Počítačové vírusy

Vírus je program, ktorý sa sám rozmnožuje do iných programov tým, že sa k nim pripojí podľa určitých kritérií (napr. dátum nar. autora vírusu, počet spustení infikovaného programu, ...) sa aktivuje a škodí.

Delenie vírusov:

1)súborové- napádajú súbory

2)bootovacie - napádajú bootovacie oblasti diskov

sú to tie oblasti, z ktorých BIOS načítava dáta ako prvý (odtiažto sa začína

načítavať aj systém, a miesto neho sa načíta vírus, ktorý zavedie systém)

3)trójske kone- vírusy, ktoré sa aktivujú len v určitý dátum/hodinu prípadne pri

splnení určitých podmienok a vykonávajú najnepríjemnejšiu činnosť (mazanie súborov,

formátovanie disku..)

Vírusy škodia vo dvoch fázach svojej činnosti a to obdobie

Latencie- vírus sa neprejavuje, len sa skryte mnohí

Akcie- vírus sa prejaví

ĎALŠIE ROZDELENIE JE PODĽA SPÔSOBU MANIPULÁCIE S OBJEKTOM SVOJHO NAPADNUTIA, PRÍPADNE PODĽA SPÔSOBU ŠÍRENIA:

prepisujúci vírus – prepíše kód napadnutého súboru, čím ho zničí

link vírus – pripojí sa k súboru, pričom zachová jeho funkčnosť

doprovodný vírus – nezapisuje svoj kód do EXE súboru, ale vytvára si tieňový súbor s rovnakým menom a príponou COM.

vírus priamej akcie – pri svojom spustení vykoná svoju “prácu“, čo je typické pre prepisujúce vírusy

rezidentný vírus – je trvalo prítomný v pamäti počítača a môže neustále ovplyvňovať jeho činnosť

stealth vírus – dokáže prevziať kontrolu niektorých funkcií operačného systému a pri pokuse o čítanie infikovaných objektov vracia stav pred infikovaním. Pokiaľ program nie je vybavený antistealth technikami nemá možnosť takýto vírus zistiť

zakódovaný vírus – takýto vírus je zašifrovaný nejakým kľúčom a iba krátka dešifrovacia funkcia je vždy rovnaká

polymorfný vírus – takýto vírus si pre každý napadnutý objekt vytvára celkom novú dešifrovaciu funkciu a v napadnutých súboroch nie je možné nájsť žiadne rovnaké sekvencie kódu

fast infektor – tento vírus napáda súbory nie len pri ich čítaní, ale aj pri manipulácii s nimi

slow infektor – je to vlastne opak fast infektoru. Vírus sa snaží byť čo najmenej nápadný. Šíri sa pomaly a má tak aj väčšiu šancu zostať nepozorovaný

Aby ste sa niečomu takému mohli úspešne vyhnúť potrebujete nielen trochu počítačovej disciplíny ale aj kvalitný antivírusový systém

Správanie sa počítačových vírusov:

1) nevinné žartíky- zahranie pesničky o 17.00 (Yankee Doodle)

padanie písmenok z obrazovky (CR1701)

2) deštrukcia súborov- vírus Dbase prepisuje a ničí databázové súbory

3) deštrukcia hardwaru- prílišné rozkmitanie hlavičiek disku

krčenie papiera v tlačiarni

znefunkčnenie grafickej karty

Antivírové programy:

Jedným zo spôsobov ochrany proti vírusom je používanie antivírových programov.

Sú medzi nimi rozdiely v rýchlosti, počtu vírusov, ktoré poznajú a v cene.

Filozofia antivírového programu spočíva vo využití troch úrovní ochrany:

1) Nájdenie vírusu (SCAN)

2) Odstránenie vírusu (CLEAN)

3) rezidentný strá□ca (VSHIELD) - ten je v pamäti a kontroluje aktivitu vírusov

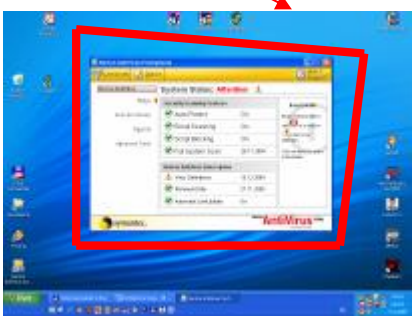
Najznámejšie:

Panda - Panda antivirus

NOD - www.eset.sk

AVG – www.AVG.sk

Norton Antivirus



Ochrana pred vírusmi:

1) Používanie len legálne kúpeného softwaru

2) Každú novú disketu sa odporúča otestoval antivírovým programom

3) Je dobré archivovať si dôležité dáta na disketách chránených proti zápisu

4) Pravidelná kontrola počítača proti vírusom

5) Kontrolné opatrenia ohžadne prístupu osôb k počítaču