

Számítógépes vírusok

Történet

•70-es években kezdődött programok, melyek olyan utasításokat tartalmaztak, amik szándékosan rongáltak, illetve hibákat okoztak. Teszteljék a számítógép terhelhetőségét
Legyen „géptidejük” a programozóknak

Mik a vírusok?

•Parazita programok
Önállóan képesek szaporodni
Létezésük programozói tevékenységnek a végeredménye

A vírusok felépítése

1. Reprodukciós rész
Működésbe lépés feltétele
Utasítás sorozat (objektív rutin)

A reprodukciós rész

A legfontosabb része, mert ez az, ami terjed, azaz megkeres olyan programokat, vagy alkalmazásokat, amelyekbe be tudja írni magát

Működésbe lépés feltétele

1. Például:
Az év megadott napja, minden hónap egy konkrét napja, a nap valamelyik órája
Valamilyen alkalmazás elindítása
Egy billentyűkombináció
Stb...

Az utasítás sorozat

Hogyan rongálja a vírus?

Boot szektor vírusok

A hajlékony- és a merevlemeznek azt a szektorát támadják, amely az operációs rendszerre, illetve az állományokra vonatkozó információkat tartalmazza.

A vírusok fajtái

A teljesség igénye nélkül... ☺

Boot szektor vírusok

Akkor aktivizálódnak, amikor az operációs rendszert a számítógép elindulásakor, a boot szektorból betöltjük.

Fertőzött rendszer indulásakor a vírus a memóriába kerül, majd mikor hajlékony lemezt (floppy) teszünk a meghajtóba, megfertőzi annak boot szektorát.

Állományvírusok

A programfájlokat fertőzi meg (COM, EXE)

A fertőzött program futtatásakor átmásolják önmagukat, és kárt okoznak.

Állományvírusok

Két fajtájuk van.

Az egyik egyszerűen felülírja az eredeti programot, vagyis tönkreteszi azt

A másik program végéhez fűzi hozzá magát, és a fájl elején található utasításokat módosítja.

Így a program indításakor órá kerül a vezérlés. Ezek ellen tudunk a legnehezebben védekezni.

Társult vírusok

A programnak a nevét gépeljük be, a kiterjesztést csak nagyon ritkán. Az operációs rendszer egy, a paranccsal azonos nevű és COM kiterjesztésű programot keres. Ha ilyent nem talál, akkor először EXE, majd BAT kiterjesztésűekkel folytatja a keresést. Amelyiket előbb találja meg, azt futtatja le.

Társult vírusok

A vírus COM kiterjesztéssel odamásolja magát a megfertőzendő - általában EXE kiterjesztésű program elé

Makróvírusok

Felhasználót segíti a makró nyelv.
A dokumentum automatizálható,
DE...
A vírusok ezt kihasználják!
Aktivizálódásuk a dokumentum megnyitásakor
NORMAL.DOT

Script vírusok

HTML oldalak nézegetésével fertőznek
JavaScriptek, AktivX
alkalmazások, amiket HTML
oldalakra szűrnak be, azért hogy a
Web lapokat vonzóbbá,
látványosabbá tegyék

Internet férgek

A férgek e-mail-hez csatolt fájlként érkeznek

A levél küldője nem biztos, hogy tud a csatolt féregről

A levélhez csatolt fertőző melléklet végrehajtása után telepíti magát a rendszerbe.

Ezután elfogja az Internetre küldött elektronikus leveleinket, és mellékletként hozzájuk csatolódik

Trójai programok

Ezek a programok csak álcázásra szolgálnak.
Mást tesznek, mint amit ígérnek

Hardvervírusok

A hardvert úgy vezérli, hogy azt tönkre teszi

A vírusok csoportosítása

- **Fertőzési módszerek:**
Memóriában elrejtőző
Közvetlen tevékenységű
Időzített bombák
Lopakodó vírus
Polimorf vírus
Retrovírus

A vírusok csoportosítása

Memóriában elrejtőző

A fertőzött program lefutásakor a vírus a memóriába írja be magát, és ott is marad, míg a gép be van kapcsolva.

Ezután minden olyan állományt megfertőz, amit a memóriába való befészkelése után elindítanak.

Rezidens vírusok.

A vírusok csoportosítása

Közvetlen tevékenységű

Aktiválásuk után adott számú állományt fertőznek meg

Majd visszaadják a vezérlést a gazdaprogramnak

A vírusok csoportosítása

Időzített bombák

Egy bizonyos lappangási idő után kezdi el a fertőzést.

Hogy mennyi ideig tart ez az inaktív időszak, azt a vírus programozója határozza meg.

Általában valamilyen feltétel hatására aktivizálódik a vírus.

A vírusok csoportosítása

Lopakodó vírus

A vírusok számára a legfontosabb, hogy el tudjanak rejtőzni a felhasználó és a víruskereső programok elől.

Egy lopakodó vírus képes akár egy fertőzött fájlt eredetinek feltüntetni azzal, hogy

lemezolvasási kéréseket figyel és fog el, majd hamis információkat szolgáltat a rendszernek.

A vírusok csoportosítása

Polimorf vírus

A polimorf vírus minden fertőzése különböző.

Generációról generációra képesek a végrehajtási kódjukat, működésüket is megváltoztatni.

Nem ritka az sem, hogy akár fertőzésről fertőzésre is megváltozik a megjelenési kódjuk.

A vírusok csoportosítása

Retrovírus

Valamilyen konkrét alkalmazásra, vagy alkalmazásokra specializálódott vírus.

A vírus azt a módszert használja, hogy megsemmisíti a kiválasztott programot, esetleg lefagyasztással, vagy más módszerrel megakadályozza annak működését, de gyakran átírja az antivírus programot úgy, hogy az ne ismerje

A vírusok csoportosítása

A vírusok saját védelmük és a mi életünk megkeserítése érdekében a különböző elemek kombinációit alkalmazhatják, azaz egyszerre fertőzhetik a boot szektort és az állományokat, miközben rejtőzködnek, lopakodnak és mutálódhatnak is.

Védekezés

Csak jogtisztá programot vásárolunk.
Gépünkhöz nem engedünk oda illetéktelen felhasználót.
Nem másolunk a winchesterre bizonytalan forrásból származó programokat.
Víruskereső –vírusirtó programmal

Víruspajzs

A programok egy része a memóriába is hajlandó betelepülni.

E darabkát nevezzük memóriarezidens résznek.

Helyes beállítás esetén szinte tökéletessé teszi a vírusvédelmet.

Ezt a fajta módszert hívjuk víruspajzs-védelemnek.

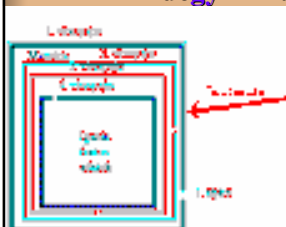
Víruspajzs

Természetesen kell hagyni egy kis rést, ahol a szükséges adatok többszöri ellenőrzés után ki-be mehetnek, de ehhez igen jól megerősített biztonsági őr-programokra van szükség.

Víruspajzs

A többszörös víruspajzs-módszer esetében, több víruspajzs van egymáson belül.

Mindegyik más és más módszerrel



ővő adatot,
különbözik az egyel
engedélyező jelszó,
külön-külön kell