent. Mivel sokféle ilyen program van, ráadásul ezek sokszor alig különböznek egymástól, ezért elég nehéz csoportosítani őket.

Leggyakrabban a következőképpen osztályozzuk őket:

1. Vírusok
2. Féreg
3. Trójai programok
4. Kémprogramok
5. Egyéb káros program, és tevékenység (hoax, spam, adathalászat)

1. Vírusok

A '80-as években a számítógépek és a hozzájuk tartozó programok terjedésével megjelentek az első számítógép-vírusok is.

Olyan programokat nevezünk vírusnak, melyek képesek reprodukálni, sokszorozítani önmagukat. Működésük, és terjedésük csak bizonyos közegben lehetséges. Ha ez a közeg nem áll rendelkezésre, nem működőképesek. Nem feltétlenül okoznak kárt, sokszor csak kisebb bosszantó tevékenységet művelnek. Bizonyos esetekben a vírus "megelégszik" ennyivel, de többnyire más kárt is okoz. Működésüknek két ciklusa van. Először megpróbálnak minél jobban elterjedni, minél több gépet megfertőzni, majd egy esemény bekövetkezésekor (például előre meghatározott napon) kifejtik káros tevékenységüket. Ez a tevékenység lehet adatok törlése, felülírása, teljes adatmegsemmisítés, vagy akár fontos programok, menüpontok eltüntetése. Léteznek olyan vírusok is, melyek képesek bizonyos hardvereszközök tönkretételére is.

Nincs ártalmatlan vírus, ha egyéb kárt nem okoz, akkor is rabolja a felhasználó idejét, lefoglalja a számítógép erőforrásait.

A vírusok olyan programok, melyeket készítőjük ártó szándékkal írt: lehetséges, hogy elbocsátott alkalmazott akart ilyen módon búcsút venni munkahelyétől, de lehet, hogy egy ambiciózus fiatal programozó kívánta tudását a publikum elé tárni.

Némelyik vírus csak letörölte időnként a képernyőt vagy ostoba, netán világhuralmat ígérő, néha mulatságos üzeneteket írt ki, s olyan is akadt, amelyik a munkaidő lejártát rövid zenével adta tudtára mindenkinek. Akadtak - akadnak - persze sokkal veszélyesebb vírusok is, a pusztítás igazi mesterei. Jelenlétüket még a szakemberek is csak későn fedezik fel, mire pl. a vírus már hozzáfogott a merevlemez információtartalmának teljes letörléséhez.

A vírusok manapság jellemzően pendrive vagy e-mail segítségével terjednek, az internetes böngészés mellett, valamint a megbízhatatlan oldalakról történő letöltések által.

Sok vírus nem azonnal lép működésbe, hanem csak egy bizonyos "lappangási idő" után, esetleg egy bizonyos időpontban aktivizálódik.

A vírusokat több szempont szerint is csoportosíthatjuk.

Károkozás mértéke, típusa szerinti csoportosítás

'Reprezentatív' vírus

Főleg a hőskorban volt jellemző. A program jelzi jelenlétét, de egyéb kárt nem okoz.

Szoftvert károsító vírus

Az ilyen programcskák az állományokat károsítják.

A támadás célpontja szerinti csoportosítás

Fájlvírusok (Állomány, vagy programvírus)

Ez a vírus állományokhoz kapcsolódik, ami leggyakrabban egy program. Ezzel az állománnyal együtt terjed egyik gépről a másikra. Amikor a program elindul, akkor aktiválódik a vírus is. Ha ezután további programokat indítunk el, akkor a vírus azokat is megfertőzi. Működése többnyire adott operációs rendszerhez, és bizonyos állománytípushoz (pl. exe) kötött.

Az ún. végrehajtható állományokat (exe, com) támadják, és használják "szaporodásra". Ez a legrégebbi típus, és talán a legegyszerűbb védekezni ellene.

Bootvírus

Nevét onnan kapta, hogy a háttértárolók meghatározott részére, az úgynevezett boot (betöltő) szektorba írja be magát. Ezt a boot szektort minden számítógép indításakor megvizsgálja a BIOS, és ha itt programot talál, akkor elindítja azt. Tehát ha egy vírus itt helyezkedik el, akkor minden indításnál automatikusan az is aktiválódik. Ennek a vírusnak a hatékonyságát nagyban megnövelte, hogy még a vírusirtó programok betöltődése előtt aktiválódik.

Különösen veszélyes típus az ún. MBR vírus, amely a rendszerlemez BOOT szektorát támadja meg, így induláskor beíródik a memóriába. Innentől kezdve egyetlen állomány sincs biztonságban, amely a memóriába kerül.

Makrovírusok

Ezek a legújabb típusú vírusok, amelyek szöveges dokumentumokba, táblázatokba, levelekbe fészkelik be magukat. Különös veszélyességüket az adja, hogy az internetes adatforgalom többsége ilyen fájlokból áll.

Sok felhasználói program rendelkezik azzal a képességgel, hogy tudását apró programokkal, úgynevezett makrókkal bővítsék. Ilyenek például a Microsoft Office csomag elemei (Word, Excel, Outlook, Power Point) is. A makrovírus olyan program, ami ezekben a nagyobb programokon belül életképesek. Általában dokumentumokhoz csatolják magukat, és azokkal együtt terjednek. Ha megnyitjuk a dokumentumot, akkor elindul a vírus is.

Vírusokból az utóbbi időkben egyre kevesebb van, mivel már kevésbé hatékonyak az újabb, modernebb károkozókhoz képest.

2. Féreg

A vírusokhoz hasonló programok. Ezek is képesek reprodukálni magukat, de a vírusokkal ellentétben nem szükséges hordozóközeg a terjedésükhöz. Önmagukban, a számítógépes hálózatokat felhasználva terjednek. Manapság a legveszélyesebb programok ebből a típusból kerülnek ki, elsősorban a gyors terjedésük miatt. Mire egy-egy újabb féreg jelenlétét észrevennék, és az ellenszert elkészítenék az erre szakosodott cégek, addig a féreg az internetet használva akár több százezer gépet is képes megfertőzni. Sokféle kárt képes okozni, de már önmagában a terjedéssel is sávzsélességet foglal, vagyis az internet egyéb, hasznos forgalmát hátráltatja.

3. Trójai programok

Olyan programok, amelyek önmagukban nem okoznak kárt, (sőt sokszor hasznos programnak álcázzák magukat) de képesek a háttérben segíteni egyéb ártó szándékú programok bejutását, és működését a számítógépen. Mivel gyakran hasznos programnak mutatják magukat, ezért leggyakrabban a felhasználó tölti azt le számítógépére. Emellett terjedhetnek e-mailben, vagy adathordozókon is.

(Trójai vírusok)

A vírusok egy speciális fajtáját képviselik a trójai vírusok. Nevüket viselkedésük miatt kapták a trójai faló nyomán: ezek a vírusok jól működő programok álcája mögé bújnak. Nem sokszorozítják magukat, inkább időzített bombaként foghatjuk fel őket: a trójai program egy darabig jól ellát valamilyen feladatot, aztán egyszer csak nekilát, és végzetes károkat okoz (pl. tönkréteszi a merevlemezen tárolt adatokat.)

4. Kémprogramok (spyware)

Angolul spyware a nevük. Feladatuk a gépen tárolt bizalmas adatok (jelszavak, kódok, bankkártya- és személyes adatok) megszerzése, és továbbítása. Sok kémprogram azt figyel, hogy a felhasználó milyen tartalmú weboldalakat néz az interneten, és az így megszerzett információ alapján célzott reklámokat, hirdetéseket küld a felhasználó gépére.

(Ha egy-egy letöltésmenedzselő-, fájlcserélő- vagy akár tömörítőprogram telepítése után különös jelenségeket produkál számítógépünk (böngészőablakok nyílnak maguktól, érdekes linkek jelennek meg, új ikon jelenik meg a tálcán), nagy valószínűséggel a népszerű ingyenes programokhoz alattomban mellékelt apró szoftverek működésének jeleit tapasztaljuk. Ezek eredetileg "csak" arra szolgáltak, hogy az ingyenes program felhasználóját reklámok megjelenítésével lássák el, és váltakozó reklámok megtekintése volt az ár, amiért ingyenesen lehetett használni a többnyire freeware vagy shareware programokat. Időközben azonban már többről lett szó, mert a reklám egyedül már nem elég vonzó. A figyelem középpontjába mára már a felhasználó és az interneten tanúsított magatartása került: a reklámösszetevők ma már olyan funkciókat hordoznak, amelyekkel a szoftver fejlesztői titokban személyes felhasználói adatokat, például internetezési szokásainkból összeállított profilt tudnak készíteni, és az interneten elküldeni. Ez a fajta szoftver, amely elsősorban arra szolgál, hogy a felhasználót megfigyelje, hamar új nevet kapott az internet-zsargonban: "spyware" - a "kémszoftver" angol rövidítése. A felhasználó az ilyen programok ténykedéséről többnyire egyáltalán nem is értesül.)

5. Egyéb károkozók

A) Hoax, magyarul lánclevél (hírlapi kacsa)

Ez nem program. A lánclevél egy hasznos nem hozó, sőt sokszor bosszantó e-mail fajta. Ez az a levél, ami arra kéri olvasóját, hogy minél több példányban küldje tovább. Ennek érdekében általában az érzelmekre próbál hatni, (Ha továbbküldöd a levelet legalább 1000 ismerősödnek, meggyógyulnak az afrikai beteg gyerekek) vagy áltudományos adatokra (új vírus jelent meg, amit csak a levél továbbküldésével lehet kiirtani) hivatkozik. Bár káros tevékenysége nincs, az elolvasásával és továbbküldésével töltött időt más, fontosabb tevékenységtől vesszük el.

A Sophos antivírus kutatói megvizsgálták az e-mailen terjedő hoaxokat, hogy mik a legnépszerűbb lánclevelek közös tulajdonságai:

- Sok nagybetűs szöveget tartalmaznak.
- Felszólítanak, hogy minél több ismerősünknek, mielőbb küldjük tovább.
- Ismert nagy cégre hivatkoznak, mely szerint ők is megerősítették a hírt.
- Többször is elhangzik, hogy mennyire extrém veszélyes kártevőről van szó.
- Áltudományos nyelvezettel próbálja meggyőzni a kevésbé hozzátörőket.
- Gyakori a kódosítás, például tegnap (mihez képest tegnap, pl már egy hónapja is bolyonghat az álhír így a neten)

B) Spam (Levélszemét)

Kéretlen reklámlevél. Legtöbbször teljesen felesleges, a fogadó által nem kért, mégis nagy számban elküldött reklám a spam. Mivel a spameket milliós nagyságrendben küldik, ezért jelentősen terheli az internetet, foglalja a fontos információk elől a sávszélességet.

Az e-mail használhatóságát jelentősen csökkentik a nagy számban érkező kéretlen, rosszindulatú, ill. téves levelek. A több száz aktív „szemetelő” miatt az átlagfelhasználó napi tíz, vagy akár száz ilyen levelet is kaphat az elektronikus postaládájába. Mivel az e-mail küldés költségei igen alacsonyak, a „szemetelők” napi több száz millió e-mailt küldenek szét naponta, amely jelentősen csökkenti a kommunikációs forma hatékonyságát.

A levélszemét tipikus tartalmakkal rendelkezik, melyek gyakran keveredve jelennek meg:

Legnagyobb számú a *kéretlen kereskedelmi hirdetés*, a szoros értelemben vett spam. Az e-mail férgek (*worm*) e-maileket használnak saját maguk sokszorosítására és bejuttatására sérülékeny rendszerekbe. Bár a legelső e-mail féreg, a Morris féreg, UNIX rendszereket támadott meg, ez a probléma ma szinte csak a Microsoft Windows rendszerek velejárója. Az e-mailek csatolmányában álcázott számítógépes vírusok lapulhatnak. Levélszemétnek minősülnek azok a levelek, amelyek levelező listáról származnak, és

tartalmukra nem számít a feliratkozott felhasználó. Előfordul, hogy valaki címe hasonlít egy népszerű címre, vagy csak nagyon egyszerű, így tévedésből neki küldenek leveleket. Az U.S.A és az E.U. egyaránt megpróbálnak e problémák ellen törvényekkel védekezni.

C) Adathalászat (phishing)

Adathalászatnál egy jól ismert weboldalt (pl. bank) másolnak le a csalók, és megpróbálnak minél több felhasználót rávenni, hogy ezen az oldalon adják meg személyes, és titkos adataikat. Ehhez egy e-mailt küldenek körbe, melyben arra kéri az olvasót, hogy nézze meg az átalakított weboldalt.

Vírusfelismerés

- Indokolatlanul megváltozik egy fájl mérete.
- Indokolatlanul eltűnnek vagy megjelennek fájlok.
- Nem indulnak el programok.
- A háttértárak szabad kapacitása hirtelen lecsökken.
- Megváltozik egy program felülete (menük, eszköztárak).
- Bármilyen különös, szokatlan viselkedés.
- Vírusfelismerő program futtatása a rendszeren.
- Lelassul a számítógép működése, gyakran percekig csak tölt, és semmilyen funkció nem elérhető ezalatt.
- Nem megszokott programműködés. Egy funkció nem úgy működik, ahogy megszoktuk, vagy megváltoznak a program beállításai.
- Hardverhibával nem megmagyarázható adatvesztés történik.
- Lelassul az internetes kommunikáció

Védekezés a vírusok ellen

Legjobb védekezés ebben az esetben is a megelőzés. Nagyon fontos, hogy mindig csak tisztázott eredetű programokat, adatokat használjunk. A jogtisztán beszerezett programok, nagyon ritka kivételtől eltekintve, megbízhatóak.

Használhatunk ún. víruspajzsot, amely rezidensen a memóriában van, minden oda bekerülő adatot ellenőriz és figyelmeztet, ha gyanús jelet tapasztal.

Időről időre futtassunk vírusfelismerő programot gépünkön.

Mi a teendő fertőzés esetén

Első lépésként függesszünk fel minden egyéb tevékenységet és csak a vírus mentesítésre figyeljünk!

Értesítsük a rendszergazdát (ha van, a továbbiak az ő feladatát képezik)!

Kezdjük el a vírus mentesítést!

Hogyan lehet megszabadulni a vírustól?

Töröljük a gyanús állományt! Ez adatvesztéssel jár, tehát meggondolandó.

Formázzuk a lemezt! Ez még inkább drasztikus módszer és sajnos gyakran ez sem vezet eredményre. (Főleg ha a memória is fertőzött.)

Használjunk vírusirtó programot! Ezek a programok is többféleképpen mentesítenek. Ha nem boldogulnak a vírus átkódolásával, megpróbálhatják törölni a vírust. Ez utóbbi bizonyos esetekben a fájl tartalmának elvesztésével is járhat. Ha sem így, sem úgy nem megy, marad az állomány átnevezése. Ez a fájlvírusok esetén hatásos. BOOT vírusok esetén csak akkor lehet eredményes az irtás, ha a rendszert egy vírusmentes rendszerlemezről újraindítottuk. Ez általában egy írásvédetté tett floppyról történik, amelyet legjobb rögtön a gép vásárlásakor elkészíteni.

Védekezési módszerek:

1. Vírusirtók használata

A vírusok elleni védekezés egyik legfontosabb része. A vírusirtó program képes felismerni, és a legtöbb esetben eltávolítani a fertőzött gépről a vírust. Figyelni kell arra, hogy a programot naponta(!!!) kell frissíteni, hogy felismerje a legújabb vírusokat is. Az utóbbi időben megjelentek az ál-vírusirtó programok is, ezért csak megbízható helyről beszerezett, jól ismert vírusirtót használjunk! Az ingyenesen elérhető vírusirtók közül az AVG Free, vagy az Avast Home ajánlható, a fizetősök közül például a NOD32, az F- Secure, a Kaspersky Antivírus, vagy a Norton Antivírus.

2. Kém és trójai program irtók

Hasonlóak a vírusirtókhoz, csak ezek trójai és spyware programokat keresnek és irtanak a gépünkön.

3. Tűzfalak

A tűzfal feladata megvédeni a mögötte lévő gépeket a kívülről (pl. internet) jövő veszélyekkel (betörési kísérlet, ártó programok) szemben, illetve ellenőrzik a bonyolított hálózati forgalmat. A tűzfal lehet hardveres, például routerbe épített, vagy szoftveres.

4. Egyéb, de fontos tevékenységek

A) Adatmentés, archiválás. Minden esetben csináljunk dokumentumainkról biztonsági másolatot.

B) Ismeretlen feladótól érkező levél megnyitás nélküli törlése, de legalább a csatolt állományok figyelmes kezelése.

C) Az operációs rendszer és a fontosabb programok rendszeres frissítése. Sokszor programhibát kihasználva terjednek a kártervők. Ezeket a hibákat a programok újabb verzióiban többnyire kijavítják, így kisebb az esély a károkozásra.

D) Csak jogtiszt programok használata. Gyakran a kémprogramokat, és a trójai programokat ingyen elérhető, de normál esetben fizetős programokba rejtve juttatják el a gépekre.

Néhány vírusirtó program:

- Nod32
- AVG
- Virusbuster
- Panda
- McAfee

Vírusirtók

Ezek a beazonosított vírust hatástalanítani tudják. Legtöbb esetben az utóbbi két funkciót egy programba építik, de a komolyabb szoftvercsomagok mind a három feladatot ellátják. Mivel egyre újabb és újabb vírusok jelennek meg, a vírusirtókat folyamatosan frissíteni kell. Léteznek parancssori és menüvezérelt víruskezelők is.