SZÁMÍTÓGÉPES VÍRUSOK

Vírus: Nem más, mint programsorokba öntött rosszindulat. Több szempont szerint osztályozhatjuk őket:

- Vírusprogramok
- Vírusgenerátorok
- Trójai programok
- Programférgek
- Logikai bombák
- Hátsó ajtók, kiskapuk és csapdák
- Baktériumok és nyulak

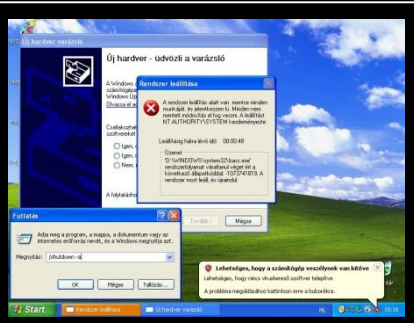
1. Vírusok

- A számítógépvírus olyan program, amely képes önmagát reprodukálni, önmagában életképtelen és gyorsan terjed.
- Több feltétel együttes teljesülése esetén minősíthető a program vírusnak: 1.Saját kód sokszorozásának képessége,
  2.Rejtőzködés alkalmazása,
  3.Adott feltételek teljesülésére való figyelés,
  4.különböző mellékhatások megjelenése
- Makrovírusok (Word): új fejezetet nyitott a vírusok terjedésében. A fertőzés időpontja után minden új dokumentum és megnyitott régi dokumentum is vírusos lesz.

2. Vírusgenerátorok

- Vírusok mellett egyre többet hallani a vírusgyártó automatákról. Ezekkel ezerszámra lehet új vírusokat létrehozni.
- A legelső próbálkozás a VCS (Virus Constraction Set) volt, amely olyan vírusokat készített, melyek kódjaikban nem különböztek jelentősen egymástól, a config.sys-t és az autoexec.bat-ot tették tönkre.

3. Trójai vírusok



- Nevüket a görög mondában szereplő trójai falóról kapták
- Járulékos funkciókat fűznek egy programhoz, maguk csak álcázásra szolgálnak
- Nehéz felismerni őket,mert gyakran egy közismert program mögé rejtőznek
- Abban különböznek a vírusoktól, hogy nem tartalmaznak szaporító rutint a kódjukban
- Gyakran védelmi célból hozzák létre a fejlesztők

3.1. Egy másik fajtája a trójai vírusoknak, a hálózatot felderítő programok.

- Ha nincs semmiféle vagy elegendő joga a felhasználónak egy hálózathoz, akkor beépíthet olyan rutint a számítógépébe, amely figyeli, hogy milyen jelszóval jelentkezik be valaki, majd ezt az információt egy számára hozzáférhető állományba menti => ezek után már hozzáférhetőek a felhasználó adatai.

3. Programférgek (Worms)

- A programférgek olyan programok, amelyek önmagukban is futóképesek, és gépről gépre vándorolnak egy számítógépes hálózaton keresztül.
- Programférget meglehetősen nehéz írni, viszont jelenlétével rengeteg kárt tud okozni
- A férgek hatása egyszerű fájlbővülés, csökkenti a tárolókapacitást
- Híres féreg volt a *Christmas Tree,* ami az IBM hálózatán terjedt el.
- Az új generációs programférgek már romboló rutinokat is tartalmaznak – jó példa erre a 2003. május 3.-án elszabadult „I Love You” névre hallgató levélféreg.

4. Logikai bombák

- Bizonyos ideig megbújnak az általunk használt szoftverekben és egy adott feltétel teljesülésére elszabadulnak
- Logikai bombákat általában szoftverfejlesztők ágyaznak be a programokba
- Logikai bombák ellen a leghatékonyabb védekezés, ha a programokat ellenőrizzük telepítés előtt.
  (vagy időben kifizetjük a szoftverfejlesztőt ☺)

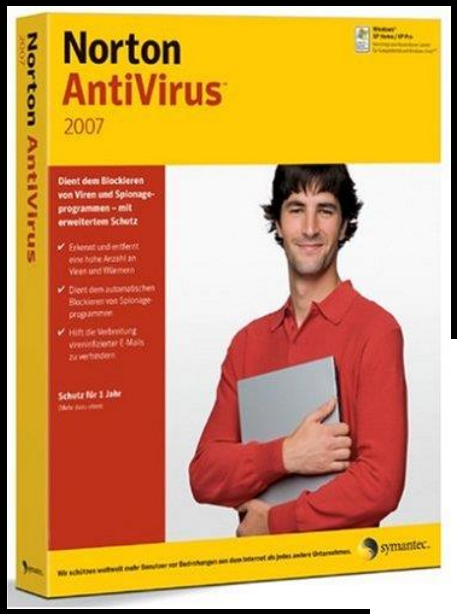
5. Hátsóajtók, kiskapuk és csapdák

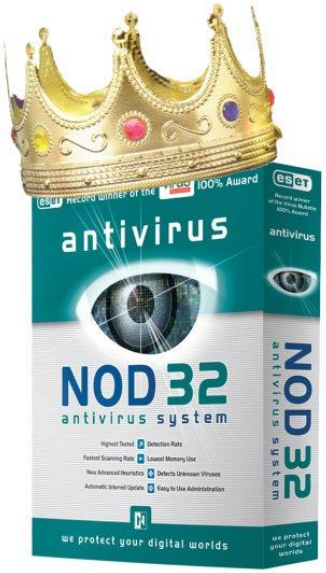
- Olyan kódrészletek, amiket azért építenek bele egyes alkalmazásokba vagy operációs rendszerekbe, hogy biztosítsák a programozók számára ezen rendszerek elérését, anélkül, hogy végig kellene járni a szokásos hozzáférési utat.
- A legtöbb hátsó bejárat csak hosszadalmas eljárások, beállítások, különböző értékek beírása után hajlandóak elindulni.
- A kiskapuk csak akkor válnak veszélyesekké, ha jogosulatlan felhasználók, programozók arra használják fel őket, hogy engedély nélkül férjenek hozzá rendszerekhez, kódrészletekhez.
- A hátsó ajtók elleni védelem nagyon bonyolult, viszont biztos forrásból származó, jogtiszta szoftverek használatával kisebb a fertőzés esélye

6. Baktériumok és nyulak

- A baktériumok vagy más néven nyulak olyan programok, amelyek csak önmaguktól készítenek másolatot.
- Lefoglalják a gép processzor idejének, memóriájának és lemezkapacitásának jelentős hányadát, ezáltal lehetetlenné teszik, hogy a felhasználó az erőforrásokat hatékonyan kihasználhassa.
- A támadásoknak ez az egyik legrégebbi módszere. Az erőforrások nélküli számítógépek különösen ki vannak téve az ilyen jellegű támadásoknak.

7. Vírusmegelőzés a gyakorlatban





7.1. Honnét kerülhet vírus a gépre?

- Munkatársak ellenőrizetlen adathordozóiról
- Szoftverkereskedőtől vásárolt programokon keresztül
- Meghajtóban felejtett lemezek révén
- Állásából eltávolított, bosszúálló munkatársak révén
- Szervizelést végző személyzet által
- E-mailben csatolt fájlként

7.2. Mit tehetünk? Néhány óvintézkedéssel csökkenthetjük a fertőzésveszélyt

- Eredeti szoftver biztos forrásból való beszerzése
- Írásvédett lemezek használata
- Tesztrendszer kialakítása
- Biztonsági másolat készítése
- Megfelelő hardver- és szoftvervédelem használta
- Egyszer írható optikai lemez használata
- Hálózati kapcsolatfelvétel forrásának ellenőrzése
- Hozzáférés-védelem alkalmazása
- Rezidens vírusdetektorok használata
- Ismeretlen feladótól érkező E-mail törlése