A számítógépes vírusok és más fenyegetések kérdései

A számítógépes programok utasítások sorozatából tevodnek össze. Ezek rendszerint valami hasznos dolgot végeznek, valamit kiszámítanak, karbantartanak adatbázisokat és kommunikálnak a felhasználókkal vagy más gépekkel. Néha azonban ezek az utasítások kárt is okozhatnak. Véletlen esemény általában akkor történik, ha programfejlesztés közben hibás programrészletet indítunk el. Az ilyen programhibák a leggyakoribb okai a nem várt programviselkedésnek.

Vannak azonban esetek, amikor a kárt okozó utasításokat valaki szándékosan helyezte el a programban és ezáltal érte el, hogy a program nem megfeleloen viselkedik, akkor szándékos programozott fenyegetésrol beszélünk. A szakértok ezeket viselkedésük, a támadás módja és terjedésük szerint osztályozzák. Az elmúlt években sajnos a médiáknak köszönhetoen ezeket a különféle módszereket, egy kalap alatt, mint számítógépes vírusokat ismerte meg a világ. Pedig a vírusok csupán a kis hányadát alkotják azoknak a programozott fenyegetéseknek, amelyeket rosszindulatú programozók eddig megalkottak.

A programozott fenyegetések fo típusai a következoek:

1. Hátsó ajtók, kiskapuk vagy csapdák, amelyek lehetové teszik, hogy jogosulatlan felhasználók elérjék a rendszereinket.
2. Programférgek, melyek géprol-gépre terjednek a számítógép hálózatokon és nem szükségszeruen módosítják a cél gép programjait.
3. Trójai falovak vagy programok, amelyek látszólag normális programok, valójában azonban a háttérben egész mást csinálnak, mint amit kifelé mutatnak.
4. Baktériumok, melyek önmagukról abból a célból készítenek másolatokat, hogy elfoglaljanak egy számítógép-rendszert.
5. Logikai bombák, amelyek aktivizálódnak, amint bizonyos feltételek teljesülnek.
6. Vírusok, melyek olyan programok, amelyek módosítanak más programokat a számítógépek, azáltal, hogy az önmagukról készült másolatokat ezekbe beágyazzák.

A fent említett fenyegetések egy részét hasznosan is fel lehet használni. Például a programférgek alkalmazhatóak processzorokon számítások megosztására, a kiskapuk jól használhatóak nyomkövetésre, hibakeresésre és olyan vírusok is írhatóak, amelyekkel kisebb-nagyobb hibákat javíthatunk programokban. Nem a megközelítés, hanem a cél az, ami egy programozott fenyegetést valóban fenyegetové tesz.

Hátsó ajtók

A hátsó ajtók, kiskapuk vagy csapdák olyan kódrészletek, melyeket azért építenek bele egyes alkalmazásokba vagy operációs rendszerekbe, hogy biztosítsák a programozók számára ezen módszerek elérését anélkül, hogy végig kelljen járniuk a normális hozzáférési

utat. Ezeket a programrészleteket tipikusan alkalmazásfejleszto programozók írják, akiknek szükségük van a kód nyomkövetésére, működésének figyelésére a fejlesztés alatt. A legtöbb hátsó bejáratot olyan programokban helyezik el, amelyek egyébként csak hosszadalmas eljárások, beállítások, különbözo értékek beírása után hajlandóak normális esetben elindulni. A program nyomkövetésekor a fejlesztoknek természetesen mindig speciális privilégiummal kell rendelkezniük. A programozók ezzel azt is biztosítják, hogy van egy módszer a rendszerbe való bejutásra, akkor is ha a normális indítás valamilyen hiba miatt lehetetlen. Ezeknek a bejáratoknak a kódjai vagy bizonyos karaktersorozatokat ismernek fel, vagy pedig egy adott felhasználói azonosítóra lépnek muködésbe. Ezek után pedig speciális jogokat biztosítanak a felhasználónak. A kiskapuk akkor válnak csak fenyegetésekké, ha lelkiismeretlen programozók arra használják fel, hogy engedély nélkül férjenek hozzá rendszerekhez, vagy amikor a fejlesztok elfelejtik eltávolítani oket miután a rendszer nyomkövetése, tesztelése befejezodött és mások ezeknek a kódrészleteknek a létezését fel is fedezik.

Programférgek

A programférgek olyan programok, amelyek önmagukban is futóképesek és géprol gépre vándorolnak a számítógép hálózatokon keresztül. Lehet, hogy több részbol állnak, amelyek teljesen különbözo számítógépeken futnak. A programférgek nem változtatnak meg más programokat, viszont szállíthatnak olyan programokat, amelyek már igen (például vírusokat). Programférgeket nagyon nehéz írni, viszont rengeteg kárt tudnak okozni. Egy ilyen program kifejlesztése nem csak hálózatos környezetet igényel, hanem egy olyan programozót is, aki a hálózati szolgáltatásokon és eszközökön felül pontosan ismeri azokat az operációs rendszereket is, amelyeket programja a vándorlása során elérhet, hiszen csak így biztosíthatja az életképességét minden környezetben.

Trójai programok

A trójai programok nevüket a görög mondában szereplo Trójai lóról kapták. Nevüknek megfeleloen a modern idok trójai lovai ismert programokhoz (játékok, táblázatkezelok, editorok, stb.) hasonlítanak. Miközben a program úgy csinál, mintha azt tenné, amit a felhasználója akar, a háttérben valami teljesen mással foglalkozik. Például azt hisszük, hogy egy játékprogramot indítottunk el. Mialatt a program adatbázisok beállításáról mesél és rákérdez a játékosok számára vagy a nehézségi fokozatra, valójában állományokat töröl, lemezt formáz vagy valamilyen más módon változtatja meg a gépünkön található információkat. Mire erre rájövünk általában már túl késo. Ezek a trójai programok - sajnos - gyakori viccek néhány programozói környezetben. Gyakran és kegyetlenül helyezik el oket nyilvános adattári rendszereken, hogy aztán kézrol kézre járjon a felhasználók között, mint szabadon terjesztheto szoftvertermék.

Baktériumok

A baktériumok (vagy nyulak) olyan programok, amelyeknek nem kifejezett célja más állományok rongálása. Ezek a kódrészletek csupán önmagukról készítenek másolatot. Egy tipikus baktérium - többfelhasználós környezetben - általában elindítja magát két példányban vagy létrehoz önmagáról két újabb másolatot. Ezután mindkét másolat szintén reprodukálja önmagát két-két példányban, és így tovább. Így ezek a programok exponenciálisan szaporodva lefoglalják a gép processzor idejének, memóriájának, lemezkapacitásának jelentos részét és ezáltal lehetetlenné teszik, hogy a felhasználó ezeket az eroforrásokat hatékonyan kihasználja. A támadásoknak ez a típusa az egyik legrégebbi programozott fenyegetés. A korai többfelhasználós gépek felhasználói már futtattak ilyen programokat, hogy "leültessenek" egy gépet vagy csak azért, hogy kipróbálják mi történik. Kvóták (lemezhasználat korlátozása) és eroforrás korlátozások nélküli számítógép különösen ki vannak téve az ilyen jellegu támadásoknak.

Logikai bombák

A logikai bombák, olyan programozott fenyegetések, amelyek békésen lapulnak általánosan használt szoftverekben egy bizonyos ideig, amikor aztán elszabadulnak. Ekkor végrehajtanak valamilyen eljárást, ami voltaképpen nem feladata annak a programnak amiben elhelyezkednek. Ilyen logikai bombákat rendszerint olyan szoftver fejlesztok ágyaznak be a programokba, akik jogosultak a rendszer elérésére. A logikai bombát élesre állító feltételek sokfélék lehetnek. Megkövetelhetik adott állományok létezését vagy hiányát, egy adott idopont elérését vagy, hogy egy meghatározott felhasználó futtassa a programot. Egy logikai bomba ellenorizheti például eloször, hogy kik vannak bejelentkezve a gépre vagy mely programok futnak pillanatnyilag a rendszeren. Miután kioldódott, tönkreteheti vagy módosíthatja az adatokat, leállíthatja a számítógépet vagy más módon rongálhatja a rendszert. Egy klasszikus eset, amikor a logikai bomba leolvassa egy alkalmazott azonosítószámát és kioldódik abban az esetben ha ez a szám nem szerepel két egymást követo fizetési listán.

Az idozített bombák speciális válfajai ezeknek a fenyegetéseknek, amelyeket általában fizetések vagy egyéb szerzodésben meghatározott feltételek nem teljesítése esetén szoktak alkalmazni. Például leállíthatják bizonyos programok muködését egy meghatározott ido után, ha nem teszünk speciális intézkedéseket.

Rosszindulatú logikai bombák ellen ugyanúgy tudunk csak védekezni, mint a kiskapuk ellen. Ne telepítsünk szoftvereket gondos tesztelés és átolvasás nélkül. Rendszeresen mentsük az adatainkat, így ha valami történik, még mindig vissza lehet állítani egy elozo jó állapotot.

Vírusok

A vírusok olyan kódsorozatok, amelyek más végrehajtható programokban helyezkednek el, így amikor ezek a gazdaprogramok futnak, akkor a víruskódok is végrehajtásra kerülnek. A vírusprogram ekkor elhelyezi az önmagáról készített másolatot egy vagy több még nem

fertozött végrehajtható állományba. A vírusok nem önálló programok, magukban nem képesek muködni, csak egy másik program részeként, amely program - ha vezérlés kerül rá - magát a vírust is aktivizálja. A vírusok viszonylag új jelenségek és olyan személyi számítógépeken léteznek, amelyeknek az operációs rendszere nem rendelkezik kello védelemmel. Ezek közé tartozik az Apple Macintosh és az IBM PC. Bár vírusok a UNIX operációs rendszer ellen is készültek, ez idáig úgy tunik nem jelentenek komoly fenyegetést a UNIX világra. Valójában minden olyan feladat amelyet egy vírus végrehajthat, - a root jogok megszerzésétol az állományok törléséig - végrehajtható egyszerubb módon is.

Boot szektor vírusok

A boot szektor a legelso szektor a floppy-lemezeken. Merevlemezeken ez a DOS partíció legelso szektora. Információkat tartalmaz a lemezrol, mint például a logikai szektorok száma, ezenkívül egy rövid program is található benne. Amikor egy gépet elindítunk, az beolvassa a boot szektort, betölti a memóriába és elindítja az ott található kis programot. A boot szektor vírus kicseréli a szektorban található kódot a sajátjára és az eredeti szektort valahová elrakja a lemezen. Erre azért van szükség, hogy később (miután o már lefutott) átadhassa a vezérlést az eredeti programnak, hogy a normális rendszertöltés folytatódjék.

Tehát ez a vírus már rendszerindítás alatt megfertozi a gépet, mielott bármilyen más program elindulhatna, ezért eközben programmal védekezni ellene lehetetlenség.

Partíciós tábla vírusok

A partíciós tábla a merevlemezek legelso szektora. Információkat tartalmaz az adott lemezrol (például a szektorok száma partíciónként, hol kezdodik a DOS partíció) és egy kis programot. Amikor egy PC elindul, beolvassa ezt a szektort és végrehatja a kódot. Egy partíciós szektor vírus hasonló a boot szektor vírusokhoz, azzal a különbséggel, hogy nehezebb megtalálni, hiszen sok program nem enged betekintést a partíciós szektorba. Floppy lemezeken nincs ilyen szektor. A partíciós tábla kódja még elobb kerül végrehajtásra mint a boot szektoré, ezért természetesen külön szoftverrel nem lehet a betöltését megakadályozni.

Az állomány vírusok

Az állomány vírusok egyik fajtája a DAFV (Direct Action File Virus).

Ezek a vírusok beleépülnek a végrehajtható állományokba. A fertozött állományok legtöbbször COM vagy EXE kiterjesztésuek, de lehetnek ugyanakkor SYS állományok vagy overlay típusúak, amelyeknek gyakorlatilag bármilyen kiterjesztésük lehet.

A COM állományok elso három bájtja egy ugró utasítás a tényleges programkódra. A vírus hozzáfuzi magát az állományhoz, az ugrási címet pedig önmagára állítja. A víruskód utolsó utasítása pedig egy ugrás az eredeti programra. Mindez természetesen pillanatok muve és a felhasználóban fel sem merül a gyanú, hogy voltaképpen a tényleges program elindulása elott a vírus is lefutott.

EXE állományokat fertozo vírusokat nehezebb írni, mert ezeknek az állományoknak bonyolultabb a struktúrája. Léteznek olyan vírusok is, amely mind az EXE mind pedig a COM állományokat fertozheti, ebben az esetben a vírus az állománytípusnak megfeleloen különbözo módszert alkalmaz.

Egy állomány dátumát megváltoztatni nagyon könnyu, ugyanilyen egyszeru az eredeti dátumot visszaállítani, erre minden ilyen típusú vírus képes. Szintén egyszeru egy állomány attribútumait megváltoztatni, tehát a DOS-os írásvédelem nem jelent akadályt ezeknek a vírusoknak a számára. Más a helyzet azonban hálózatos környezetben. Ha a bejelentkezo felhasználónak nincs privilégiuma egy állományt írhatóvá tenni, akkor a gépén található vírusnak sincs.

Az állomány vírusok másik fajtája a IAFV (Indirect Action File Virus).

Ezek a vírusok szintén a COM és EXE állományokat támadják, de avval a különbséggel, hogy ok a memóriába telepítik magukat és általában a 21h megszakítást használják, mert az operációs rendszer ezt használja a COM és EXE állományok betöltéséhez és futtatásához. De elofordul, hogy a vírusok az állományok megnyitására, lezárására, vagy éppen könyvtárbejegyzések elolvasására szolgáló funkciókat cserélik le a vírus kódjára. Természetesen ezek a funkciók nem vesznek el, hiszen a vírus, miután végrehajtotta a saját utasításait (közben továbbfertozve más programokat), visszaadja a vezérlést az eredeti megszakításnak, és így mi ebbol semmit sem veszünk észre.

Tehát elég csak egyszer is futtatni egy IAFV vírust ahhoz, hogy egy csomó állományt megfertozzünk.

Külön kell szólni az utóbbi idoben igen elterjedt ún. makróvírusokról. A makró utasítások egy-egy rendszer utasításainak csoportba foglalását jelentik. Ma már szinte minden szerkesztorendszer – legyen az szöveg vagy rajzszerkeszto – támogatja a feladatok ilyen módon való hatékonyabbá tételét. Ezt használják ki rosszindulatú makróutasítások fejlesztoi is. Ezek a makrók az állománnyal együtt terjednek, és az új környezetben is hatékonnyá válnak. A legelterjedtebb szövegszerkeszto, a Word is alkalmas ilyen fertozésre. Ezek a makróvírusok néha csak apró vicces üzeneteket tartalmaznak, de más esetben letiltják a szövegszerkeszto néhány utasítása-

nak felhasználhatóságát, illetve lehetetlenné teszik a fertozött állomány mentését.