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.

Természetesen a felsorolt vírusok közül nem mindegyik látogatott el hozzánk, de figyelembe véve a "*hoci-nesze*" software másolást hamarosan találkozunk velük, hogy a hazai tenyészetet ne is említsük (*Lipici 1., Lipici 2, FSN*)

A listából kiemelünk néhányat, amelyek jelenléte bizonyos és ráadásul különösen pusztító: - a Jerusalem sorozat tagjai, Michelangelo, Tequila, Joshi, Dark Avenger.

Bár a Dark Avenger aktiválódása nem dátumhoz kötött, mégis megemlítjük mint jó öreg klasszikus kemény fickót.

E naptár hasznos lehet abból a szempontból is, hogy új programjainkat - egy jó *Scan* hiányában - úgy is tesztelhetjük vírusvédelem szempontjából, hogy többször előreállítjuk a számítógép rendszeridejét.

Azonban, ez a vírus aktiválódásának élesben való kipróbálását teszi lehetővé - amennyiben jelen van -, de még mindig jobb ezt elvégezni egy tesztgépen minthogy értékes adatainktól mondjunk búcsút.

AKTIVÁLÓDÁS IDŐPONTJA	VÍRUS NEVE
minden vasárnap	Sunday
	Sunday-2
minden hétfőn	1-B (Bad Guy)
	1-B (Bad Guy 2)
	1-B (Exterminator)
minden kedden	Ah
	1-B (Demon)
	1-B (Demon-B)
kedd 1-én	kedd elseje (magyar péntek 13)
kedd 13-án	Jerusalem B (Anarkia)
csütörtök 12-én	CD
minden pénteken	Frère Jacques
	Smack
pénteken ha az nem 13-a	Payday
péntek 13-án	1720
	Friday The 13th COM
	Jerusalem
	Jerusalem B
	New Jerusalem
	RAM Virus
	Suriv 3.00
	Westwood
péntek 13-án (1992-től)	Hybryd
minden hó 15-e utáni pénteken	B Jerusalem (Skism-1)
minden szombaton	Italien Pest (Finger)
szombat 14-én	Saturday The 14th
minden hó másodikán	Flip
minden hó 5-én	Frog's Alley
minden hó 8-án	Taiwan
minden hó 13-án	Monxla
minden hó 18-án	FORM-Virus (Formv-18)
minden hó 24-én	FORM-Virus
január 1-től - szept. 21-ig	Plastique (COBOL)
január 5-én	Joshi
január 25-én	Jerusalem B (January 25 TH)
március minden napján	903
március 6-án	Michelangelo

április elsején	Casper
	Christmas Tree
	Suriv 1.01
	Suriv 2.01
	Suriv 4.02
április 15-én	Murphy (Swarni)
május 1-től - május 4-ig	1210
június 6-án	Kennedy
június 16-án	June 16 TH
július 1. - szeptember 1. között	Töltögető (Filler)
július - december közt naponta	Got-you
	Jerusalem B (Mendoza)
július 13-án	July 13 TH
szeptember minden napján	1554
szeptember minden napján	1704 Format
	AirCop (AirCop-B)
	Cascade, Cascade-B
szeptember 4-én	Violator (Violator B1)
szeptember 20-tól december 31-ig	Plastique, Plastique-B
szeptember 22-től december 31-ig	4096
október 1-től december 31-ig	1554
	1704 Format
	4096
	Cascade
	Cascade-B
október 4-én	Violator (Violator B1)
október 13-tól december 31-ig	Datacrime
	Datacrime-B
	Datacrime II
	Datacrime II B
október 31-én	Violator (Violator B2)
november 4-én	Violator (Violator B1)
november 18-án	Kennedy
november 22-én	Kennedy
december minden napján	1253
december 4-én	Violator B1
december 19-31. között naponta	Father Christmas
december 21-én	Poem
december 24-én	Icelandic-III
december 24-től január 1-ig	Christmas Tree
december 25-én	Christmas In Japan
	Violator (Violator B3)
december 28-án	Spanish April Fools
december 31-én	Violator (Violator B2)
1989 augusztus 1. után	Fu Monchu
1990 augusztus után	Data Lock
1990 augusztus 14. után	Violator
1990 november 11. után	Fingers
1992 január 1 - december 31 között	Europe-92
1990 július 1-jétől	Flash

Vásárhelyi József