VÍRUSPROGRAMOK
II.

Vírusprogramokról szóló előző cikkünkben meghatároztuk ugyan, hogy mit értünk a kifejezés alatt, hogyan előzhető meg nagy valószínűséggel a fertőzés és milyen szimptomák utalnak a számítógép működésében a vírusprogram által előidézett zavarokra. Tehát alkalmaztuk a *"jobb félni mint megijedni"* elvet. Ugyanis egy vírusprogram pillanatok alatt tönkreteheti hónapok megfeszített munkáját. Ma lehetséges olyan programot írni, amely belátható időn belül tönkreteheti egy számítógép-generáció működését.

A vírusprogram az élő anyag működését utánozó modell. Ebben az esetben is alkalmazhatók a járvány-matematika törvényszerűségei, eredményei. (*Mint példa: egy fertőző gócból kiinduló járvány terjedése modellezhető, de ha gyógyíthatatlan kórról van szó, akkor a megfertőzhető népesség mintegy kétharmadának kihalása után a fertőzés önmagától már nem terjed tovább, majd teljesen megszűnik*). A témával kapcsolatos kutatások már 1957-ben elkezdődtek. (N.T.J. Baily;The Mathematical Theory of Epydemics Ed: Hafner 1957)

Az 1980-as évben a katonai körök is úgy látták, érdemes ezzel foglalkozni. Sokáig azonban nem lehetett elrejteni az önreprodukáló programok létét, hiszen 1984-ben a Der Spiegel magazin egy rövid cikkben hívta fel a figyelmet, sőt a számítógépes kultúrára leselkedő veszélyekről is írt.

E történelmi áttekintésből nem hagyhatjuk ki Friedrich Cohen nevének említését, aki egy tanulmányban (*Computer Viruses Theory and Experiment 1983*) számolt be kutatásainak eredményeiről. Kísérleteit egy VAX típusú gépen, UNIX multitasking (*többfeladatos*) operációs rendszerkörnyezetben végezte. Az eredmények több mint megdöbbentőek voltak. A multitask környezetben a vírus elindítása után szinte a nulladik időpillanatban megfertőzött több rendszerállományt valamint az adminisztrátor programot. Az elindítás utáni 18. másodpercben négy felhasználó állományai is fertőzöttek voltak.

Számítógépes hálózatban végzett kísérleteknél a fertőzés a 600. másodpercben vált teljessé. Hangsúlyoznunk kell, hogy a kísérletek alatt a rendszerek nem rendelkeztek semmilyen beépített vírus elleni védelemmel.

A vírusprogramok írását a hackerek - hobbysok - jó tréfának tekintették és az első gyakorlatban is használható elméleti közleményeket is ők közölték a Bayrische Hackerpostban. Sajnos azonban a témát átvették a terrorista szervezetek is. Így az első olyan programvírus, amit kifejezetten terrorista szellemben írtak, az izraeli Hebrew University számítógépes hálózatát célozta meg.

Ezután a lavina elindult és nem lehetett megállítani. Napjainkban az ismert vírusprogramok (*a Mc Afee Associates által katalogizált vírusok*) száma több százra (*700-800*) tehető.

Osztályozásuk tekintetében szabványnak fogadható el a John Mc. Afee féle Virscan programrendszer által használt elnevezések.

Hogy mégis tisztán lássunk a kárt okozó programok sokszínű rengetegében megadunk egy általánosabb osztályozást:

Programférgek - azok a programok, amelyek mintegy átrágják magukat egy számítógép-rendszer védelmi mechanizmusán, és legtöbbször az a feladatuk, hogy az operációs rendszer magvából - a kernelből - kihozzanak bizonyos információkat (pl. *jelszótáblákat*). Kárt nem okoznak. (Hm!?)

Trójai programok (vagy *trójai faló típusú programok*) - azok a programok, amelyek mást tesznek mint amit igérnek. (Pl. *trójai program lehet akár egy játék is, vagy mialatt lefut egy számítógépes pornó-show tönkremegy a merevlemez*). Az ilyen típusú programok még nem egészen vírusprogramok hiszen szaporodásuk szigorúan a hordozó programhoz kötött és csak ennek a lemásolása útján terjednek.

Vírusprogramok - azok a programrendszerek, amelyek képesek önmagukat reprodukálni. Programok fertőzésével, formázott mágneslemezzel vagy

magával a számítógéppel terjednek illetve számítógépes adathordozókon keresztül is terjedhetnek. A fertőzés, a támadási felület, a kórokozás és terjedés további osztályozási kritériumok (*feltételek*). Ezek jól meghatározott szerepet kapnak a McAfee féle Virnet rendszerben.

Ennek alapján beszélhetünk a következőkről:

1. Memóriaszemét vagy "kuka-vírusok"

Általában nem rongálják a rendszerben lévő adatokat: egyéb kárt nem okoznak, csupán teleszemetelik a memóriát (*ezáltal lehetetlenné tehetik egy másik program futását*) és egy kicsit lefagy a rendszer (*néhány száz gépen*). Ide tartoznak még az úgynevezett "*kiszolgáltató*" vírusok, amelyekkel a számítástechnikai adatvédelmi rendszereket lehet kijátszani. Ez utóbbiak a "*poloskák*", amelyek a teljesjogú rendszergazda által használt jelszót figyelik, majd ezt egy állományba beírják. Innen már csak le kell kérdezni a jelszót és ennek ismeretében a rendszer teljes ellenőrzés alá vonható.

2. A programkódot módosító vírusok

Olyan programok, amelyek önmagukat képesek reprodukálni és a legtöbb kárt okozzák. Eredeti formájukban sosem találkozunk velük, kivéve ha magunk nem írunk ilyent, viszont az általuk módosított, megfertőzött programokkal a legtöbb felhasználónak már volt dolga. Úgy is mondható, hogy ezek a tulajdonképpeni programvírusok. Ezek hatásmechanizmusáról, a későbbiekben lesz szó.

3. Hardware vírusok

Ezen programok gyári uton már a gyártás folyamatában kerültek be a számítógép rendszerbe. Ismerve, hogy a számítógépek kategoriájában az AT az első olyan gép, amelynek rejtett zugaiban (*óra IC vagy C-MOS memória*) lehet ilyen programokat tárolni.

A COCOM listával kapcsolatos vitában hangzott el az, hogy a szuperszámítógépek és programjaik olyan védelemmel vannakellátva, amelyek megakadályozzák ismeretlen helyen való működésüket. Ezek a gépek műholdas kommunikáción keresztül ellenőrizhetők és tönkre is tehetők. (lásd: iraki háború).

4. Hardware-módosító vírusok

Sokáig tartotta magát az a tévhit, hogy programok segítségével nem tehetők tönkre az áramkörök. Az integrált áramkörök gyártása tipizált és tulajdonképpen csak a mikroprogram beégetése után dől el, hogy az áramkört milyen célra tervezték. A mikroprogramot pedig bármikor módosítani lehet. Igy van ez a 80386-os mikroprocesszor esetében is. Léteznek olyan nem publikált utasítások, amelyek segítségével elérhető a mikroprogram átírása és máris vihetjük gépünket a szervizbe. Ilyen hatásmechanizmussal működik az a hardware-módosító vírus, amelyet a Sierra Software cég Larry játékprogramjainak egyes kalózváltozatai terjesztettek. Ez a vírus először megfertőzte a számítógépen levő rezidens programokat, majd a magasszintű programnyelven megírt szövegszerkesztőket. Azután pedig ha a felhasználó nyomtatni szeretett volna Epson típusú nyomtatóján, akkor már érthetetlen zagyvalékot kapott. A vírus kissé megkeverte a nyomtató memóriájában levő karakterkészletet.

Mivel a programkódot módosító vírusok a legelterjedtebbek és ezek okozzák a legtöbb bajt, a továbbiakban főleg róluk lesz szó, illetve azokról a módszerekről amelyekkel detektálhatók illetve írthatók. A vírus egyfajta rablópandur relációban van a víruskereső és immunizáló programokkal. Mindig megelőzi egy lépéssel az utóbbiakat.

Tulajdonunkban lehet a legszebb és a legjobb, mondjuk 1000 vírust detektáló és írtó program, ha a "*piacon*" egy újabb szörnyet engedett el valaki. Egyértelmű tehát, hogy felkészíteni egy víruskereső programot egy újabb vírussal való találkozásra csakis ez utóbbi tulajdonában tehetjük meg. Igaz, ugyan, hogy léteznek bizonyos alapelvek és ezen elvek alapján felépített kártyák, amelyek nagy valószínűséggel érzékelik, ha egy fertőzött program bejut a rendszerbe.

A vírusprogramok minden esetben valamely program segítségével (*elindításával*) kerülnek be a számítógépbe. Ha a vírusprogram beépül az úgynevezett boot szektorba illetve a particiós táblába akkor boot-vírusról illetve particiós-tábla-vírusról beszélünk.

A fertőzési módszer a következő: - a boot szektor a mágneses lemezek 0. sávjának 0. szektorát jelenti. Az operációs rendszer a formázás során egy program jellegű bevezető részt hoz létre. A számítógép betöltési folyamata a következőképpen zajlik le: - a gép bekapcsolása után először a BIOS (*Basic Input Output System*) lefuttatja a számítógép tesztjét, majd az "*A*" lemezegységhez fordul. Ha ott nem talál lemezt akkor a merevlemez első "*C*" jelölésű egységét vizsgálja és megnézi, hogy van-e a lemezen operációs rendszer. (*Ezt az információt is a boot szektor tartalmazza.*) Ha van, akkor betölti a memóriába a boot-szektorban levő programot, majd ennek segítségével az operációs rendszert is.

A boot vírusok beépülnek a boot szektorba, előbb azonban ennek tartalmát elmentik valahova a lemezen úgy, hogy ezt az elmentett részt hibás szektorként álcázzák. Ha tehát az operációs rendszert akarjuk betölteni, akkor, a boot vírus megszakítja ezt a folyamatot, előbb ő töltődik a memóriába, majd folytatódik az operációs rendszer betöltésének folyamata. Mindez olyan hamar megy végbe, hogy a felhasználó észre sem veszi.

Egy másik típusú vírusprogram a programvírus, amely a számítógépen levő végrehajtó állományba a COM, EXE, OV* típusúba épül be. Minden végrehajtható program két részből áll:

- adatokból
- végrehajtható kódból

Azt, hogy mi adat illetve kód, a program fejléce határozza meg. A COM típusú programoknál a program első három byteja egy ugróutasítás amely átadja a vezérlést a programkódba. Míg az EXE típusú programoknál az úgynevezett header (*fejléc*) mondja meg, hogy hol kezdődik a programkód. Ha egy programvírus megtámad egy ilyen típusú állományt (*COM, EXE*) szépen kivájja a program kezdeti állapotára vonatkozó adatokat, azokat saját kódjában elraktározza, majd bemásolja magát a programba és a vezérlést saját magára irányítja a program fejlécében. Így rögtön a memóriába való betöltéskor a vezérlést előbb a vírus veszi át.

Ennek alapján most már nyugodtan elmondhatjuk, hogy a víruskeserő programok is ezt a módszert követik. Azaz megnézik hol kezdődik az állományban a programkód és ott kezdik keresni a vírust.

AJÁNLOTT IRODALOM

1. Famosi István-Szegedi Imre-Kis János: Viruslélektan, Ed. Cédus 1990.
2. Scan. Doc
3. Virlist. TXT
4. dr. Szegedi Imre-Kis János:Topguard. Doc-1991.

Vásárhelyi József

VÍRUSNAPTÁR: 1992

Igaz ugyan, hogy jelen kiadványban még nem írtunk részletesen az egyes vírusprogramokról és azok előfordulásáról, mégis úgy gondoljuk, hogy a jelenlegi katasztrófális jogrendszer és ennek minden következménye ami a PC világot érinti szükségessé teszi az alábbi vírusnaptár közlését.