Ja, vírus

Hľa, monitor už dohasína,
súbory z disku miznú v diaľ,
bezmocný užívateľ ruky spína,
na duši zloba, v srdci žiaľ.

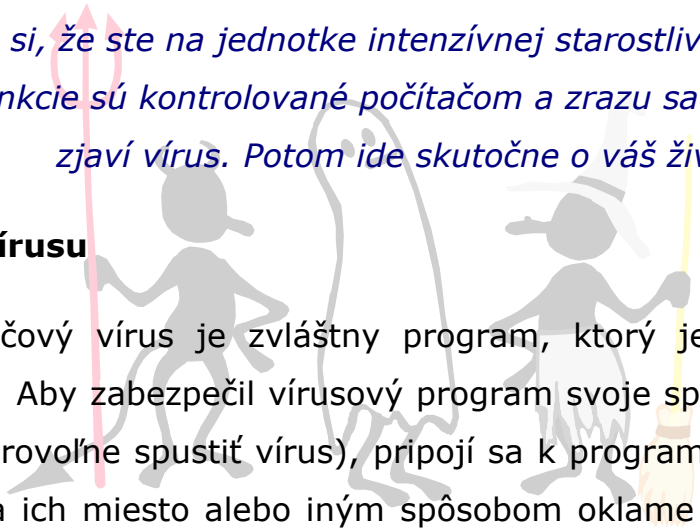
Ja, vírus, všetko zničím,
z disku vám stokrát vzklíčim,
za mesiac obehnem svet,
úniku predo mnou niet!

Päťkrát ma porazte,
desaťkrát vstanem.
Dúfate, že ma už niet?
Ja vás vždy sklamem.

Bráňte sa, ako len chcete,
Psami, Scanom, Toolkitom.
Účinnú zbraň nenájdete,
zničiť vírus je len snom.

Zrodený nenávisťou temnou,
stvorený z bahna zloby,
zotročím všetky počítače,
a navždy vrhnem do poroby.

"Predstavte si, že ste na jednotke intenzívnej starostlivosti. Vaše základné životné funkcie sú kontrolované počítačom a zrazu sa na tomto počítači zjaví vírus. Potom ide skutočne o váš život."



Definícia vírusu

Počítačový vírus je zvláštny program, ktorý je schopný vytvárať svoje kópie. Aby zabezpečil vírusový program svoje spustenie (veď kto by si chcel dobrovoľne spustiť vírus), pripojí sa k programom na disku, alebo sa položí na ich miesto alebo iným spôsobom oklame užívateľa. Vírusové programy vytvorili šikovní programátori s pochybnou morálkou.

1. Boot vírusy

Boot vírus je na začiatku diskety alebo pevného disku. Na tomto mieste sa nachádza program, ktorý je automaticky vykonávaný pri zapnutí počítača. Ak je na mieste tohto programu vírus, automaticky sa aktivuje po spustení počítača.

Po zapnutí sa počítač díva najprv do disketovej jednotky. Ak je tam disketa, pokúša sa spustiť program zo začiatku diskety (tzv. zavádzací program). Ak je disketa napadnutá, spustí sa vírus. Preto nesmieme zabúdať diskety v disketovej jednotke! Ak počítač nenájdee disketu, prejde na pevný disk a púšťa program zo začiatku pevného disku (z tzv. partičného sektoru).

Tento vírus sa prenesie z pevného disku aj na disketu, kde nie sú žiadne súbory. Z diskety na pevný disk sa prenesie len vtedy, ak zabudneme diskety v mechanike pri bootovaní (štarte) počítača.

2. Súborový vírus

Súborový vírus sa pripája k vykonávateľným súborom - programom (tie majú príponu - rozšírenie - COM, EXE, OVL, BIN a iné), alebo ich prepisuje. Tento vírus sa aktivuje, ak spustíme napadnutý program. Na diskete s údajovými súbormi sa tento typ vírusu nevyskytuje.

Vírusy sa delia aj inak na dve veľké skupiny - pamäťovo rezidentné (trvalo umiestnené v pamäti) a nerezidentné.

Nerezidentný vírus môže spôsobovať nákazu len pri spustení napadnutého programu. Nakazí bežne 1 - 4 súbory.

Rezidentný vírus sa po spustení napadnutého programu usadí v pamäti počítača. Potom už len sleduje, čo sa deje na pevnom disku, alebo diskete. Za istých okolností (spúšťanie programu, otvorenie súboru, prezeranie adresára) napáda ďalšie programy. Jeden vírus môže napadnúť ľubovoľne veľký počet programov. Jeho činnosť sa zvyčajne končí po vypnutí alebo resete počítača.

Škody spôsobené vírusmi

Mnohé vírusy okrem tvorby svojich kópií majú zabudovanú schopnosť spôsobovať užívateľov škody. Bežné škody sú tieto:

- preformátovanie pevného disku,

- znemožnenie prístupu k súborom na disku,

- poškodenie obsahu časti pevného disku,

- vymazanie alebo poškodenie programov,

- poškodenie údajových súborov.

Menšie škody sú spôsobené stratou programov. Tie si opätovne nahráme z originálnych diskiet. Veľké škody bývajú, ak stratíme súbory s dôležitými údajmi. Takýmto škodám môžeme zabrániť pravidelným zálohovaním (skopírovaním) dôležitých údajových súborov na diskety.

Ako sa dostanú vírusy do počítača

- disketami,

- linkami počítačovej siete,

- telefónnou linkou a modemom.

Cyklus prenosu prostredníctvom diskiet:

1. Prenos vírusu z diskety do počítača.

2. Rozmnoženie sa vírusu v počítači.

3. Prenos vírusu z nakazeného počítača na ďalšie diskety.

Vírus vykonáva škodlivú činnosť počas druhej fázy.

Ako sa brániť proti vírusom

a) Používaním len legálnych programov (aj v nich môžu byť vírusy!).

b) Využitím antivírusových programov.

c) Dostatočnou informovanosťou o problematike a následným prijatím adekvátnych opatrení.

Antivírusové programy

Vyhľadávací program, polydetektor (scanner)

Vyhľadáva jemu známe vírusy na pevnom disku alebo diskete, zvyčajne podľa malých kúskov kódu, ktoré sú typické pre daný vírus. Keďže sa objavujú stále nové vírusy, je potrebné aspoň raz za 3 mesiace scanner aktualizovať. Týmto programom vieme zachytiť vírus ešte na diskete, bez toho aby sa dostal do nášho počítača (prevencia).

Pamäťovo rezidentný polydetektor (resident scanner)

Tento program funguje rovnako ako bežný scanner, ale je trvalo usídlený v pamäti. Kontroluje všetky spúšťané a kopírované programy. Ak zistí v niektorom z nich vírus, zastaví prácu s napadnutým programom. Aj tento program slúži k prevencii.

Indikátor zmien v programoch (checksummer)

Tento program si vytvorí o všetkých programoch na disku isté údaje (zvyčajne kontrolné súčty). Potom pravidelne porovnáva aktuálny stav s uloženými údajmi. Ak dôjde k zmene v porovnaní s minulým stavom, je pravdepodobné, že vírus napadol počítač. Tento typ programu zaregistruje aj prítomnosť neznámych vírusov a netreba ho aktualizovať. Vírus zaregistruje až vtedy, keď sa prejaví (teda už je v počítači).

Monitor podozrivých činností

Tento program sa usadí v pamäti a kontroluje, či nedochádza k pokusom o nedovolenú činnosť, napr. formátovať pevný disk, modifikovať programy. Ak dôjde k takémuto pokusu, program užívateľa na to upozorní a pýta si povolenie na vykonanie danej činnosti. Tento typ programu je určený skôr pre profesionálnych užívateľov.

Liečiaci program (cleaner)

Tento program dokáže odstrániť súborové a boot vírusy. Niekedy sa dá vírus odstrániť len za cenu vymazania napadnutého súboru.

Zhrnutie:

• Vírusy sú škodlivé programy.

• Prenášajú sa najmä disketami.

• Diskety a pevné disky treba kontrolovať antivírusovým programom.

• Dôležité údaje pravidelne zálohujeme.

• Ak nájdeme vírus, treba ho odstrániť (po zálohovaní údajov).

Replikátory - objekty schopné vyrábať (alebo byť predlohou pre) svoje kópie. Patria tu aj počítačové vírusy.

Sú počítačové vírusy užitočné?

Tvorba škodlivých vírusov je prospešná evolúcii vírusov. Škodlivé vírusy nútia ľudí vytvárať čoraz dokonalejšie antivírusové programy. Tieto antivírusové programy nútia tvorcov vírusov vyrábať čoraz viac dokonalejšie, životu podobnejšie formy vírusov. Preto sa objavili stealth (neviditeľné) vírusy, potom enkrypčné (ktoré sa zakódujú), mutačné (potomkovia sa líšia od rodičov). Možno špičkový tvorcovia vírusov pracujú na výrobe vírusov, ktoré by boli schopné darwinovskej evolúcie (to by bola sila!) podobne ako v živom svete.

Preto sú práve škodlivé vírusy hnacím motorom evolúcie počítačových vírusov. A možno práve táto vetva vývoja technológie povedie k stvoreniu iných foriem života.

Parazity

Parazitujú na iných replikátoroch (hostiteľoch). Parazit bez svojho hostiteľa zvyčajne nie je schopný sa replikovať (napr. u ľudí pásomnica).

Mimikry

Ide o napodobovanie tvaru jedného replikátora iným.

Podobne je to aj s počítačovými vírusmi. Tiež parazitujú na bežných aplikačných programoch, alebo na programoch na začiatku diskov. Iné vírusy, aby sa mohli rozmnožovať, využívajú istú formu mimikry preto, aby sa zamaskovali pred užívateľom.

Textové replikátory

- porekadlá, príslovia, vzorce, texty pesničiek, básne, návody, ale aj zdrojové texty vírusov.

Na uchovávanie textových replikátorov vytvorili ľudia mnoho médií: hlinené tabuľky, pergamen, papier, celuloidový film, vonkajšie počítačové pamäte (optické a magnetické disky, pásky). Osobnitným médiom je ľudský mozog.

Zvukové replikátory

Aj vírusy môžu existovať vo forme zvukovej nahrávky, napr. ak je program nahraný na bežnú magnetofónovú pásku.

Niektoré vírusy využívajú zvuk na svoju exhibíciu. Najznámejším príkladom takéhoto vírusu je Yankee Doodle, ktorý o 17:00 zahrá melódiu, aby sme vedeli, že ho máme.

Počítač a replikátory

Počítače poskytujú mimoriadne vhodné prostredie pre replikátory. Replikátorom je tu zvyčajne súbor (text, program, databáza, obrázok a pod.) alebo jeho časť. Replikácia prebieha zvyčajne medzi vonkajšou (disk) a vnútornou pamäťou (RAM) počítača.

Uskutočnenie replikácie je vďaka službám operačného systému veľmi triviálne (príkaz COPY).

Čo sa deje v počítači?

Základné pojmy

Počítač je univerzálne programovateľný automat.

Z hľadiska vírusu je *počítač* prostriedok, pomocou ktorého vytvorí vírus svoje kópie. Počítačový vírus nevie (zatiaľ) modifikovať hardware počítača (napr. pridať si pamäťový čip). Snáď je potenciálne schopný spôsobiť nejaké poškodenie hardwaru.

Jednou z hlavných úloh v živote vírusu je stať sa programom, ktorý počítač vykonáva.

(Program je zápis algoritmu v jazyku zrozumiteľnom počítaču. Algoritmus je návod.)

Software - programy, programové vybavenie, dokumentácia k programom a pod.

Hardware - technické vybavenie počítača (procesor, pamäť, disketa, pevný disk a pod.).

Vírusy vedia poškodzovať software, ale (zatiaľ) nepoškdzujú hardware.

Klasifikácia počítačových infiltrácií

1. Infiltrácie jednorazovej akcie

Sú určené len na jednu akciu na jednom počítači, nemajú schopnosť replikácie (*bomby, špióni, škriatkovia*).

2. Infiltrácie mnohonásobného použitia, bez replikácie

Sú určené len na jednu akciu na väčšom počte počítačov, nemajú schopnosť replikácie (*míny*).

3. Infiltrácie mnohonásobného použitia, s pasívnou replikáciou

Sú určené pre mnohonásobné použitie. Kopírovanie týchto infiltrácií je ponechané na vedomú činnosť ľudí (*chameleóny, trójske kone, nosiče vírusov*).

4. Replikatívne infiltrácie

Vedia vyrábať svoje kópie, preto rozsah ich šírenia je obmedzený len protiakciami ľudí (*vírusy, červíky, zajace*).

Bomby

Programy určené k likvidácii istých údajov, súborov, programov na vybranom mieste. Pôsobia okamžite. Bomba sa skladá z rozbušky, generátora škôd a maskovania a ničenia stôp.

Rozbuška slúži k aktivácii škodlivej činnosti. Príkladom rozbušky je malý program, ktorý kontroluje, či sa je tvorca hlási, napr. heslom Ak sa neohlási mesiac (bol prepustený), spúšťa sa rozbuška. Alebo rozbuška čaká na špeciálne heslo od tvorcu. Ten môže byť na druhom konci sveta, vyšle po sieti do svojho počítača heslo a rozbuška sa aktivuje.

Hovorí sa, že pri operácii Púštna búrka vo vojne USA s Irakom bol takto vyradený počítačový systém Iraku. Iné rozbušky môžu byť aktivované časovo (spúšťa sa v istý deň či hodinu) alebo logicky (aktivuje sa na základe istého stavu prostredia - zaplnenosť diskov a pod.).

Generátor škôd má na starosti vykonanie škodlivej činnosti.

Maskovanie a ničenie škôd - mnohé bomby majú prostriedky sebalikvidácie. Ak sa zdá, že niekto začína jej existenciu tušiť, zlikviduje sa.

Obrana proti bombám je veľmi ťažká, pretože ich vyrábajú zvyčajne systémoví programátori, ktorí dokonale poznajú počítačový systém organizácie. Pomôže jedine niekoľko vzájomne izolovaných skupín, ktoré sa vzájomne kontrolujú. Inou možnosťou je predchádzať vniku týchto bômb. Poskytne sa zaujímavá práca programátorom, dostatočné oceňovanie, prípadné prepúšťanie sa deje náhle, aby programátor nevytvoril protiakciu.

Míny

Sú zamerané len na poškodenie, znefunkčnenie, likvidáciu svojho nosiča. Používajú sa napríklad v demoverziách, ktoré sú úplne funkčné, ale len po istú dobu. Potom sa program napríklad vymaže alebo prestane spracovávať údaje. Míny sa používajú aj v programoch, ktoré sú prenajímané inej organizácii a tá za ich použitie platí. Ak sa platba včas nevykoná, nedostane organizácia správne heslo a bez neho sa program zlikviduje.

Škriatkovia

Sú to programy vytvorené jedným z užívateľov počítača. Ich cieľom je pobaviť tvorcu, prípadne ostatných užívateľov (tých skôr vystrašiť, prekvapiť). Napríklad niekomu do AUTOEXEC.BAT dá výpis textu "FOUND DISK KILLER VIRUS" hneď po prebehnutí antivírusového programu. Alebo sa vytvorí malý pamäťovo rezidentný program, ktorý občas spôsobí neplechu (na chvíľu zablokuje klávesnicu, napíše neslušné slovo, vygeneruje podivný zvuk). Škriatok spôsobuje škodu len nepriamo (napr. vystrašený užívateľ preformátuje pevný disk, stratí dôveru k počítaču).

Trójske kone

Názov má pôvod v gréckej mytológii. Starovekí Gréci sa pokúšali dobyť mesto Tróju. Keďže obrancovia Tróje boli veľmi šikovní, napriek veľkej snahe Gréci neuspeli. Po jednej krvavej bitke naoko porazené grécke vojská opustili okolie Tróje. Pred bránami mesta nechali veľkého dreveného koňa. Trójania si mysleli, že je to grécky náznak ponúkaného mieru. Otvorili brány a vtiahli koňa do mesta. Nastala veľká oslava víťazstva nad Grékmi. Keď prišla noc a spánok opantal vínom opojených Trójanov, z koňa vyliezli ukrytí grécki vojaci. Dali znamenie skrytým vojskám a otvorili brány do mesta. Gréci vnikli do Tróje, obrancov pobili a mesto zrovnali so zemou.

Preto ako trójske kone označujeme programy, ktoré sa tvária ako milé, zaujímavé, užitočné. V sebe ale obsahujú procedúru pre spôsobenie škôd užívateľom.

Možné spôsoby prenosu na počítač:

- rozposlanie poštou: trójsky kôň AIDS bol rozposlaný na 20 000 adries. Problém je v tom, že pri veľkom počte zasielaných kópií sa dá vypátrať, kto diskety rozposiela.
- inštalovanie z BBS (Bulletin Board System - počítač prístupný užívateľom prostredníctvom modemov) je najčastejší spôsob spustenia šírenia trójskeho koňa,
- ponuka na výstave - cez demo programy ponúkané na výstavách,
- nahranie priamo na počítač - počítače v školách.

Prečo je trójsky kôň nebezpečný?

1. Je ťažko rozoznateľný až do spôsobenia škody.

2. Je dosť veľký na to, aby mal v sebe skryté rafinované metódy škodenia.

Ochrana pred trójskymi koňmi

100% ochrana neexistuje. Ale dostatočne spoľahlivou ochranou je:

a) používať len software renomovaných firiem nakupovaný u serióznych predajcov,

b) napoužívať software z neznámych zdrojov,

c) mať všetky dôležité údaje aj oblasti disku zálohované,

d) používať hardwarovú ochranu disku,

e) používať antivírusový program (scanner), ktorý vyhľadáva aj trójske kone,

f) používať checksummer aplikovaný na všetky súbory,

g) používať monitorovacie a blokovacie prostriedky.

Najznámejší trójsky kôň **AIDS***:*

V decembri 1989 jedna panamská firma rozoslala tisícom užívateľov disketu s informáciou o chorobe AIDS a obslužným programom. Adresy si vybrala z distribučného zoznamu časopisu "PC Business World". Disketa prišla s licenčným ujednaním, kde je užívateľ upozornený, aby poslal 189 dolárov firme PC Cyborg Corporation, pretože program má mechanizmy, aby zistil, kto je neplatič a ten bude postihnutý. Kto to čítal pozorne, mohol tušiť, že s týmto softwarom budú nejaké problémy. Ale ujednanie skoro nikto nečítal.

Čo si autor programu vymyslel? Po inštalácii sa vytvorili skryté podadresáre s neviditeľnými názvami skrytých súborov. Súbor AUTOEXEC.BAT tiež skryl a tento volal dávkový súbor AUTO.BAT, ktorý mal užívateľ používať. V súbore AUTOEXEC.BAT bola poznámka REM, ktorá sa nevykonáva. Ale za REM bol neviditeľný znak, takže REM s touto

koncovkou nebola poznámka, ale vyvolanie programu so spomínaným menom. Program REM počítal do 90 a po 90 spusteniach súboru AUTOEXEC.BAT sa aktivovala škodlivá činnosť.

Tá spočívala v zakódovaní mien všetkých súborov na disku a zmenu atribútu súborov na "hidden" - skrytý. Pri štarte počítača sa spustil emulátor DOSu, ktorý nechcel vykonávať skoro žiadnu činnosť. Trójsky kôň sa aktivoval v stovkách organizácií.

Tvorcom tohto trójskeho koňa bol Dr. Joseph Lewis Popp, proti ktorému bol začatý súdny proces 11. 11. 1991 v Londýne. Súd ho prepustil, keďže trpí psychickými poruchami a v súčasnosti sa lieči. Psychické poruchy vraj vznikli v dôsledku informácií o škode, ktorú disketa s trójskym koňom ľuďom spôsobila. Ale asi ani predtým to nebolo s ním v poriadku. Bol fascinovaný biologickým vírusom HIV spôsobujúcim AIDS. Mal v pláne rozposlať ďalšie 2 milióny zamorených diskiet, ak by na to získal financie. Súd skonštatoval, že rozoslanie týchto diskiet spôsobilo veľké škody najmä výskumu AIDS (jedna inštitúcia v Taliansku stratila 10 rokov výskumu). Niekoľko správcov PC prišlo o zamestnanie. Podľa odhadu inšpektora J. Austena diskety boli použité na 1 000 počítačoch. Právnym problémom bolo, že sprievodný text upozorňoval na možné poškodenie, aj keď bol písaný malým písmom a bol veľmi nenápadný.

Nosiče vírusov

Príbuzní trójskych koní. Ich úlohou je preniesť na počítač vírus tak, aby neboli zaregistrované scannerom (sú v zakódovanom tvare). Po spustení nosiča sa odkóduje vírus a nosič ho nainštaluje do pamäte. Preto dobré scannery rozpoznávajú aj nosiče vírusov.

Chameleóny

Programy, ktoré napodobňujú správanie sa iných programov (napr. napodobňujú antivírusové programy). Ak chce niekto získať heslá iných užívateľov, napíše program, ktorý simuluje prihlasovanie sa do systému. Tento program nechá bežať na svojom pracovisku. Užívateľ, ktorý príde na toto pracovisko, ide sa prihlásiť. Chameleón prijme heslo, uloží ho na bezpečné miesto a potom vyvolá skutočné prihlasovanie sa do systému spolu s hlásením nejakej systémovej chyby.

Špióni

Sú programy, ktoré majú za úlohu preniknúť do počítačového systému, získať isté informácie, odoslať ich tvorcovi špióna a potom nenápadne zmiznúť. Špióni sa zvyčajne snažia preniknúť do veľkých databánk a čerpať z nich dôverné informácie.

Červy

Programy, ktoré putujú po počítačových sieťach, prechádzajú z počítača do počítača. Zvyčajne nespôsobujú žiadne škody. Dobre naprogramované červy sa rozmnožujú len obmedzene, aby príliš nezahltili sieť. Občas vytvárajú svoje kópie - články, aby nezanikli.

Najznámejší červ je *"Veľký internetovský červ"*, ktorý vytvoril 23 ročný študent Cornellovej univerzity Robert T. Morris. Jeho otec pracoval v National Computer Security Center a zaoberal sa vezpečnosťou počítačových sietí. Syn využil otcove poznatky o slabých miestach v zabezpečení unixovských sietí a prakticky dokázal, že siete sú napadnuteľné. Tento červ napadol vyše 6000 unixovských počítačov siete Internet (tvorcovi sa vymklo množenie červa). Blokoval sieť vyše 36 hodín. Priame a nepriame škody dosiahli skoro 10 mil. dolárov.

Zajace

Sú to programy podobné červom. Divoko sa množia zvyčajne na jednom počítači a zakrátko zahltia disk, pamäť, komunikačné linky v sieti.

Vírusy

Parazitné programy, ktoré sú schopné vytvárať svoje vlastné kópie parazitujúce zas na ďalších programoch.

Parazitizmus má veľa podôb:

1. Pripojenie sa ku programom.

Takto sa správa súborový vírus. Ak sa spustí napadnutý program, vírus sa zaktivuje. Nájde si nenapadnutý program, do neho vloží svoju kópiu.

2. Nahradenie programu na danom mieste.

Tento spôsob používajú boot a partičné vírusy. Operačný systém po štarte systému vždy skáče na zavádzací program v partičnom a boot sektore pevného disku alebo na zavádzací program v boot sektore diskety. Ak sa tam umiestni vírusový program, automaticky sa vykoná.

3. Nahradenie smerníka na počiatočný cluster programu.

4. Využitie mena programu.

Prepisujúce vírusy sa vložia na miesto napadnutého programu a ponechajú si jeho meno. Užívateľ sa domnieva, že spúšťa svoj program a nie vírus.

Podporné prostriedky na tvorbu infiltrácií

a) *Virus Construction Set*

Jeden čas bol v Nemecku ponúkaný ako shareware za 20 DM (platiť sa malo firme RED CROSS) program "Virus Construction Set", ktorý umožňoval užívateľovi, aby si sám navrhol a vytvoril vírus podľa svojich predstáv. Aj keď konštruktér vírusov bol pomerne rýchlo stiahnutý z trhu, na jeho základe vzniklo niekoľko nových vírusov.

b) *Falošné údaj*

Infiltráciou môže byť aj textový súbor s poplašnou správou a výzvou poslať správu ďalej.

c) *Kooperatívne efekty*

Možno si spomínate na krach na londýnskej burze. V značnej miere sa na ňom podieľali počítače. Na počítačoch mnohých maklérov bežal software, ktorý vyhodnocoval aktuálnu situáciu a navrhoval, prípadne automaticky vykonával niektoré burzovné operácie (nákup a predaj akcií). Na týchto počítačoch bežali rovnaké programy, ktoré medzi sebou interagovali. V ich činnosti došlo k spriahnutiu (pri poklese akcií začal jeden program ich odpredaj, ďalšie na základe tejto činnosti ešte zintenzívnili odpredaj). Tým vznikol kooperatívny efekt, ktorý nikto nečakal a týmto vyviedli z rovnovážnej situácie celú burzu. Pohyb peňazí, ktorý vtedy prebehol, bol cca. 2 000 miliárd dolárov!!!

V budúcnosti možno očakávať, že spriahnutie masovo nasadzovaných programov pracujúcich v autonómnom režime povedie k vzniku nepredvídaných javov, ktoré budú spôsobovať veľké škody (riadenie energetickej sústavy, telefónna sieť a pod.).

d) *Počítačové hry*

Hra napadne mozgy užívateľov a núti ich, aby si ju skopírovali aj na svoj počítač.

Ako sa dostane vírus do počítača

- diskety, sieťové linky (pri zapojení do siete), telefónna linka (pri použití modemu), výmenné pevné disky, pevné disky, papier (uverejnený zdrojový text vírusu), programátor píšuci vírusy.

Ako zistíme napadnutie počítača vírusom

Hardwarové a softwarové problémy podobné prejavom vírusu:

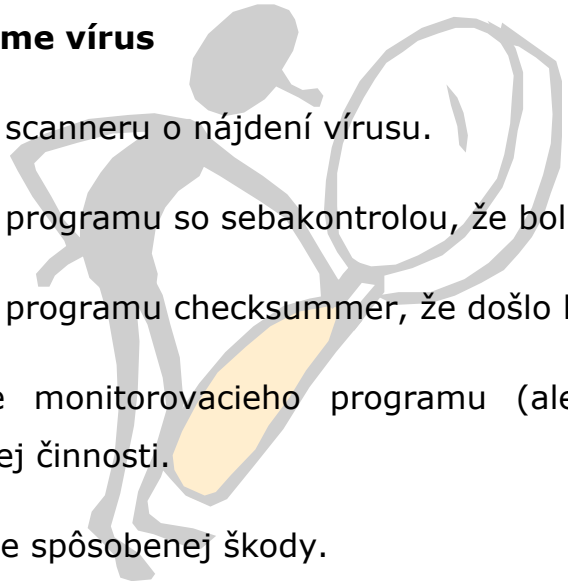
Nekvalitná disketa - NONAME, údaje nahrané na takýchto disketách nevieme prečítať.

Nesprávne naformátovaná disketa.

Starý pevný disk - životnosť je asi 5 rokov. Po tejto dobe vzrastá riziko nespoľahlivej funkcie disku.

Vybitá CMOS batéria - strata údajov, vtedy sa počítač nevie nabootovať a hlási chybu.

Ako objavíme vírus



1. Hlásenie scanneru o nájdení vírusu.
2. Hlásenie programu so sebakontrolou, že bol infikovaný.
3. Hlásenie programu checksummer, že došlo k modifikácii súborov.
4. Hlásenie monitorovacieho programu (alebo hardwarovej karty) o podozrivej činnosti.
5. Objavenie spôsobenej škody.

6. Viditeľné prejavy vírusov. (zvukové prejavy - Yankee Doodle zahrá o 17.00 hod. melódiu, modifikácia obrazovky - začnú vám padať pri práci v textovom režime písmenka (vírus Cascade), alebo bezdôvodne behá po obrazovke akási loptička (vírus Ping-Pong), nečakané hlásenia, rast veľkosti súborov, zmena volume label (názvu disku))

7. Skryté prejavy vírusov.

Škody spôsobené vírusmi

Na základe prieskumu špičkového časopisu Byte 53% čitateľov potvrdilo, že v ich organizácii vznikla strata údajov v dôsledku napadnutia vírusmi. Priemerná veľkosť škody bola 14 000 USD.

Najčastejšie vírusy: Stoned, Jerusalem, Joshi.

Najčastejší zdroj infekcie: diskety z domácich počítačov (43%), programy z BBC (7%)

Rozsah škôd: 31% do 2 000 USD, 29% od 2000 do 10 000 USD, 33% od 10 000 do 100 000 USD, 7% nad 100 000 USD.

Podľa domácich prieskumov bolo napadnutých vírusmi vyše 70% organizácií v našej republike (školy, firmy, štátne inštitúcie).

Škody: poškodenie údajových súborov; poškodenie programov; nesprávna činnosť bežiacich programov; spomaľovanie behu počítača; teoreticky poškodenie hardwaru; poškodenie zákazníkov, ktorí sa nakazili od vašej firmy; priame finančné straty v dôsledku práce s chybnými údajmi; poškodenie psychiky užívateľa; poškodenie mena firmy; náklady na odstránenie vírusu; náklady na kúpu antivírusových programov;

náklady na školenie pracovníkov; straty spôsobené behom antivírusových programov (najväčšia škody - odhadom 5 000 000 000 USD ročne).

Poškodenie hardwaru:

(Je to zatiaľ teoretická možnosť.)

a) prepáliť monitor neustálym prepínaním textového a grafického modu,

b) poškodiť disketovú jednotku posielaním hlavičky na neexistujúcu stopu,

c) poškodiť pevný disk parkovaním hlavičky na nesprávnom mieste,

d) poškodiť periférne zariadenia.

Poškodenie užívateľa

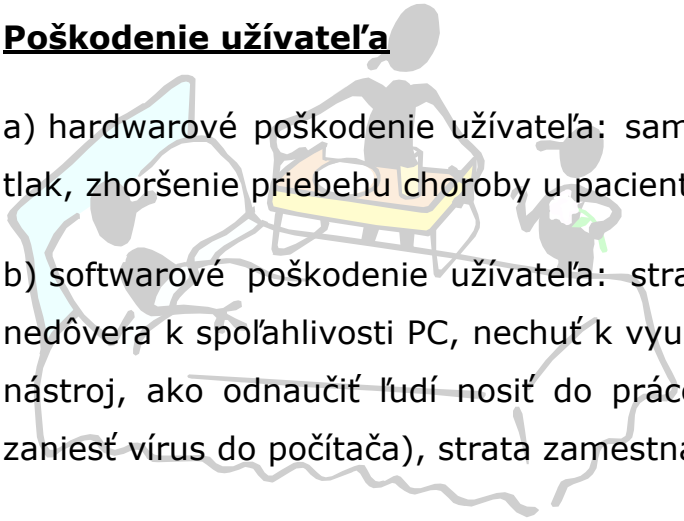
a) hardwarové poškodenie užívateľa: samovražda, infarkt, zvýšený krvný tlak, zhoršenie priebehu choroby u pacienta, migréna;

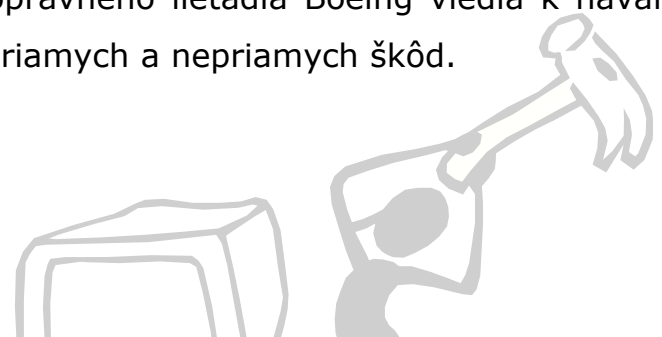
b) softwarové poškodenie užívateľa: strata chuti do života a depresie, nedôvera k spoľahlivosti PC, nechuť k využívaniu PC, strata prémií (účinný nástroj, ako odnaučiť ľudí nosiť do práce nelegálny software a takto si zaniesť vírus do počítača), strata zamestnania.

Niektoré známe veľké škody spôsobené softwarom:

a) Nesprávne ožiarenie pacienta v Kanade chybou programu. Poisťovňa platila skoro 1 mil. dolárov.

b) Chybná činnosť autopilota dopravného lietadla Boeing viedla k havárii lietadla, cca. 20 mil. dolárov priamych a nepriamych škôd.





c) Zničenie jedného z Apoll krátko po štarte, vyše 50 mil. dolárov škody.

d) Veľký internetovský červ, blokoval vyše 6000 počítačových uzlov, cca. 100 mil. dolárov strát.

e) Likvidácia torpédoborca Sheffield v boji o Malvíny chybným vyhodnotením nalietávajúcej rakety Exocet, cca. 300 mil. libier škody.

f) Niekoľko falošných poplachov strategických síl USA, vyše 100 mil. dolárov nákladov.

g) Krach na londýnskej burze s výraznou zásluhov špeciálnych burzových programov. Vyše 3 000 mil. dolárov priamych strát.

Najviac vírusov pochádza z Bulharska (vyše 50). Patrí tu Yankee Doodle, Dark Avenger atď. Potom nasledujú USA.

Prvý vírus pre PC bol asi "Brain", objavil sa v roku 1986 v Pakistane. Je to boot vírus, napáda len 360 kB diskety. Vraj ho napísali dvaja bratia Basit a Amjads z mesta Lahore. Poskytli ho každému cudzincovi, ktorý v ich obchode nakupoval nelegálne skopírovaný software.

Pohľad do budúcnosti

V súčasnosti pribúda mesačne vyše 120 vírusov. Pribúda aj tvorcov vírusov. Relatívne najviac vírusov pochádza z východnej Európy. Jednou z príčin je aj absencia zákonov, pomocou ktorých by bolo možné trestne stíhať tvorcov vírusov. Zvyčajne je to možné len vtedy, ak vírus spôsobí škodu veľkého rozsahu.

Možno očakávať vírusy, ktoré budú aktívne bojovať s antivírusovými programami. Budú napr. vymazávať antivírusový program, alebo modifikovať databanku sekvencií, upravovať tabuľku kontrolných súčtov pre súbory.

Vírusy budú používať nové techniky pre svoje skrývanie sa. Nepríjemné bude samoodstraňovanie sa vírusov zo zdrojov nákazy, aby sa nedalo dopátrať, odkiaľ vírus prišiel. Iné vírusy sa budú periodicky inštalovať a odinštalovať, meniť svoj spôsob správania sa, napodobňovať iný vírus.

Vzdialená budúcnosť

1. *Inteligentné vírusy* - istú mieru inteligencie budú využívať na maskovanie svojej činnosti, boj proti antivírusovým programom, pôsobenie škôd. Pomocou neurónovej siete získajú vírusy schopnosť učiť sa a aktívne spracovávať informácie o vonkajšom prostredí.

2. *Vírusy napádajúce zariadenia* - mimoriadne nebezpečné budú napadnuté roboty (napr. nútia robot kradnúť).

3. *Vírusy napádajúce ľudí* - ak vírus napadne počítač riadiaci syntetizátor génov, vloží sekvenciu do systetizovaného génu. Ak sa gén vloží do ľudských buniek, po čase sa aktivuje vírus. Zatiaľ komunikujú osobné počítače s ľuďmi najmä prostredníctvom písaného textu. Začína sa aj hlasová komunikácia. V budúcnosti bude spojenie medzi ľudským mozgom a počítačom asi priame, napojením na nervový systém človeka. Vírus napádajúci počítač bude mať možnosť priamo ovplyvňovať ľudský mozog.

V súčasnosti sa rozširuje počet "osobných" medicínskych zariadení pomáhajúcich chorým (napr. kardiostimulátor, dialyzačné zariadenie, automatické dávkovače inzulínu, zariadenia na pomoc nepočujúcim, či slepcom). Tieto zariadenia budú v budúcnosti riadené počítačmi, ktoré môžu byť napadnuté vírusmi. Účinok takéhoto vírusu sa priamo prejaví na zdraví človeka.

Vojenské aplikácie - nasadzovanie infiltrácií do riadiacich systémov velenia protivníka možno prebieha už aj teraz (hovorí sa, že niečo také bolo použité vo vojne v Perzskom zálive). Schopný vírus môže na niekoľko hodín vyradiť stovky vojenských počítačov (ako sa to stalo v roku 1988 v USA) a výrazným spôsobom ovplyvniť istú fázu vojenskej operácie.

Terorizmus - chemická výroba, jadrové elektrárne, riadenie strategických zbraní.

Hviezdne baktérie - mohli by spôsobovať zásahy v galaktickom meradle (ich vzniku nebráni žiadny fyzikálny zákon). Išlo by o systémy so schopnosťou autoreprodukcie a syntézou prvkov z vodíka (v malom meradle vieme syntetizovať prvky už teraz). Tieto systémy by čerpali vodík z Jupitera, reprodukovali sa a mohli by byť nástrojmi planetárneho inžinierstva. Patologické formy by boli schopné napádať planéty typu Jupitera, prípadne poškodzovať či likvidovať hviezdy. Šírili by sa po galaxii od jednej napadnutej hviezdy k druhej. Podľa odhadu je ľudstvo schopné teoreticky vytvoriť takéto systémy do sto rokov.

História

CREEPER - v roku 1970 vytvoril Bob Thomas demnštračného červa v sieti ARPAnet. Tento červ vypisoval na počítačoch "I´m the creeper ... catch me if you can!". Potom zostrojil červa REAPER, ktorý mal za úlohu likvidovať červa CREEPER.

Prvý trójsky kôň EGABTR sľuboval lepšiu grafiku a bol zadarmo. Po spustení vymazal všetky súbory na pevnom disku a ukončil to správou: "Arf! Arf! Gotcha!"

Prvý PC vírus - BRAIN.

Prvý odsúdený za počítačovú infiltráciu (1988) - v septembri 1988 v Texase sa začal súdny proces proti D. G. Burlesonovi, ktorý spôsobil softwarovou časovanou bombou škodu firme USPA&IRA Co 21. 9. 11985, dva dni po svojom prepustení. Firma prišla o 168 000 záznamov z databázy. Zaplatil pokutu 12 000 dolárov a dostal 7 rokov väzenia.

Boj s vírusmi

1. Hlavný problém je skoro vždy ľudský faktor (neznalosť, nedodržiavanie opatrení, panika).

2. 100% ochrana pred infiltráciami neexistuje; ide o znižovanie pravdepodobnosti napadnutia počítača na prijateľnú mieru.
3. Naše údaje sú cennejšie ako používané programy, preto sa viac zameráme na ich ochranu.
4. Prevencia je zvyčajne menej nákladná ako likvidácia spôsobených škôd.
5. Hardwarová ochrana je istejšia ako softwarová.
6. Papieru vírusy neublížia (a preto všetko, čo dávame do počítača, hneď aj tlačíme).
7. Základné heslo v boji s vírusmi: "Nedôveruj, preveruj!" Veď vírusy sú občas aj v softwari od serióznych firiem.
8. Do dobrej prevencie sa musí aj niečo investovať (zaškolenie pracovníkov, kúpa antivírusových programov).

Oblasti prevencie

a) Ochrana údajov zálohovaním (na viacerých miestach viac kópií, kontrolovať ich, ...).

b) Obmedziť budúci vstup vírusov do počítačov firmy, kšoly, inštitúcie.

c) Obmedziť šírenie sa vírusu v prípade napadnutia.

d) Minimalizovať škody na napadnutých počítačoch.

e) Rýchla likvidácia vírusu.

- osveta, hmotná zodpovednosť pracovníkov, predbežné opatrenia (čistá boot DOS disketa, údaje o disku - CMOS, boot a partičný sektor), vstupná kontrola.

Ako sa prejaví známy vírus:

1. Hlásenie antivírusového programu.

2. Vznik škody k istému dátumu (napr. 6. marca Michelangelo).

3. Niekedy spoznáme vírus podľa akcie, ktorú vykonáva.

Sú dve možnosti po nájdení vírusu:

a) vírus ešte neškodil

b) vírus už vykonal škodlivú akciu

Čo sa bežne robí po zistení vírusu?

1. Užívateľ uvidí hlásenie scanneru o víruse.

2. Zadá antivírusovému programu príkaz k vyliečeniu súborov.

Skúsenejší užívateľ pokračuje ďalej:

3. Resetuje, alebo vypne počítač.

4. Ešte raz skontroluje pevný disk scannerom.

5. Skontroluje a vylieči všetky diskety.

Čo robiť po zistení známeho vírusu?

1. Ak zistíme vírus počas akcie, vypneme počítač (výnimka - Disk Killer a Casino).

2. Ak nám vírus zahlásil scanner spúšťaný z pevného disku, tiež vypneme počítač - niektoré antivírusové programy môžu pri kontrole prenášať vírus.

3. Ak vieme meno vírusu, snažíme sa o ňom zistiť čo najviac - o aký vírus ide a aké škody spôsobuje.

4. Informujeme o nákaze ľudí, s ktorými si vymieňame diskety. Potom sa ukľudníme. Ak patríme k začiatočníkom, je vhodné poradiť sa s odborníkom. Ak nie je nablízku a čas súri, musíme si poradiť sami.

5. Bootujeme počítač z čistej DOS diskety.

6. Potom z diskety spustíme antivírusový program. Jeden z napadnutých súborov si skopírujeme na disketu, označíme ju nápisom "Pozor, vírus!" a uložíme na bezpečné miesto pre potreby odborníka.

7. Obnovíme boot sektor.

8. Ak ide o partičný vírus, zálohujeme si najprv všetky údaje.

9. Kontrola všetkých diskiet.

10. Analýza škôd.

11. CMOS, boot a partičný sektor máme uschovaný na záchrannej diskete, ktorá je čistá, bootovateľná, obsahuje aspoň programy CHKDSK, FORMAT, FDISK, SYS. Údaje sú zálohované aspoň dvakrát, uložené na dvoch fyzických miestach.

Napadnutie neznámym vírusom

1. Zistiť, či ide skutočne o vírus.

2. Nájsť spôsob, ako vírus rozpoznať a zlikvidovať.

3. Zistiť spôsobené škody.

Podozrenie:

1. Checksummer.

2. Monitorovacie a blokovacie programy.

3. Počítač nemá prístup na pevný disk.

4. Počítač sa správa neštandardne:

   a) Pevný disk pracuje vtedy, keď nemá.

   b) Na obrazovke sa objavujú podivné hlásenia.

   c) Nejaký program, ktorý bežal, hlási zrazu nedostatok pamäti.

   d) Občas sa počítač zablokuje.

   e) Niekedy sa ozývajú melódie.

   f) Programy pri práci sa nesprávajú ako obyčajne.

   g) Naše údajové súbory sú poškodené.

Klasifikácia bacilonosičov

- rizikové skupiny, ktoré sú prenášačmi počítačových vírusov.

Hráč hier

Hry sú pre neho droga, potrebuje ich stály prísun. Keďže nemá na nich peniaze, zháňa si nelegálne kópie, ktoré zvyčajne hrá z pevného disku kamarátovho počítača, ale nie z inštalačných diskiet. Občas si potrebuje zahrať hru aj v práci (najmä ak nemá svoj počítač). Nainštaluje si hry na pevný disk alebo ak má prísnejšieho šéfa, tak si ich spúšťa z diskety. Takto môže nakaziť počítač. Osobitne nebezpečným je ten hráč, ktorý behá s novou hrou po organizácii a láka ostatných užívateľov, aby si hru nahrali (svojho času sa to dialo veľmi často s hrou Tetris). Takto môže v krátkej dobe zamoriť vírusom celú organizáciu. Ešte nebezpečnejším javom je skupina hráčov, ktorí medzi sebou súťažia a neustále zháňajú a vymieňajú nové počítačové hry.

Zberateľ programov

Mnoho ľudí zbiera známky, motýle, pivné tácky. Nieto divu, že existuje aj mnoho zberateľov programov. Tí sú dvoch druhov:

a) Pre istotu si program ktorý uvidia, skopírujú. Veď čo keď sa v budúcnosti zíde.

b) Túžia mať ihneď novú verziu programu, aby sa s ním mohli oboznámiť.

Zberateľ vírusov

Aspoň jeden zberateľ vírusov sa isto nájde v každej väčšej organizácii. Vlastnenie vírusu (niečo nebezpečného, škodlivého) je pre niektorých ľudí veľmi lákavé, má to príchuť zakázaného ovocia. Zberateľ vírusov je skutočný bacilonosič. Vírusy zvykne mať na svojom počítači a aj na disketách. Občas sa mu môže stať, že si spletie disketu a aktivuje vírus. Alebo niekto iný na jeho počítači spustí napadnutý program. Alebo sa na niekoho nahnevá a z pomsty mu nasadí vírus. Ako nájdeme takéhoto zberateľa? Oznámime na verejnosti, že na istom počítači sa našiel nový vírus a sledujeme, kto k počítaču pobeží a čo bude robiť.

Technická skupina

Vo väčších organizáciách (firmách, školách) má na starosti údržbu, prípadne aj menšie opravy technická skupina. Pre kontrolu iných počítačov používajú technici vlastný software. Často sú diskety nedisciplinovaných technikov s programami nechránené proti zápisu. Na takúto disketu sa dostane vírus a ten sa šíri po ďalších kontrolovaných počítačoch.

Administratívne pracovníčky v strednom veku s deťmi

Tieto pracovníčky prenášajú zvyčajne spracované údajové súbory na disketách. Občas si ich potomok chce zahrať hru a nemá kde. Hry si zoženie od kamarátov, mama poskytne počítač. O týždeň nesie naklepané údaje na diskete šéfovi, často s boot vírusom.

Učitelia

Pracujú v počítačových učebniach, kde je veľké riziko nákazy, keďže je tam veľký tok diskiet. Svoje programy poskytujú študentom, berú programy od študentov.

Študenti

Pracujú v počítačových miestnostiach, kde je veľké riziko nákazy. Vytvárajú svoje vlastné programy, na ktoré sa môže pripojiť vírus. Nemajú trvalý partnerský vzťah s jedným počítačom, preto flirtujú s mnohými. Nosia kopu diskiet s programami z pochybných zdrojov, nemajú peniaze na legálny software.

Rizikové miesta

Počítačové miestnosti

V počítačových miestnostiach sa vystrieda veľké množstvo ľudí. Každý nosí svoje diskety, kopíruje si na disky a z diskov programy. Antivírusové programy (ak sú) nie sú zvyčajne najnovšie.

Výstavy

Na počítačových výstavách mnohé firmy ponúkajú demo verzie svojich programov. Ak je náhodou počítač nakazený a diskety sa pripravujú na ňom, môže dôjsť k masovej nákaze (najmä ak je program aj s disketou zdarma).

Konferencie

Každoročne sa koná mnoho odborných konferencií. Na väčšine sa predvádza a vymieňa nejaký software. Pokiaľ to nie sú ľudia od počítačov, na vírusy si príliš nedávajú pozor. Stačí, že jeden účastník pri predvádzaní zamorí počítač, potom si každý vezme nakazenú kópiu. Doma si od neho skopírujú program kolegovia a je z toho nepekná masová nákaza.

Antivírusové centrum v organizácii

V pracovných organizáciách, kde sa používa veľa počítačov sa stáva ochrana údajov vážnym problémom. Je vhodné vyčleniť niekoľkých pracovníko, ktorí by sa starali o ochranu údajov a bojovali s počítačovými vírusmi.

Potrebné vedomosti:

1. Rozumieť problematike počítačových vírusov, pravidelne sledovať novinky v odbornej literatúre.
2. Mať prehľad o bežných vírusoch.
3. Poznať na trhu dostupný antivírusový software.
4. Vedieť plne využívať antivírusový program, používaný v pracovnej organizácii.
5. Vedieť pracovať s pomocnými programami - Norton Utilities, CheckIt, Disk Manager a pod.
6. Mať dostatočne hlboké vedomosti o DOSe a BIOSe, o štruktrúre údajov na disku.
7. Je žiadúce, aby aspoň jeden zo skupiny vedel analyzovať a disassemblovať vírusy.
8. Aspoň jeden zo skupiny by mal mať organizačné schopnosti a vedieť dobre komunikovať s ľuďmi.

Materiálno-technické zabezpečenie (MTZ)

Čo by v antivírusovom centre veľkej firmy malo byť:

1. Vlastná telefónna linka, aby sa každý pracovník mohol dovolať priamo do centra. Každý pracovník firmy by mal mať pri telefóne číslo antivírusového centra.
2. Vyhradený počítač na experimenty s vírusmi.
3. Špičkový antivírusový program s mesačnou aktualizáciou.
4. Modem pre spojenie s BBS antivírusových firiem a výskumníkmi po celom svete.
5. Časopis o vírusoch - Virus News International, alebo Virus Bulletin.
6. Odborná literatúra - knihy o vírusoch, BIOSe, DOSe, pevných diskoch.
7. Pomocný software - Norton Utilities, CheckIt, Disk Manager a pod.
8. Prostriedky pre analýzu vírusov - disassembler, debugger, komentovaný BIOS a DOS atď.
9. MS DOS vo všetkých verziách používaných vo firme.
10. Dostatok diskiet.
11. Vhodné je mať záchranné diskety zo všetkých počítačov organizácie.
12. Dôležitou vecou je spracovaný plán jednotlivých typov akcií - známy vírus, neznámy vírus, poškodené údaje.
13. Ďalšou dôležitou vecou je zoznam s umiestnením a užívateľov počítačov organizácie (pri likvidácii masovej nákazy).
14. Ak ide o veľkú firmu, je potrebný pre kontrolu diskiet tzv. autoloader - berie si diskety zo zásobníka a automaticky prevádza ich kontrolu.

Aktivity centra

a) Spoznať realitu

Toto znamená prejsť všetky počítače, skontrolovať ich špičkovým antivírusovým programom, zistiť nakoľko sa používa nelegálny software, aké sú vedomosti užívateľov.

b) Navrhnúť ochranné opatrenia

To zvyčajne spočíva vo výbere antivírusového programu pre multilicenciu a návrh stratégie používania daného antivírusového programu, realizácie aktualizácie.

c) Inštalácia antivírusového programu

Ak je počítačov veľa, je vhodné zvolať užívateľov, zaškoliť ich a potom im rozdať program na inštaláciu.

d) Zaškolenie

Zaškolenie užívateľov je dôležitá vec. Ináč budú obchádzať používanie antivírusových programov. Školenie má dve časti:

- všeobecná informácia o vírusoch,

- práca s daným antivírusovým programom.

Je vhodné rozdeliť užívateľov na dve skupiny - úplní laici a skúsení užívatelia s istými vedomosťami o počítačoch.

e) Občasná kontrola využívania antivírusového programu

Je vhodné po čase sa pozrieť, ako sa reálne antivírusový program využíva, spýtať sa na názory užívateľov, v čom vidia problémy. Dôležité je skontrolovať, či je ku každému počítaču záchranná disketa.

f) Distribúcia aktualizovaného scanneru

Aspoň raz za štvrťrok sa aktualizuje scanner. Vtedy potrebujeme zabezpečiť jeho distribúciu na všetky počítače.

Epidémie

Likvidácia veľkej epidémie je nepríjemná vec. Predstavme si firmu s 300 počítačmi, ku každému počítaču je 50 diskiet. Celkovo je to 15 000 diskiet. Na každý počítač potrebujeme 15 až 60 minút (príchod, zapnutie, kontrola, likvidácia vírusu, kontrola, odchod). Na disketu potrebujeme aspoň minútu bez autoloaderu. Čiže clekovo ide aspoň o 20000 minút práce, t. j. vyše 300 hodín. Ak je denný výkon 12 hodín a chceme to mať za víkend, do akcie musíme nasadiť aspoň 12 ľudí.

Zlozvyky užívateľov

Podceňovanie nebezpečenstva vírusov

Toto je najrozšírenejší zlozvyk. Je to rovnaké, ako v prípade AIDSu: "Mne sa to nemôže stať!". Našťastie v prípade napadnutia počítačovým vírusom nejde o náš život. Podceňovanie časť vychádza z nevedomosti. Preto je vhodné užívateľom vysvetliť, v čom spočíva nebezpečenstvo vírusov.

Preceňovanie nebezpečenstva vírusov

Existujú užívatelia, ktorí sa priam panicky boja vírusov. Ak sa na ich počítači objaví vírus, hneď všetko formátujú. Takého užívateľa spoznáme podľa toho, že nám nedovolí na svojom počítači prezrieť si obsah diskety s tvrdením, že sa môže do počítača zaniesť vírus. Vyplašený užívateľ vie narobiť toľko škody, ako nebezpečný vírus. Ak dôjde k masovej epidémii v organizácii, dôležité je panikárov izolovať, aby sa panika nerozšírila na celú firmu (hrozba davových efektov).

Preceňovanie vlastných schopností

Toto sa objavuje u užívateľov, ktorí už dlhšie pracujú s počítačom a myslia si, že už sú experti na počítače. Podarilo sa im pár krát odstrániť vírus Yankee Doodle (neškodný), takže si veria. Uvidia akýsi vírus Stoned, idú ho odstrániť a zrazu je disk neprístupný. Bootujú z pevného disku, nie z čistej DOS diskety. Ručne zasahujú do FATu, partičného sektoru bez predbežného zálohovanie obsahu pevného disku. Alebo odstránia vírus a vyhlásia: všetko je v poriadku. Pritom zabudnú na poškodené údajové súbory. Alebo hneď formátujú pevný disk a diskety. Ak niečo pobabrú, zvalia to na vírus a povedia, že nič viac sa nedalo urobiť.

Starý scanner

Mnoho užívateľov vie, že treba používať antivírusový program. Preto si takýto program zoženú, alebo kúpia. Pravidelne kontrolujú všetky diskety a jedného dňa je pevný disk neprístupný. Ani ich nenapadne, že to mohol spôsobiť víru. Veď používajú antivírusový program!

Mesačne pribúda vyše 100 vírusov. Ak neaktualizujeme scanner, po čase nás napadne vírus, ktorý je pre scanner neznámy, Hlásenie "Viruses

not found" neznamená, že na disku niet vírusov, ale len to, že scanner nič nenašiel.

Diskety zabudnuté v mechanike

Ako vieme, boot a partičné vírusy sa dostanú na náš počítač, len ak sa z napadnutej diskety pokúšame bootovať. Ak zabudneme disketu v mechanike, pri resete, výpadku prúdu, zrútení niektorého programu či zapnutí počítača je pokus o bootovanie z diskety. Preto disketu držíme v mechanike len po dobu potrebnú ku práci so súbormi, alebo ju máme chránenú proti zápisu.

Používanie programov z iných počítačov

Mnoho užívateľov má na pevnom disku programy, ktoré nie sú inštalované z originálnych diskiet. Nemusí ísť o pirátsky software. Môže to byť freeware a shareware, programy, na ktoré má firma multilicenciu. Ak bol program na pevnom disku iného počítača, môže byť napadnutý. Preto si vždy programy inštalujeme z originálnych diskiet.

Bezpečnostné opatrenia

a) Kontrolovať diskety pred spúšťaním programov z nich.

b) Formátovať diskety podľa možnosti na svojom počítači.

c) Aktualizovať scanner.

d) Sledovať zmeny na disku pomocou kontrolných súčtov.

e) Po odvírusovaní vypnúť počítač (alebo resetovat).

f) Pri zistení nákazy informovať tých, ktorí sa mohli od nás nakaziť.

g) Vytvoriť si záchrannú disketu s CMOSom, partičným a boot sektorom disku.

h) Nedovolíme nikomu spustiť svoj program bez kontroly diskety.

i) Neodkladáme zálohovanie údajov.

j) Po likvidácii vírusu sa treba starať aj o údajové súbory, nie oslavovať víťazstvo.

Antivírusové programy

Sú komplexom preventívnych, diagnostických a liečebných prostriedkov. Tieto programy sú pomerne zložité, takže si ich neprogramuje každý sám, ale vyberie si z ponuky na softwarovom trhu.

Ako sa vyberá antivírusový program

Zvyčajne je impulzom k nákupu napadnutie vírusmi s následnou stratou dôležitých údajov.

Ako sa takýto program zvyčajne vyberá?

Snáď najčastejším spôsobom je referencia od kolegov alebo známych. Kolega má istý program, je s ním spokojný, tak si taký istý kúpim aj ja. Snáď ešte pred kúpou skočím k nemu a program otestujem.

Chybou tejto metódy výberu je, že kolega si nemusel vybrať práve najlepšie, prípadne v čase jeho kúpy bolo na trhu najlepšie niečo iné, ako je teraz.

Ďalším častým spôsobom je pozrieť sa na reklamy v počítačových časopisoch. Nájdem reklamu na 2 - 3 programy a vyberiem si ten, ktorý sa mi zdá najvhodnejší.

Chybou tejto metódy výberu je to, že nemusím uvidieť reklamy práve najlepších antivírusových programov. Ukazuje sa, že mnohé firmy ponúkajúce antivírusové programy si vyberú jeden-dva časopisy, kde reklamujú. Ak tieto časopisy neodoberáme, nedozvieme sa o danom programe. Ďalším problémom je, že reklama zvyčajne vyzdvihuje len prednosti programu.

Skúsenejší užívateľ sa orientuje na základe recenzií programu. Prečíta si recenzie o niekoľkých programoch a tak si vyberie.

Tu je problémom, že nie všetky dobré antivírusové programy boli v poslednej dobe recenzované, prípadne recenzia nedostatočne posúdi niektoré dôležité aspekty programov.

Profesionál si vyberá na základe porovnávacích testov veľkého počtu antivírusových programov v odborných časopisoch, kde redakcia aj vyberie najlepšie programy (napr. Best Buy, Editor´ Choice a pod.).

Mimoriadne vhodným miestom pre výber antivírusového programu je nejaká výstava, alebo veľtrh výpočtovej techniky (u nás Invex, v Európe CeBit). Programy si možno pozrieť a otestovať za počítačom, zástupcovia firmy zodpovedia na naše otázky, zvyčajne sa poskytujú zľavy na nákup. Na začiatku prehliadky si v informačnom systéme nájdeme všetky firmy ponúkajúce antivírusové programy, aby sme niečo neprehliadli.

Čo býva v antivírusovom softwari

Ak si kúpime alebo prezeráme nejaký antivírusový software, zistíme, že v ňom je niekoľko programov:

Detekcia vírusov

Keďže vírusy sú uložené na disku v napadnutých súborch, boot sektore, partičnom sektore či inde na disku, ich prítomnosť je zistiteľná. Na tom sú postavené protivírusové programy. Tie zvyčajne používajú dve metódy: vyhľadávanie známych vírusov a sledovanie zmien na disku. Pre každú metódu sa používa osobitný program, často aj v pamäťovo rezidentnej verzii.

Scanner (prehľadávač, polydetektor)

Prítomnosť vírusu sa zvyčajne zisťuje na základe existencie známej vírusovej sekvencie (postupnosti bytov). Tieto sekvencie má antivírusový program uložené v databanke. Program prezerá najprv pamäť, potom partičný a boot sektor a nakoniec vykonateľné súbory. Pritom testuje, či

sa nenájde sekvencia charakteristická pre istý vírus. Takémuto typu programu sa hovorí scanner.

Výhodou tejto metódy zisťovania je, že vieme, aký vírus napadol naše súbory. V literatúre si pozrieme, čo od neho možno očakávať, aké škody nám mohol spôsobiť. Táto metóda je vhodná pri testovaní diskiet, s ktorými pracujeme a najmä diskiet, ktoré niekam posielame.

Nevýhodou je, že sa rozpoznejú len známe vírusy, ktorých sekvencie má antivírusový program v databanke. Nové vírusy bohužiaľ pribúdajú veľmi rýchlo a ak sme 3 mesiace neaktualizovali scanner, je vysoké riziko napadnutia.

Problémom je, ak je vírus enkrypčný - sám seba zákóduje a vždy ináč. Na rozpoznanie takéhoto vírusu nestačí postupnosť (sekvencia) bytov, ale ho treba logicky analyzovať a porovnávať so skupinami vzoriek sekvencií.

Pamäťovo rezidentný scanner

Tento scanner sa nainštaluje do pamäte a kontoluje každý spúšťaný či kopírovaný súbor. Ak zistí v súbore vírusovú sekvenciu, nedovolí bez súhlasu užívateľa vykonanie danej činnosti.

Istou nevýhodou tejto metódy je spomaľovanie niektorých činností (kopírovanie, spúšťanie programov). Nevadí to na rýchlejších počítačoch.

Podstatnou výhodou tohto programu je to, že užívateľ nemôže zabudnúť skontrolovať nejaký program, ako sa to stáva občas užívateľovi používajúcemu bežný scanner. Preto je tento antivírusový program pre bežných užívateľov asi najvhodnejší.

Programy pre kontrolné súčty

Prítomnosť vírusu sa zisťuje na základe zistenia modifikácie napadnuteľných súborov alebo oblastí disku. Ako sa zistí modifikácia? Vytvorí sa tzv. kontrolný súčet súboru (CRC), ten sa uloží do databanky na disku, alebo sa pripojí ku kontrolovanému súboru (nevhodná metóda). Pri kontole sa porovnáva aktuálne zistený súčet so súčtom na disku. Ak sú rozdielne, znamená to, že došlo k modifikácii súboru.

Výhodou tejto metódy je, že sa dá zistiť prítomnosť aj nových, neznámych vírusov. Táto metóda je veľmi vhodná pre ochranu pevných diskov, kde sú inštalované legálne, zaručene zdravé programy.

Nevýhodou tejto metódy je, že pri prvom vytvorení CRC musím mať istotu, že program už nie je napadnutý. Preto ak vkladám do počítača disketu so súbormi, neviem, či tie neboli napadnuté. Aj keď viem, že som napadnutý vírusom, neviem, či je to len neškodný (napr. Yankee Doodle), alebo zabiják (Nomenklatura, Dark Avenger). Ďalším problémom je zistiť, ktorý súbor je nositeľom nákazy.

Existuje jeden sruh vírusov, ktorý uniká mnohým programom pre kontrolné súčty. Sú to satelitné (companion) vírusy. Prečo? Na začiatku si vytvoríme o každom súbore kontrolný súčet a potom ho porovnávame s aktuálnym stavom. Čo ak pribudli nové súbory (satelitné vírusy)? Tie sú mimo kontroly. Niektoré programy umožňujú zistiť, či nepribudli v danom adresári nové súbory bez kontrolných súčtov.

Niektoré programy si okrem kontrolných súčtov uchovávajú aj ďalšie údaje o súbore - dátum a čas, veľkosť, prípadne smerník na prvý cluster.

Pamäťovo rezidentný checksummer

Je to podobný program, ako ten predchádzajúci, ale je pamäťovo rezidentný. Kontroluje každý spúšťaný program, či nebol modifikovaný. Ak používame tento program (je pomerne zriedkavý), sme schopní zachytiť neznámy vírus hneď na začiatku akcie.

Odstraňovač vírusov (cleaner)

Dôležité je vírus zaregistrovať, ale rovnako dôležité je vírusu sa zbaviť. Najjednoduchšie je vypnúť počítač, aby sme odstránili vírus z pamäte a potom vymazať všetky napadnuté programy. Problém je, ak nemám z daného programu záložnú kópiu. Iným problémom je, ak vírus sedí v boot alebo partičnom sektore. Z boot sektoru ho môžem dostať

príkazom SYS A: (B: či C:). Ale z partičného sektoru to tak jednoducho nejde. Preto potrebujeme pomoc odstraňovača.

Cleaner podľa typu vírusu buď vírus zo súboru úplne odstráni, alebo vírus inaktivuje, alebo oznámi, že daný súbor sa musí vymazať. Dokáže dať do poriadku aj boot a partičný sektor. Ak máme z daného súboru záložnú kópiu, radšej ho vymažme a nainštalujme znova.

Ak sú na disku nezálohované údaje, pred odstránením partičného vírusu je nutné tieto údaje zálohovať. Je isté riziko, že pri pokusu o odstránenie vírusu dôjde k poškodeniu partičnej tabuľky a tým sa zneprístupní celý pevný disk. Dať do kopy partičnú tabuľku nie je činnosť pre amatéra.

Dôležitá vlastnosť cleaneru je schopnosť odstrániť aj neznámy partičný vírus. Ak to nevie a partičný sektor nemáme zálohovaný, máme smolu. Musím nízkoúrovňovo formátovať pevný disk.

Monitor podozrivých činností

Mnoho vírusov pre svoju činnosť potrebuje presmerovať niektoré prerušenia. Súborové vírusy musia otvoriť súbor, ktorý chcú napadnúť. Tieto a podobné aktivity je možné sledovať (pokus o zápis na disk, formátovanie disku, prístup na disketu) a informovať o tom užívateľa. Ten rozhodne, či je daná činnosť prípustná alebo nie.

Takýto prístup je vhodný len pre profesionálov pracujúcich na úrovni assembleru, služieb DOSu a BIOSu.

Vytvorenie záchrannej diskety

Dôležité údaje sú uložené v partičnom a boot sektore, v pamäti CMOS, v tabuľke FAT a v hlavnom adresári. V mnohých antivírusových balíkoch máme program pre nahranie niektorých z týchto dôležitých častí na tzv. záchrannú (rescue) disketu. Ak sa vyskytne problém (najmä s partičnou tabuľkou a CMOSom), tieto dôležité údaje sa nahrajú z diskety späť na dané oblasti disku. Niektoré antivírusové programy majú možnosť porovnať aktuálny boot a partičný sektor so sektorom uloženým na diskete a ohlásiť prípadné zmeny. Je to užitočná funkcia.

Autorizácia prístupu

Často sa vírus dostane na náš počítač vďaka niekomu, kto nemá oprávnenie používať ho. Preto mnohé antivírusové balíky ponúkajú možnosť uzamknúť na heslo klávesnicu, disketovú jednotku, pevný disk, vybrané adresáre.

Je to veľmi príjemná možnosť na ochranu nášho počítača pred bežnými neoprávnenými užívateľmi. Treba poznamenať, že skutočný profesionál prakticky všetky softwarové ochrany vie prekonať. Ale na náš počítač vírus zanesie najskôr amatér.

Integrované prostredie

Programy sa obsluhujú omnoho jednoduchšie, ak sa užívateľ nemusí učiť množstvo parametrov pre spustenie programu v príkazovom režime. Stačí si vybrať v menu príslušnú činnosť, nastaviť parametre. V slušnom prostredí je ku každej činnosti "help" - pomocná informácia. Dobrý antivírusový program by mal mať v prostredí aj informáciu o vírusoch.

Dokumentácia

Súčasťou dodávky softwaru býva aj manuál. Ten má zvyčajne dve časti. Jedna časť je opis práce s programami v balíku a druhá časť je informácia o vírusovej problematike a samotných vírusoch.

Prečo je potrebná druhá časť? Ak nájdeme vírus, nestačí ho odstrániť. Vírus mohol poškodiť aj údajové súbory. Ak o tom nevieme, môžeme zálohovať aj poškodené súbory a keď na poškodenie prídeme, už je neskoro. Preto po odstránení vírusu musíme vždy zistiť, akú škodu mohol daný vírus spôsobiť.

Doplnkové programy

Okrem základných programov každá firma pridá do balíka ešte nejakú príjemnú maličkosť, aby sa líšila od konkurencie. Čo to môže byť?

- *Udička, pasca, lovec* - slúži na chytanie vírusov. Cieľom tohto programu je pokúsiť sa zachytiť na seba vírus a informovať o tom užívateľa.
- *Autorizácia diskety* - umožňuje používanie len autorizovaných diskiet (označených heslom) na danom počítači. Takéto diskety sa ľahko evidujú a kontrolujú.

- *Výpis obsahu pamäte* - zíde sa to, ak nás zaujíma, aký software máme nainštalovaný. Ak sa tam objaví niečo, o čom nič nevieme, je isté podozrenie na vírus.
- *Sektorový prezerač* - umožňuje pozrieť sa aj na obsah partičného a boot sektoru. Pri prezeraní týchto sektorov môže skúsený užívateľ rozpoznať vírus.

Kritéria pri výbere antivírusového programu

Ešte pred výberom antivírusového programu mal by som mať ujasnené:

1. Ako chcem antivírusový program používať.
2. Koľko mám na nákup peňazí.
3. Na koľko počítačov program kupujem.

Pozrime sa na niektoré vlastnosti programov, ktoré by nemali usjť našej pozornosti. V stručnosti:

a) Potrebujeme scanner zachytávajúci čo najviac vírusov, pravidelne aktualizovaný, v bežnej aj rezidentnej verzii.

SCANNER - Vždy sa nájdu nové vírusy, ktoré ani špičkové scannery nezachytia. Mali by sme si overiť, ži scanner, o ktorý máme záujem, chytá niektorý z nových rozšírených vírusov. Nech je pre užívateľa útechou, že 98 % infekcií spôsobuje 20 najčastejších vírusov, ktoré väčšina scannerov zachytí (1376, Slovakia, NoInt, Michelangelo, NewCom, Dir2, Stoned, Jerusalem, Dark Avenger, Yankee Doodle,

Vienna, ...). Dobrý scanner má zabudovanú sebakontrolu. Pri spustení sa skontroluje a ak je napadnutý vírusom, nespustí sa. V súčasnosti je potrebné aktualizovať scanner aspoň raz za 3 mesiace, väčšia organizácia raz mesačne, výnimočne aj on-line. Aktualizácia sa realizuje zaslaním diskety, možnosťou nahrať si najnovšiu verziu z BBS dodávateľa či producenta alebo zasielaním vírusových sekviencií, ktoré sa vkladajú do externej databázy faxom, listom, modemom. Dôležitá je cena za aktualizáciu. Je aktualizácia priamo v cene programu, alebo sa platí osobitne? Čo stojí aktualizácia 4 krát do roka, prípadne raz mesačne? Toto si treba zistiť ešte pred nákupom scanneru. Je vhodné, aby sme si mohli do externej databanky vkladať aj svoje vírusové sekvencie. Napr. čítame článok o novom víruse a je uvedená jeho charakteristická sekvencia. Ak náš program tento vírus nechytá, dopíšeme si jeho sekvenciu Toto je vhodné aj pri získavaní aktualizácií z BBS zo zahraničia. Omnoho lacnejšie je skopírovanie a poslanie po telefónnej linke niekoľko bytovej sekvencie ako celého scanneru. Vkladanie nefunguje zvyčajne pri polymorfných vírusoch.

CLEANER - Dobrý program by mal vedieť odstrániť všetký bežné vírusy tam, kde sa to dá. Odstraňovanie je veľmi dôležité pri partičných vírusoch. Ak ich program nevie odstrániť, je nanič. Špičkové programy vedia odstrániť aj mnohé neznáme vírusy z partičného sektoru. Aj tak je lepšie, ak môžeme mať partičný sektor uložený na záchrannej diskete.)

b) Potrebujeme checksummer.

(Mal by byť dosť rýchly, aby sme jeho používanie neobchádzali. Je vhodné, ak sú údaje o súboroch uložené v jednom súbore, ten si ľahko nahráme na disketu.)

c) Potrebujeme podporu pre vytvorenie záchrannej diskety.

d) Potrebujeme informáciu o škodách, ktoré spôsobujú vírusy.

Hardwarová ochrana

Tá je realizovaná zvyčajne pomocou rozširujúcej karty. Na takejto karte je pamäť ROM so špeciálnym softwarom. Pri bootovaní je jednou z prvých činností scanovanie inštalovaných kariet a inicializácia programov z ROM týchto kariet.

Preto tento software pôsobí ešte pred bootovaním z partičného sektoru. Treba poznamenať, že ani tieto karty nedávajú stopercentnu ochranu proti infiltráciám, ale postačujú ako ochrana pred väčšinou známych vírusov.

MS DOS 5.0

Obsahuje množstvo programov, z ktorých väčšinu bežný užívateľ nepotrebuje.Ak sa však objavia problémy s vírusmi, mnohé programy operačného systému sa nám veľmi zídu.

BACKUP

Program na zálohovanie súborov z jedného disku na druhý disk (disketu). Zálohovanie je nutná vec. Údaje na pevnom disku nám môže zlikvidovať vírus alebo sa pokazí samotný pevný disk. A čo potom? Programy obnovíme z inštalačných diskiet a svoje súbory zo záložných diskiet.

Môžeme zálohovať súbor, adresár, celý disk. Ak zálohujeme len niekoľko súborov, stačí použivť príkaz COPY, ak adresár, použijeme príkaz XCOPY. Takže načo BACKUP?

Problémy nastanú, ak pre zálohovanie súborov z viacerých adresárov potrebujeme niekoľko diskiet a v prípade potreby chceme všetko obnoviť do pôvodného stavu. Iná zábavná vec je, ak je súbor väčší ako kapacita diskety. Tu nepomôže COPY a XCOPY. BACKUP umožňuje aj zálohovanie iba tých súborov, ktoré sa zmenili od minulého zálohovania,

alebo len súborov po istom dátume. To nám umožní znížiť počet diskiet, skrátiť čas zálohovania a preto je menšia pravdepodobnosť, že zálohovanie v piatok o pol štvrtej pustíme k vode.

K obnove súborov slúži príkaz RESTORE. Pre zložitejšie zálohovanie je vhodné vyrobiť si BAT súbor. Ešte lepšie je pre zálohovanie používať špecializované programy (Norton Backup, PC TOOLS).

CHKDSK

Program slúži ku kontrole stavu disku. Vypíšu sa logické chyby zistené v alokačnej tabuľke a v systéme súborov. Dve hlásenia programu môžu indikovať napadnutie disku vírusom:

a) Hlásenie: "bad sectors - chybné sektory".

Niektoré vírusy pre uloženie svojho tela používajú sektory na disku, ktoré označia ako chybné - vlastne označia clustery vo FAT (aby telo vírusu neprepísal nejaký súbor). Iným dôvodom pre toto hlásenie môže byť chyba na disku.

b) Hlásenie "File XXX is cross linked on allocation unit YYY".

Toto hlásenie sa objaví vtedy, ak jeden cluster je v dvoch zreťazeniach clusterov súborov. Takto napr. spoznáme vírus DIR-2, ktorý ukazateľ v adresári na počiatočný cluster súboru presmeruje na seba.

Pomocou tohto programu vieme zistiť aj škody, ktoré spôsobil vírus v tabuľke FAT - úplné poškodenie FAT, prekríženie clusterov v reťazcoch, stratené clustery a podobné radosti.

COMP

Program na porovnanie obsahu dvoch súborov po bytoch. Vhodný je na porovnávanie súborov rovnakej veľkosti (inak použijeme program FC). Tento program použijeme, ak nám test kontrolných súčtov hlási modifikáciu daného súboru a my chceme vedieť, kde je zmena a aká je veľká.

Samozrejme, musíme mať k dispozícii aj neporušený súbor na inštalačnej diskete. Mnoho inštalačných diskiet obsahuje komprimované súbory. Vtedy si podozrivý súbor dáme na disketu a prevedieme inštaláciu celého softwarového balíka.

Ak sa nájdu rozdielne byty, program vypíše hlásenie:

Compare error at OFFSET xxxxxxxx

file1 = xx

file2 = yy

Po 10 zistených rozdieloch sa porovnávanie skončí a program COMP vypíše hlásenie:

10 Mismatches - ending compare

Ak je zmena hneď od začiatku súboru a má aspoň 10 bytov, je veľmi vážne podozrenie, že súbor napadol prepisujúci vírus. Ak sú zmeny neveľké, s náhodnou polohou, ide buď o chybu magnetického média, alebo je podozrenie, že v počítači je vírus, ktorý spôsobuje náhodné zmeny na

disku. Toto podozrenie je oprávnené, ak sa podobné zmeny našli vo viacerých súboroch.

Ak je zmena v prvých 3 bytoch súboru a na konci je niečo naviac, takmer isto ide o napadnutie súborovým neprepisujúcim vírusom. Zmena prvých troch bytov je spôsobená zmenou adresy skoku zo začiatku súboru na telo vírusu.

Ak chceme porovnávať súbory, ktoré sú nerovnako veľké (jeden má možno naviac vírusovú sekvenciu), musíme pridať parameter "/n". Súbory sa porovnávajú len do konca kratšieho súboru.

COPY

Príkaz na kopírovanie súborov. Mnohé vírusy napádajú programy práve pri ich kopírovaní. Bezpečne môžeme kopírovať, ak bootujeme počítač z čistej DOS diskety.

Mnoho ľudí sa bojí manipulovať s disketou, na ktorej sú vírusy. Ak sú na tejto diskete údajové súbory, spokojne ich možno príkazom COPY skopírovať na iné magnetické médium. Netreba zabudnúť potom ihneď vybrať disketu z mechaniky. Zabudnutá disketa spôsobí pri zapnutí počítača aktiváciu boot vírusu a nakazenie počítača. Súborový vírus sa prenesie buť skopírovaním alebo spustením napadnutého programu.

Niektorí užívatelia sa zasa domnievajú, že ak si na disketu skopírujú len údajové súbory, isto na diskete nemajú vírus. Zabúdajú na boot vírusy.

Ak sa kopíruje niečo z diskety na pevný disk, treba disketu chrániť proti zápisu. Ináč sa pri procese kopírovania môže na disketu dostať vírus z nakazeného počítača. A my sa potom čudujeme, že na diskete je vírus, aj keď sa na ňu nič nenahrávalo.

DEBUG

Program na debugovanie (ladenie) vykonateľných súborov. Je málokedy používaný. Často sa zíde schopnosť programu zobraziť obsah ľubovoľnej časti pamäte. Napr. programom "MEM" zistíme, že v pamäti je nainštalovaný neznýmy program. Zapamätáme si jeho adresu a cez "DEBUG" sa pozrieme, čo sa na tomto mieste nachádza. Je možnosť hľadať v pamäti RAM miesto, kde sa nachádza špecifikovaný reťazec. Zaujímavá je aj možnosť spustiť program uložený v pamäti RAM. DEBUG umožňuje nahrať si ľubovoľný sektor z disku do pamäte a pozrieť sa naň, krokovanie programu, disassemblovanie programu a kompiláciu z assembleru.

DEL

Príkaz na vymazanie súborov. Mnoho užívateľov PC si myslí, že ak týmto príkazom vymažú vírusom napadnuté programy, je všetko v poriadku. Mýlia sa.

Pri vymazaní súboru príkazom DEL súbor z disku nezmizne. Len sa miesto, kde sa tento súbor nachádza (reťazec clusterov), určí na ďalšie použitie a prvý znak mena súboru v adresári označí špeciálnym znakom. Potom sa takáto položka adresára nezobrazuje. Dokiaľ sa na miesto vymazaného súboru nevloží iný súbor, je vždy možnosť obnovenia súboru príkazom UNDELETE alebo programami ako je Norton Utilities, či PC TOOLS. Ak je súbor nakazený, takto si možno obnoviť vírus.

DEVICE

Príkaz na nahratie driveru zariadenia do pamäte. Príkaz býva uvedený v súbore CONFIG.SYS. Niektoré vírusy nahliadnu priamo do súboru CONFIG.SYS, prečítajú si názvy driverov a potom ich infikujú. Teoreticky je možný taký vírus, ktorý zabezpečí svoje spustenie tým, že sa vloží do zoznamu driverov v súbore CONFIG.SYS.

DIR

Príkaz na výpis obsahu adresára. Niektorým vírusom stačí použitie príkazu DIR na to, aby infikoval nejaký súbor z vypisovaného adresára. Preto aj obyčajný výpis adresára diskety nechránenej proti zápisu môže spôsobiť zanesenie vírusu.

Príkaz DIR zneužívajú aj niektoré vírusy. Vedia, že pri výpise adresára príkazom DIR neuvidíme nastavenie sekúnd a storočia súboru. Preto môžu použiť sekundy a storočia ako indikátor napadnutých súborov. Vírus Vienna si nastavuje hodnotu 62 sekúnd a vírus Frodo zvýši dátum o 100 rokov.

DISKCOMP

Program, ktorý porovnáva obsah dvoch diskiet (musia mať rovnakú kapacitu). Porovnávanie prebieha po stopách. Tento príkaz sa nám hodí, ak vyrábame záložné diskety z originálnych diskiet, použitím príkazu DISKCOPY. Po vyrobení záložnej diskety treba mať istotu, že sa na ňu nedostal vírus. Bootujeme počítač z čistej DOS diskety a porovnáme diskety. Ak sú diskety rozdielne, objaví sa hlásenie: "Compare error side X, track Y.". Dôvodom zisteného rozdielu môže byť aj chyba na jednej z diskiet. Ak sme skopírovali z jednej diskety na druhú všetky súbory pomocou príkazu COPY, môže sa nám objaviť toto hlásenie: "Compare error on side 0, track 0".

DISKCOPY

Program na fyzické kopírovanie diskiet (zo zdrojovej - source na cieľovú - destination). Cieľová disketa nemusí byť naformátovaná. Program sa používa na výrobu záložných diskiet, ktoré majú byť vernou kópiou originálu. Ak je počítač napadnutý boot alebo partičným vírusom, môže vírus počas kopírovania prejsť do boot sektoru cieľovej diskety. Preto po ukončení kopírovania ochránime cieľovú disketu proti zápisu, bootujeme z čistej DOS diskety a príkazom "DISKCOMP" porovnáme diskety (viď predchádzajúci program).

DOSKEY

Pamäťovo rezidentný program, zapamätá si zadané príkazy MS DOSu, umožňuje ich prezeranie, úpravy a vyvolávanie. Tento program sa

zíde, ak sa počítač správa podozrivo (je vážne podozrenie na vírus) a chceme vedieť, aké programy sa na počítači spúšťali. Pomocou DOSKEY možno vytvárať aj makrá, ich spúšťanie má vyššiu prioritu ako interné príkazy DOSu! Aj v makrách programu DOSKEY môžu byť počítačové infiltrácie.

FC

Program umožňuje porovnanie dvoch súborov a výpis rozdielov medzi nimi. Toto je veľmi vhodné, ak je podozrenie, že niektorý program je napadnutý vírusom. Bootuje sa z čistej DOS diskety. Na disk sa skopíruje z čistej DOS diskety program "FC", založí sa inštalačná disketa s programom, ktorý chceme porovnávať. Ak je rozdiel medzi programom na disku a na diskete v prvých bytoch a na konci jedného súboru je čosi prilepené, ide o vážne podozrenie, že je súbor napadnutý.

Prečo treba bootovať z čistej DOS diskety? Existujú niektoré stealth (neviditeľné) vírusy, ktoré ak sú aktívne, spôsobia, že pri čítaní súboru z disku preskočia vírusové sekvencie a program sa zdá napadnutý.

FDISK

Program na konfigurovanie pevného disku (pre prácu s partíciami). Nemal by chýbať na diskete brávanej na antivírusový zásah. Použije sa vtedy, ak došlo k preformátovaniu disku alebo jeho prepísaniu alebo k prepísaniu začiatku disku, kde je partičný a zvyčajne aj boot sektor.

FIND

Program, ktorý vyhľadáva zadaný textový reťazec v súbore. Ak "FIND" nájde reťazec, vypíše riadok, kde sa reťazec našiel. Tento program sa nám zíde, ak poznáme charakteristický reťazec vírusu, ktorý asi máme

na počítači. Príkazom "FIND" možno hľadať tento reťazec vo všetkých súboroch na disku.

FORMAT

Program na logické formátovanie pevného disku alebo diskiet. Tiež nesmie chýbať na diskete pre antivírusový zásah. Po použití programu FDISK sa musia jednotlivé partície naformátovať. Bežné použitie tohto príkazu je na formátovanie diskiet.

A práve táto činnosť je jedným zo spôsobov, ako si nakaziť diskety boot vírusom. Ak je počítač nakazený boot alebo partičným vírusom, po skončení formátovania sa tento vírus môže preniesť na naše diskety.

Preformátovanie mnohí používajú, ak sa chcú zbaviť vírusu na diskete, alebo na pevnom disku. Formátovanie diskety zvyčajne nie je nutné. Boot vírus sa odstráni použitím programu DOSu napísaním SYS A: (B:, C:), alebo pomocou antivírusového programu. Súborový vírus možno odstrániť vymazaním súborov (pozor na obnovenie programom UNDELETE). DOS 5.0 má dve možnosti formátovanie. Prvá možnosť uschová údaje, ktoré sú na disku. Druhá možnosť (s parametrom "/u", u ako unconditional) prepíše všetky údaje na disku, takže sú neobnoviteľné použitím príkazom UNFORMAT.

MEM

Dôležitý program, umožňuje získať informáciu o obsadení pamäte. Ak sa vie, aká veľká voľná pamäť je k dispozícii a zrazu sa zmenší, musíme pátrať po dôvodoch. Môže ísť totiž o vírus. Ak sa vo výpise obsadenia pamäte objaví niečo podozrivé, čo tam nemá byť (napr. meno objektu - unknown), je riziko napadnutia vírusom. Ihneď treba skontrolovať disk antivírusovým programom a postupuje sa tak, ako by išlo o napadnutie neznámym vírusom.

MIRROR

Program slúžiaci na nahranie aktuálnej informácie o disku. Pomáha pri obnove vymazaných súborov. Pri vymazaní súboru príkazom DEL súbor z disku nezmizne. Len sa miesto, kde sa tento súbor nachádza, určí na ďalšie použitie a prvý znak mena súboru v adresári sa označí špeciálnym znakom. Potom sa takáto položka adresára nezobrazuje. Dokiaľ sa na miesto vymazaného súboru neuloží iný súbor, je vždy možnosť obnovenia súboru, nie je ale vždy stopercentná. Program MIRROR značne zvyšuje šance na úspešnú obnovu vymazaného súboru (a teda aj vírusu).

Program MIRROR je pamäťovo rezidentný. Ak vidí, že mažeme súbor, uloží si o ňom informáciu na prípadné neskoršie obnovenie súboru príkazom UNDELETE do špeciálneho súboru PCTRACKR.DEL. Dá sa nastaviť, o maximálne koľkých súboroch sa uchovávajú údaje na prípadné obnovenie. Program MIRROR pomáha aj pri obnove poškodených systémových oblastí disku.

RECOVER

Program slúži na to, aby vytiahol informácie z chybného (po akcii vírusu) alebo poškodeného disku. RECOVER číta súbor sektor za sektorom a vyberá údaje z dobrých sektorov. Všetky údaje ukladá do hlavného adresára (súbory sú označené ako FILE0001, FILE0002, ...). Na obnovu súborov je ale omnoho vhodnejšie použiť Norton Utilities.

REN

Príkaz na premenovanie súboru. Väčšina vírusov odlišuje vykonateľný súbor (program) podľa rozšírenia. Ak súbor s rozšírením

"EXE" sa premenuje na súbor s rozšírením "EX", postačuje to na ochranu pred mnohými vírusmi, ktoré napádajú aj súbory, s ktorými sa nepracuje. Zmenou rozšírenia zabránime, aby niekto nechtiac spustil program napadnutý vírusom (ak tento program je potrebné z nejakých dôvodov si ponechať).

RESTORE

Program na obnovenie súborov zálohovaných použitím programu BACKUP. Zvyčajne sa obnovujú zálohované súbory z diskety na pevný disk. Jedným z bežných dôvodov obnovy je práve napadnutie disku vírusmi. Pri obnovovaní súborov sú pôvodné súbory prepísané. Ak sú údaje zálohované len na jednej diskete, ešte pred obnovením si zálohujeme údaje z pevného disku (ak sa dajú). Veď čo ak je disketa chybná a obnovenie sa nepodarí? Radšej treba zálohovať údaje na dve diskety.

Pred obnovením treba skontrolovať, či je disk skutočne bez vírusov. Existujú totiž vírusy, ktoré napadnú každý obnovovaný program.

Po obnovení sa opäť skontroluje, či nie je na disku vírus. Zálohované programy mohli byť napadnuté vírusom - existujú vírusy, ktoré vedia pri zálohovaní napadnúť každý zálohovaný program.

Je vhodné mať zálohované len údaje a programy obnovovať z inštalačných diskiet. Aby nebolo všetko pomiešané, uchovávame svoje údaje v osobitných adresároch.. Zálohujeme iba obsah týchto adresárov, prípadne konfiguračné súbory našich programov.

SYS

Program slúži na skopírovanie systémových súborov na disk, disketu. Využíva sa aj na likvidáciu vírusov v boot sektore (ale nie v partičnom sektore!). Napíšeme SYS A: a po víruse v boot sektore diskety

ani stopy. Pritom sa nám na disk skopíruju aj súbory IO.SYS, MSDOS.SYS a COMMAND.COM.

UNDELETE

Program na obnovu súborov vymazaných príkazom DEL. Šance na obnovu súborov zvýši uloženie údajov o disku príkazom MIRROR. Pri obnove programov je riziko, že sa obnoví aj program s vírusom (ktorý práve kvôli napadnutiu vírusom niekto pred chvíľou vymazal). Preto stratený program radšej nainštalujeme z originálnej diskety. Ak to nie je možné, aspoň skontrolujeme program po obnovení antivírusovým programom.

UNFORMAT

Príkaz na obnovu logicky formátovaného disku, diskety. Funguje vtedy, ak nebo disk preformátovaný nízkoúrovňovo alebo s parametrom "/u". Ak je na diskete vírus a pod DOSom 5.0 napíšeme " FORMAT A:", vírus úplne nezlikvidujeme. K tomu je potrebný príkaz " FORMAT A: /u".

Program UNFORMAT vie obnoviť aj poškodenú partičnú tabuľku (napr. vírusom). K tomu sa použije paramater "/partn". Ale pozor! Vie to len vtedy, ak bol predtým použitý program MIRROR s parametrom "/partn" a je k dispozícii súbor PARTNSAV.FIL (na diskete!). Ináč máme smolu.

XCOPY

Príkaz na kopírovanie súborov a adresárov aj s podadresármi. Niektoré vírusy vedia napadnúť všetky programy kopírované pomocou XCOPY. Preto, ak kopírujeme veľa programov, je vhodné pre istotu bootovať počítač z čistej DOS diskety.

DR DOS 6.0

Okrem operačného systému MS DOS existujú aj iné, MS DOS kompatibilné operačné systémy pre PC. Najznámejším z nich je práve DR DOS. Oproti MS DOS 5.0 má DR DOS 6.0 niekoľko rozšírení súvisiacich aj s ochranou údajov a prácou s vírusmi. Pozrime sa, o čo ide:

DELPURGE

Program umožňuje uvoľniť diskový priestor, ktorý zaberajú vymazané súbory pri nainštalovanom programe DELWATCH, ktorý ich udržiava na disku. Ak vymazávame napadnuté programy z pevného disku, použijeme tento program, aby ich nikto ľahko neobnovil.

DELWATCH

Pamäťovo rezidentný program, ktorý chráni programy vymazané príkazom DEL (udržuje si údaje až o 200 vymazaných súboroch). Nie je žiadny problém obnoviť tieto súbory príkazom UNDELETE. Ak vymazujeme napadnuté programy, ľahko ich môže niekto iný obnoviť.

DISKMAP

Tento program umožňuje zálohovať si FAT do súboru. Súbor je vhodné mať na diskete. V prípade rozrušenia FAT na disku si nahrajeme FAT uloženú na diskete. Použitie DISKMAP zvyšuje šance na obnovu vymazaných súborov pomocou príkazu UNDELETE (a tým aj vymazaných programov s vírusmi). Časť FAT je konštantná (ak ide o nainštalované programy) a časť sa neustále mení (pracovné súbory).

LOCK

Program umožňuje dočasné zablokovanie počítača. Zíde sa, ak si potrebujeme niekam odskočiť. Opätovná aktivácia je možná pomocou zadania správneho hesla. Je to užitočné, lebo často užívateľ, ktorý

potrebuje niečo skopírovať či pozrieť, vykoná činnosť na najbližšom voľnom počítači. Stačí, ak odskočíme na chvíľu na WC a už môže byť náš počítač zamorený.

PASSWORD

l) **System Info**, program vypisujúci informácie o systéme.

Trochu filozofie na záver

Profík o antivírusových programoch:

Niet dobrých antivírusových programov, sú len slabí programátori vírusov.

Zákon prideľovania peňazí:

Peniaze na nákup antivírusového programu pridelí šéf deň po napadnutí nášho oddelenia vírusmi.

Postreh operátorky:

Najskôr sú vírusmi napádané nezálohované súbory.

Pragmatické rozdelenie vírusov:

Užitočné: napadnú počítač šéfa, ktorý nechce prideliť peniaze na nákup antivírusového programu.

Dobré: napadnú len susedné pracovisko.

Zlé: napadnú aj naše pracovisko.

Veľmi zlé: napadnú len naše pracovisko.

Svinské: napadnú len môj počítač.

Postreh hráča hier:

Aj vírusy obľubujú dobré hry.

Uvedenie na pravú mieru:

Hlásenie "Virus not found - vírus nenájdený" nie je hlásením vášho antivírusového programu. Je to oznam vírusu, že ho váš program nenašiel.

Svet počítačových vírusov, Michal Danilák, Grada 1992

455107, Sgn: 681-318 Cp