

Počítačové viry

Na viry se v dnešní době stále pohlíží jako na něco magického nebo mystického. Doufáme, že u vás tomu bude jinak po přečtení tohoto příspěvku nebo nejpozději za měsíc, kdy přineseme navazující článek "Antiviry '97".

Viry '97

Máte-li svá data efektivně chránit, musíte poznat svého nepřítele. Budete-li přesně vědět, co všechno viry dokážou, budete také přesně vědět, jaké operace jsou bezpečné a kdy je třeba si dát pozor.

Měl bych úvodem ještě podotknout, že virová a antivirová problematika je součástí širší problematiky ochrany dat a informačních systémů. Lze si totiž snadno představit situaci, že pro účely průmyslové špionáže nebo vydírání by mohl být vyroben "virus na míru" nějaké organizaci nebo nějakému jednotlivci.

Definice a charakteristika

Většina "klasických" definic virů vzala zaslé s příchodem makrovirů. Dnešní definice viru by mohla vypadat takto: Počítačový virus je část programového kódu, která se bez vědomí uživatele sama replikuje. Není třeba, aby každá replika vypadala stejně – stačí, má-li stejnou funkci. Definici sice vyhovují i makroviry, ale je tak obecná, že asi nikomu nic neřekne. Virus je jakýsi programový kód, který je obvykle uživateli skryt. Hlavní vlastností viru je jeho vlastní replikace, probíhající bez kontroly a požadavku uživatele. A ne vždy musí vir zrovna škodit (škodlivost dokonce není často ani ve viru přítomna). Podstatné je, že replikace probíhá bez kontroly uživatele – jinak by bylo možné virem nazvat i operační systém, který se při instalaci sám zkopíruje na disk. Rád bych hned v úvodu zdůraznil, že počítačový virus je program. Nic víc, nic míň. Nemůže tedy proto provádět nic, co by nemohly provádět jiné programy. Nemůže se tedy jen tak stěhovat mezi počítači "vzduchem", ani nemůže "sežrat procesor". Zato vás může během několika sekund připravit o veškerá data.

Nabízí se otázka, kolik vlastně virů na světě je. Na to mohu odpovědět jen to, že nikdo přesně neví a není to ani důležité. Podívejme se na tento problém trochu podrobněji. Záleží na tom, zda dvě varianty viru, které se od sebe liší jen nepatrně, považují za dva rozdílné viry, či nikoliv (autoři virů si totiž na autorská práva příliš nepotrpí a klidně předělávají konkurenční viry k obrazu svému). Pokud započítáváme každou variantu, mohl by se počet virů pohybovat okolo 13 000 (je však otázka, kolik "téměř shodných" virů odborníkům uniklo a kolik virů nikdy neopustilo "stáj" autora). Pro viry však platí modifikovaná varianta "Murphyho zákona 80/20", kterou lze nazvat "99/1", tvrdící, že 99 % infekcí je způsobeno 1 % virů. Virů, které byly zaznamenány na světě alespoň dvakrát (v různých lokalitách nebo časových obdobích), je jen kolem 200 (viz [1]). Při této příležitosti bych též připomenul, že v názvech virů není příliš velký pořádek. Je tedy zcela běžné, že jeden virus je dvěma antivirovými programy nazván zcela odlišně.

Historické počátky

Viry jsou v dějinách výpočetní techniky poměrně mladou záležitostí. První virus byl pro počítač Apple Macintosh a byl vytvořen v roce 1981. První viry pro počítače PC se

datují k roku 1986, ale masovější rozvoj nastal až později. Od roku 1988 je problematika virů brána vážně a o dva roky později už existuje většina dnes známých firem zabývajících se antivirovou problematikou. V roce 1990 se také objevují první polymorfní viry a "první virový toolkit" (nástroj na masovou tvorbu virů). Rok 1991 byl rokem viru Michelangelo, neboť se díky sdělovacím prostředkům o virové problematice dozvěděla široká veřejnost. Následující léta byla ve znamení soutěže autorů virů a antivirových firem. Posledním velkým mezníkem je rok 1995, kdy spatřil světlo světa první makrovirus.

Druhy virů

Pro podrobnější popis a pro pochopení možností infiltrace do systému si musíme nejdříve viry rozdělit do několika skupin. Pro každou skupinu jsou charakteristické jisté vlastnosti, jimiž se odlišuje od ostatních. Viry je možné třídit podle různých hledisek. Nejčastější a nejdůležitější způsob, jakým dělíme viry, je podle uložení kódu viru:

□ **Boot-viry:** Boot-viry jsou obvykle uloženy v bootovacím sektoru diskety anebo v master boot recordu (MBR) pevného disku. Virus však může být uložen i v bootovacím sektoru pevného disku (bootovací viry však ale raději napadají MBR, neboť s ním lze zacházet stejně jako s bootovacím sektorem diskety).

□ **Programové viry:** Programové viry ukládají svůj kód přímo do těla programových (a tedy spustitelných) souborů. Tyto viry typicky infikují soubory s příponou COM a EXE, výjimečně (velmi zřídka) i soubory OVL, OVR, SYS, BIN, DLL a případně také jiné. Můžeme je ještě rozdělit do dvou malých podskupin – na viry přepisující a viry prodlužující. Viry přepisující necitelně přepíší část hostitelského programu, zatímco prodlužující se snaží připsat k hostitelskému programu tak, aby pracoval pokud možno i nadále.

□ **Makroviry:** Makroviry jsou "hitem" posledních dvou let. Základním pojmem z této oblasti je "Makro". Jde o programový kód, napsaný v tzv. makrojazyce různých programů. Mnoho programů (především z řad kancelářských balíčků) nabízí takové možnosti pro tvorbu maker, že lze s jejich pomocí vytvořit i "množivá makra", která se mohou nepozorovaně šířit. Jejich vznik zavinila skutečnost, že si autoři makrojazyků neuvědomili, jakou dávají programátorům do rukou sílu. V současnosti je největší počet makrovirů k dispozici pro Microsoft Word; navíc existují i makroviry pro Microsoft Excel a Lotus AmiPro.

Ačkoli se proti makrovirům můžeme velmi účinně bránit, jsou oproti programovým virům v ohromné výhodě – výměna dokumentů je daleko častější než výměna programových souborů. Jelikož však proti makrovirům autoři makrojazyků mohou vybudovat účinnou ochranu, nevěštím této skupině virů příliš dlouhou a růžovou budoucnost.

□ **Doprovodné viry:** Doprovodné viry využívají mechanismu, jímž DOS vyhledává soubor, který požadujete spustit. Pokud napíšete do příkazové řádky DOS nějaký příkaz, například EXPORT, hledá DOS v aktuálním adresáři soubor EXPORT.COM. Nenalezne-li jej, zkusí to s EXPORT.EXE a nakonec s EXPORT.BAT. Pokud žádný z nich nenalezne, bude tyto soubory v tomto pořadí vyhledávat v adresářích uvedených v systémové proměnné PATH. Nenalezne-li žádný z takových souborů ani tam, objeví se chybové hlášení, že soubor nebyl nalezen. Doprovodné viry fungují tím způsobem, že umístí svůj kód tak, aby byl díky tomuto mechanismu spuštěn dříve než vlastní program – pokud např. chtějí "infikovat" MOUSE.EXE, zapíše své tělo do souboru MOUSE.COM. Jestliže pak uživatel napíše příkaz "MOUSE", spustí vlastně podstrčený virus, a ne požadovaný program. Virus však obvykle po provedení

nějakých svých akcí (např. množení) spustí "správný" program, aby uživatel nic nepozoroval. V dnešní době však doprovodných virů příliš nepřibývá.

□ **Clusterové viry:** Clusterové viry jsou zvláštní a poměrně úzkou skupinou virů. Napadají programové soubory, avšak neukládají se do nich. Tyto viry upravují FAT tabulku pevného disku tak, aby ukazatel na soubor ukazoval na virus.

□ **Speciální viry:** Mezi speciální viry bych zařadil např. viry, které se šíří v dávkových souborech. Autoři [3] udávají také viry, které se dokonce šíří ve zdrojových textech programů, a viry vkládající do komprimovaných archivů (ZIP, ARJ) infikované soubory. Jde však spíše o rarity, dokazující, co všechno je také možné naprogramovat. Žádné vážné nebezpečí vám od těchto virů však v současnosti naštěstí nehrozí.

Poznámky: Termínem "Souborové viry" jsou ve starší literatuře (z doby, kdy neexistovaly makroviry) nazývány programové viry. Dnes pod tímto pojmem myslíme souhrnně programové viry, makroviry a případně i doprovodné viry. Multipartitní viry jsou viry, které mohou uložit svůj kód i několika způsoby. Na tyto viry můžeme nahlížet podle toho, v jaké z podob se zrovna nacházejí. V praxi jsou však známé pouze takové multipartitní viry, které přecházejí mezi podobami programových virů (obvykle na disketách) a bootovacích virů (obvykle na pevném disku). Podívejme se ještě na některé skupiny virů, o nichž byste měli něco vědět.

□ **Polymorfní viry** jsou viry, které se umějí zakódovat mnoha různými způsoby, takže se pak velmi obtížně hledají. Mohou mít až několik miliard podob. Příchod těchto virů způsobil, že nejedna antivirová firma musela rychle přeprogramovat svoje antivirové systémy, neboť detekci těchto virů je nutné založit na trochu jiných principech.

□ **Rezidentní viry** jsou takové viry, které po první aktivaci zůstávají v operační paměti počítače. Jsou tak schopny zasahovat do činnosti vašeho počítače kdykoliv a jakkoliv. Pojem "rezidentní program" je typický pro operační systém DOS. V jiných operačních systémech (např. Windows 95) se jako rezidentní programy někdy označují ovladače zařízení (soubory VxD a nebo 386). Drtivá většina nejčastěji se vyskytujících virů jsou viry rezidentní; i všechny bootovací viry jsou také rezidentní. Veškeré ostatní viry jsou viry nerezidentní.

□ **"Stealth" viry** jsou speciální skupinou rezidentních virů, které se velice důmyslně maskují. Při žádosti programu (i antivirového) o zjištění údajů, které by vedly k odhalení viru, vrátí virus původní údaje. Proto antivirové programy používají speciální techniky pro zjišťování skutečných údajů o paměti a disku.

Mechanismy infiltrace a šíření

Jeden z důležitých okamžiků, který nás bude zajímat, je okamžik infiltrace – tedy okamžik, kdy počítač napadne virus a začne provádět svoji škodlivou činnost. Jelikož je dnes prakticky každý počítač vybaven pevným diskem, virus se obvykle snaží "nainstalovat" na pevný disk – a to nejlépe tak, aby se příště aktivoval ihned při startu systému.

Bootovací viry mohou infikovat počítač jediným způsobem – nabootováním (resp. pokusem o bootování) z infikované diskety. Všechny starší počítače (a většina nových) po startu kontrolují, zda je v disketové mechanice A: přítomna disketa. Nenajdou-li disketu (což je obvyklý případ), je zaveden operační systém z pevného disku. Pokud je disketa nalezena (ať už obsahuje operační systém nebo ne), snaží se počítač z této diskety načíst operační systém. A je-li na této disketě bootovací virus, zaktivuje se a s velkou pravděpodobností přepíše na pevný disk. Při dalších startech počítače je už

virus načítán z pevného disku. Bootovací viry se obvykle šíří na všechny diskety, které jsou vloženy do disketové mechaniky a s nimiž se pracuje (a nejsou chráněné proti zápisu).

Souborové viry (či doprovodné viry) se mohou do počítače infiltrovat přinesením infikovaných souborů. A ty se mohou na počítač dostat mnoha různými způsoby – z diskety, z CD disku, po modemu ze stanice BBS, elektronickou poštou v připojeném souboru, z internetu a jistě by se podařilo najít i další způsoby. K aktivaci takového viru (a k možnosti dalšího šíření) dojde při prvním spuštění infikovaného programu anebo při otevření infikovaného dokumentu příslušným programem. Aktivovaný programový virus se pravděpodobně pokusí infikovat jiné soubory na počítači. I aktivovaný makrovirus se pokouší aktivovat jiné dokumenty anebo šablony. Makroviry pro Microsoft Word téměř vždy napadají šablonu "normal.dot", odkud se mohou šířit dále do všech nových dokumentů. Rezydentní programové viry zůstanou obvykle po první aktivaci uloženy v paměti a infikují každý další program, který spouštíte.

Je však třeba říci, že se žádné viry nešíří "prostou" elektronickou poštou (bez připojeného souboru). Zprávu bez souboru lze zatím považovat za bezpečnou. Souborové viry se však mohou (jak už jsme uvedli) šířit v připojených souborech. Takovýto virus je aktivován v okamžiku, kdy spustíte přijatý infikovaný program anebo když otevřete infikovaný dokument. Na tomto místě si též dovoluji zmínit, že v [8] je popsán makrovirus pro Word, který využívá speciálních vlastností pošty Microsoft Mail. Tento virus po své aktivaci (otevřením dokumentu) zašle několika uživatelům (z vašeho seznamu adres) zprávu obsahující soubor s makrovirem (a takto se šíří). O to horší je, že makrovirus si poslaný dokument sám "vybere" a příjemci mohou dostat do rukou dokument s citlivými daty. Jde opět o virus šířený v souborech – ne v těle zprávy.

Existují však ještě dva způsoby, jak lze počítač s Windows 95 nebo Windows NT 4.0 virem infikovat. První možnost vychází z toho, že standardní instalace Windows 95 nebo NT 4.0 má zapnutou funkci AutoPlay pro CD. Vložíte-li do mechaniky CD-ROM nějaký CD disk, Windows na něm hledají a spouštějí soubor Autorun.inf. Soubor sice nemá příliš mnoho možností manipulace se systémem, lze z něj však spustit libovolný soubor z tohoto CD i z vašeho disku. A tento soubor už může obsahovat běžné souborové viry anebo makroviry (jde-li o "spouštění" dokumentu). (Nutno říci, že tuto "rošárnu" je možné narafičit i na pevný disk. Autorun.inf z kořenového adresáře tohoto disku – potažmo virus – bude však aktivován až po poklepání ikony s diskem z okna Můj počítač). Druhá možnost infikování je zatím trochu otázkou budoucnosti, avšak ne tak vzdálené.

S uvedením ostré verze Internet Exploreru 4.0 (i ten bude obsažen v nových Windows 98) se autorům virů dostane do rukou další zbraň. Každý adresář v souborovém systému bude možné prohlížet "jako webovou stránku". Při vstupu do adresáře se tedy vyhledává soubor folder.htm a v případě, že je nalezen, zobrazí se jako WWW stránka. Tato stránka může jako kterýkoli jiný HTML dokument obsahovat odkazy na spustitelné soubory, na dokumenty Office (případně i jiných programů) anebo komponenty ActiveX, které se nacházejí buď na internetu, anebo přímo na disketě. Tyto programové soubory mohou obsahovat programové viry, dokumenty mohou obsahovat makroviry anebo ActiveX objekty mohou provádět různorodou činnost. Připouštím, že tato druhá cesta je poněkud krkolomná, ale ne zase tak nepravděpodobná. Internet Explorer se sice zeptá, zda má soubor opravdu otevřít, či zda ActiveX objekt opravdu instalovat a aktivovat. Troufám si však tvrdit, že většina běžných uživatelů by na varování Exploreru reagovala "OK, otevřít". (Je též nutné vzít v úvahu, že Explorer si umí sám takovýto odkaz "odklepnout". Pak už jen zbývá na stránku napsat "za chvíli vás bude Internet Explorer varovat... Vyberte Otevřít a

klepněte na OK". A ještě jedna poznámka. Tato potenciální nebezpečí byla už u Internet Exploreru 3.x. Internet Explorer 4.0 pouze k těmto mezerám přidal možnost automatického otevření HTML souboru.)

Trendem je tvorba virů s co nejdelší "inkubační dobou" – tedy virů, jež svou nekalou činnost začnou až po dlouhé době. Mohou se tedy nekontrolovaně šířit poměrně dlouhou dobu, než na sebe svým útokem upozorní.

Škodlivost virů

Třebaže to často není ani jejich primárním účelem, viry uživatelům v několika směrech škodí. Škody virů bych si dovolil rozdělit do tří skupin:

□ Škody "implicitní" páchají viry už svou přítomností. Jelikož virus musí nutně být někde uložen, blokuje diskovou kapacitu, a je-li rezidentní, i paměťovou kapacitu. Pokud se virus příliš rozmnožuje, může to zpomalovat práci s počítačem.

□ Neúmyslné škody nejsou úmyslem jejich autorů, ale spíše chybou ve viru (chyby se nevyhýbají ani autorům virů). Viry mohou způsobovat, že počítač "nevysvětlitelně" zamrzá anebo programy po infikování nepracují zcela korektně. Havárie virů často vznikají za jakýchsi přesně specifikovatelných okolností (určitá délka infikovaného souboru, určitá míra zaplnění paměti apod.). Častá bývá kolize s jinými rezidentními programy anebo jinými operačními systémy (např. Windows). I rafinovanější "stealth viry" anebo tunelující viry mohou kolidovat s různými (zejména rezidentními) programy. Boot-viry, které umísťují svoji část (anebo původní boot sektor) na část nulté stopy, se např. mohou dostat do kolize s programem "Ontrack Disk Manager". Tento program umožňuje používání pevných disků větších než 500 MB na počítačích se starším BIOS a také ukládá svůj kód na část nulté stopy.

□ Úmyslné škody bývají nesmírně vážné. Méně závažnými projevy virů jsou různé efekty na obrazovce, různé nesmyslné hlášky (pomluva či propagace čehokoliv – třeba i politické strany), zvukové projevy a jiné. Mezi závažné patří např. smazání části disku (či disku celého). Jelikož by rozsáhlejší okamžité katastrofy virus prozradily, bývají načasovány na nějakou událost (autorovy narozeniny, pátek 13., státní svátky, určitý počet dní od infikování počítače apod.) anebo mohou zasáhnout s určitým stupněm náhody. Existují dokonce kalendáře, které vám na viry prozradí, ve které dny začnou působit (pokud byste se však podle takového kalendáře chtěli řídit a počítač zapínat jen v "bezpečných dnech", musím vás zklamat – žádné "bezpečné dny" už neexistují).

Možná ještě závažnější jsou "plíživé katastrofy", kdy virus velmi pomalu přepisuje obsah disku různými nesmysly. Na tuto jeho činnost obvykle uživatel hned tak nepřijde a poškozené a nepoužitelné soubory si může proto zanést i na záložní kopie (a nahradit si jimi ty správné). Při návrhu strategie zálohování proto pamatujte, že můžete třeba dohledávat i na zálohách několik měsíců starých.

Viry a platformy

Hlavní platformou, pro niž je určena drtivá většina virů, je DOS. Umožňuje poměrně jednoduchou tvorbu programů na úrovni assembleru, je už poměrně dobře zdokumentovaný, dovoluje přímý přístup k hardwaru, neobsahuje téměř žádné bezpečnostní prvky apod. Rozšiřování DOS virů napomáhalo i to, že na platformě DOS byla výměna programových souborů (a tedy potenciálních nosičů programových virů) poměrně běžnou záležitostí. S rozšiřováním moderních 32bitových operačních systémů lze očekávat nový přísun virů pro tyto systémy.

Ty, kdo si myslí, že s příchodem nových operačních systémů budou mít pokoj od virů, musím tedy zklamat. Nejen že tyto systémy téměř žádnou ochranu proti virům neposkytují a že na těchto operačních systémech většinou pracují i DOS viry (viz dále),

ale tyto systémy poskytují i autorům virů mnoho nových příležitostí. Naštěstí se zatím tyto nové operační systémy autorům virů nelíbí.

Staré Windows 3.1x žádné zvláštní ochrany proti virům neobsahovaly, proto se v prostředí Windows 3.1x bez větších problémů šířila většina původních DOS virů. To, že speciálních virů pro Windows 3.1x je tak málo, je spíše dáno tím, že z pohledu autora viru bylo zbytečné tvořit takovéto viry (když dostatečně dobře fungovaly viry klasické). Jisté zábrany řádění virů přinesly až Windows 95. Windows 95 jednak kontrolují obsah bootovacího sektoru a jednak varují při instalaci rezidentního programu, který nějak zasahuje do přístupu na disk. Navíc jsou Windows 95 už "méně kompatibilní" se starým klasickým DOS, takže zdaleka ne všechny staré viry budou v novém prostředí schopny života. Pokud by se někdo snažil vyrobit speciální 32bitový virus pro Windows 95, mohl by narazit při pokusu o obcházení systémových služeb a také by narazil na ochranu kódu v paměti, která zabraňuje tvorbě kódujících se virů. Zato nové Windows 95 přinášejí mnoho nových možností pro tvorbu virů – např. ovladače VxD, OLE 2 a další. Nehledě na to, že Windows 95 jsou daleko rozsáhlejší systém, a viry se v takovém "guláši" daleko snadněji skryjí.

Windows NT přinášejí konečně mechanismy, které mohou (alespoň částečně) zabránit infiltraci virů do počítače. Při použití souborového systému NTFS je možné specifikovat práva přístupu do jednotlivých adresářů pro jednotlivé uživatele. Avšak i na tomto operačním systému může působit určitá část starých dosových virů. Jinak pro tento operační systém platí stejné informace jako pro systém Windows 95 (co se týče znesnadnění tvorby nových virů a možností skrývání). Měl bych také upozornit, že některé boot-viry mohou při infekci NTFS disku tento disk (resp. data na něm) nenávratně poškodit.

Viry a síť

Po sítích se obecně viry šířit mohou, ale samozřejmě nemohou překonávat standardní ochrany sítě (zákaz zápisu do určitých oblastí apod.). Přestože se tedy viry často po síti šíří jako na běžných discích (neboť nepoznají rozdíl), viry na počítačové síti mohou napáchat větší škody než na samostatných počítačích. Při "chytrém" infikování jednoho souboru nemá virus problém rozšířit se během dvou hodin na všechny počítače sítě (je-li dostatečně infekční). Existuje i jistá (poměrně úzká) skupina virů využívající speciálních vlastností určitých sítí (zejména Novellu). Tyto viry se snaží např. zjistit heslo administrátora a získat tak nad sítí administrátorská práva.

V tomto kontextu stojí také za to zmínit se, jak je to s viry na Síti sítí – tedy na internetu. Problematika virů na internetu má několik rovin. Pokud z internetu získáte nějaký soubor (pomocí služeb FTP, WWW anebo vám přijde elektronickou poštou), neměli byste zapomínat, že jako kterýkoli jiný soubor může obsahovat souborový virus – ať už programový virus, vyskytující se v programových souborech, nebo i makrovirus, např. ve wordovém dokumentu. Proto si soubory stahujte pouze z důvěryhodných serverů a pro jistotu si je raději zkontrolujte dostupnými antivirovými programy. Další rovinou tohoto problému je nebezpečí, které na uživatele čeká jindy než při práci se soubory. Práce s WWW stránkami byla v dobách "hloupých" prohlížečů poměrně bezpečná, neboť tyto prohlížeče neumožňovaly nic jiného než **zobrazovat** přijímaný text. Dnešní "chytré prohlížeče" však umožňují **interpretaci** různých "aktivních" objektů, jako jsou moduly plug-in, ActiveX objekty anebo Java applety.

Prohlížeče se obecně snaží chránit uživatele před nekalou činností těchto objektů, nicméně se už našla nejedna chyba (zejména u microsoftských prohlížečů), která umožňovala provádět různou "nečistou" činnost – např. spuštění viru (viz např. [5] nebo [6]). Je sice pravda, že firma Microsoft všechny "provalené" chyby okamžitě odstranila, ale kdo ví, kolik jich tam ještě zůstalo... Dále byste měli vědět, že ActiveX prvky jsou chráněny pouze jakousi "podpisovou signaturou" – te- dy jakýmsi kódem,

jenž jednoznačně identifikuje autora a který není možné "zfalšovat". Avšak podepsaný ActiveX prvek může na počítači provádět naprosto cokoli, co mu dovolí operační systém (tedy i množivou činnost). Objevily se i určité (podle mých zpráv zatím nepotvrzené) informace, jak je možné "zfalšovat" podpisové signatury. Java applety (jelikož jde o interpretovatelný kód) jsou před spuštěním verifikovány, zda neobsahují nějaký nekorektní kód a applety stažené z internetu mají jistá bezpečnostní omezení. Avšak i zde se vyskytlo několik problémů (byly však ihned vyřešeny).

Nechci nikoho strašit, ale WWW už není stoprocentně bezpečný. Zde se nabízejí dvě rady: Navštěvujte pouze důvěryhodné servery, a pokud nejste zatíženi na různé pohyblivé a interaktivní objekty, používejte staré, hloupé (ale bezpečné) prohlížeče. Takové rady jsou však k ničemu. Samostatnou kapitolou je šíření virů elektronickou poštou. Zde odkazují na výše uvedené informace o infiltraci a na pověru "Good Times", uvedenou v závěru.

Viry a pověry

Jednou z pověr je, že viry mohou ničit hardware. Jak vtipně uvádějí autoři v [4] (údajně však vymyšleno u Alwil Software), hardware, který lze zničit programovými prostředky, si ani nic jiného nezaslouží. Je pravda, že některé zastaralé pevné disky bylo možné zničit tzv. "low-level formátováním" či některé monitory bylo možné zničit přehřátím při pokusu o přepnutí na nesmyslnou zobrazovací frekvenci. Měl bych však zdůraznit, že moderní hardware nemusí mít před viry (a softwarem obecně) žádný strach, neboť je dostatečně chráněn od výrobce proti pokusům o programové poškození.

Mohou viry nakazit datové soubory? Před několika lety bychom na tomto místě mohli uvést, že z datových souborů žádné nebezpeční nehrozí. Dnes je však všechno trochu jinak... Viry sice stále nemohou nakazit **obecné** datové soubory, ale některé **speciální** datové soubory (např. výše jmenované dokumenty Wordu) je možné při **znalosti jejich struktury** pomocí **speciálních** virů infikovat. Nepatříte-li tedy k odborníkům, nemůžete si dnes být zcela jisti ani před datovými soubory. Lze ale předpokládat, že autoři programů pracujících s těmito datovými soubory znemožní šíření virů v takovýchto souborech (neboť to není zas tak velký problém...).

Jednou z pověr také je, že "chytrý" virus může být do počítače zatažen pouhým prohlédnutím obsahu diskety, případně CD. Před několika lety se také uvádělo, že to není možné. Je to v podstatě pravda i dnes, neboť v prostředí DOS a Windows 3.1x opravdu není možné prohlédnutím obsahu diskety (pomocí Manažeru602, příkazu DIR či jiných prostředků) virus z diskety aktivovat. Jak už jsem se však zmínil, ve Windows 95 a NT 4.0 je možné počítač infikovat při zapnutí funkce "AutoPlay" pouhým zasunutím CD disku či prohlédnutím adresáře pomocí Internet Exploreru 4.0. A naopak, disketu je možné infikovat pouhým prohlédnutím jejího obsahu. Mohou viry napadnout disketu chráněnou proti zápisu? Ochrana disket proti zápisu je na počítačích PC opravdu bytelná, takže viry se na chráněnou disketu skutečně zkopírovat nemohou. Pro jistotu podotýkám, že hovořím o ochraně pomocí "šoupátka" (které v poloze "otevřeno" chrání disketu proti zápisu). Některé viry jsou však tak drzé, že si o povolení zápisu na disketu prostě požádají uživatele. A ne jeden uživatel jim jistě vyhoví...

Také bych zde vyvrátil letitou fámu, která se šíří už dlouhou dobu po internetu a čas od času zasáhne i moji poštovní schránku. Že zpráva s názvem (subjektem) "Good Times" (občas nazývaným i jinak) obsahuje jakýsi škodlivý virus, který se po otevření zprávy nekontrolovaně šíří, ničí procesor a kdovíco ještě. Nic podobného není dost dobře možné – jak už jsme uvedli, viry se mohou elektronickou poštou šířit jen

jako připojený soubor, z něhož se notabene virus může aktivovat až jeho spuštěním, resp. otevřením.

Často se též setkávám s otázkou, zda může být virus uložen v paměti CMOS hlavní desky počítače. Představa uložení viru v paměti CMOS je sice velice atraktivní (především pro autory virů), ale naštěstí nerealizovatelná, a to hned z několika důvodů. Jednak v paměti CMOS nemůže být uložen spustitelný kód, paměť CMOS je příliš malá a změna jejího obsahu by se okamžitě projevila (vedla by k okamžitému prozrazení viru). Paměť CMOS však bývá poměrně často předmětem útoku virů – za určitých podmínek vám virus zničí její obsah.

Martin Beran

Literatura:

1. Baudiš P., Zelenka J.: Antivirová ochrana, Plus 1996.
2. Jalůvka J.: Moderní počítačové viry, Computer Press 1996.
3. Odehnal P., Zahradníček P.: Praktická sebeobrana proti virům, Grada Publishing 1996.
4. Počítačové viry a Vy, dokumentace k AVG 5.0, Grisoft Software 1997.
5. Svět Internetu č. 6/97, str. 5.
6. Svět Internetu č. 7/97, str. 5.
7. CHIP 10/96, Rosa, T.: "Crack 95", str. 138.
8. CHIPweek 10/97, "Čtyřikrát na téma bezpečnost", str. 25.

Autor:

Martin Beran

Rubrika:

Magazín

Vydání:

729298 - 729328

Počítačové viry a jak na ně

Tento článek volně navazuje na článek "Viry '97" z minulého čísla Chipu. Tam jsme se podrobně zabývali tím, co se dnes na virové scéně odehrává.

Antiviry '97

Proti infekci počítačovým virem se můžete chránit řadou způsobů. V ochraně proti počítačovým virům je možné používat prostředky programové, technické, psychologické a jistě mnohé další. V článku se budu zabývat především prostředky programovými a částečně i prostředky technickými. Ostatní prostředky jsou popsány např. v [3]. Je však jasné, že tyto prostředky je nutné vždy zkombinovat dohromady – nemá cenu instalovat antivirový program a nepoučit ostatní uživatele o jeho používání, o nebezpečí virů a o tom, co dělat, hlásí-li antivirový program přítomnost viru.

Článek je koncipován tak, aby jej mohli číst i méně zkušené uživatele (po přečtení prvního dílu – viz úvod). Některé zde popsané metody detekce a odstraňování vyžadují určité znalosti a zkušenosti a nejsou proto určeny pro "běžné" uživatele.

Používání antivirů

Má-li mít používání antivirových programů smysl, je nutné je používat pravidelně a důsledně. Některé důležité antivirové techniky mají také spíše preventivní účinek anebo mají smysl pouze při jejich nasazení ještě před vlastním infikováním.

Kdo by měl používat antivirový software? Odpověď zní: každý, kdo používá disketovou mechaniku, jednotku CD-ROM, internet či se připojuje k ne zcela "bezpečné" lokální síti – tedy de facto každý. V době makrovirů, které se šíří prostřednictvím dokumentů, si tedy nemohou být před viry jisti ani ti, kdo používají počítač jako psací stroj, žádné programy na počítač nepřinášejí a internet nepoužívají. Uživatele bych také rád upozornil na to, že viry se čas od času objevují i na různých sharewarových CD. I s originálním softwarem si můžete přinést virus (jistá firma, která nyní ve sdělovacích prostředcích tvrdí, že originální software nemůže obsahovat viry, by mohla z vlastních zkušeností ukázat opak). A pokud si přesto myslíte, že antivirový program je zbytečný luxus, protože vy jistě viry na počítači nemáte, snad vás poučí, že přesně to si myslela i většina těch, u nichž jsem viry nakonec našel. Antivirový program si nepořizujte, až budete mít s viry problémy, můžete snadno zjistit, že už není co zachraňovat.

Ačkoliv to bude znít poněkud fádně, je nutné vždy používat "antivirus" jménem "backup" (tedy obecně zálohovací program). I sebelepší antivirový program občas selže – většinou je však na vině spíše nesprávná obsluha. V takovém případě opravdu nezbyvá, než se uchýlit k záložním kopiím... Nehledě na to, že o data můžete přijít i jinak, než jen působením virů (po živelné pohromě, úmyslným zničením či selháním technického vybavení). Na závěr tohoto odstavce snad už jen malý citát: "Cenu svých dat poznáte, až o ně přijdete."

Metody konkrétní detekce virů

Metody konkrétní detekce virů jsou zaměřené na hledání přítomnosti konkrétních a známých virů. V podstatě jedinou metodou této skupiny, kterou se stojí za to zabývat, je "vyhledávání sekvencí". Výhodou této metody je minimální možné procento falešných poplachů (tj. – když už něco antivirový program najde, je to skoro určitě virus), poměrně vysoká úspěšnost a velká rychlost. Je to také v podstatě jediná metoda, která dovede poměrně úspěšně objevit virus na disketě (CD disku), kterou chcete použít. Nevýhodou ale je, že tyto techniky se musejí velice často aktualizovat, neboť jak jsme si řekli minule, virů rapidně přibývá. Přesto se této metody používá ve všech antivirových programech a patrně je i nejdůležitější a nejpoužívanější. Proto se jí budeme zabývat také podrobněji než ostatními. Jde o metodu zvanou "vyhledávání sekvencí", protože v dobách "virového starověku" opravdu antivirové programy procházely soubory a bootovací sektory (případně paměť) a hledaly v nich několikabajtové sekvence, které byly charakteristické pro některé viry. Od dob, kdy se objevily měnící se viry – zejména viry polymorfní – bylo nutné tuto techniku trochu přeprogramovat tak, aby byla schopná si poradit s dekryptovacími cykly. Je to metoda velmi univerzální, neboť umožňuje vyhledávat všechny základní druhy virů (bootovací viry, programové viry i makroviry) a umožňuje je vyhledávat v bootovacích sektorech, MBR, paměti i souborech na disku i disketách.

Kvalitní antivirové programy umožňují také tuto metodu aplikovat na interně komprimované programy (pomocí programů PKLite, Lzexe) a na komprimované archivy (např. pomocí programů ARJ, ZIP apod.). Navíc mohou též vyhledávat uživatelsky definované sekvence virů, generovat zprávu o nalezených virech anebo automaticky po síti informovat administrátora o nalezených virech.

Pokud byste chtěli porovnávat antivirové programy podle možností této metody, obvykle se berou v úvahu kritéria úspěšnosti nalezených virů, rychlost vyhledávání a četnost falešných poplachů. Při testu úspěšnosti (úplnosti) nalezených virů se obvykle provádějí testy jednak na nějaké velké virové databázi a jednak na malé databázi nejrozšířenějších virů. Testování na "velké" databázi je sice jistě důležitým kritériem, ale je třeba si uvědomit, že naprostá většina virů, které jsou v tomto testu programu předloženy, jsou viry "trezorové", a s těmi se "v terénu" nikdy nesetkáte. Pokud 10 % takovýchto virů program nenalezne, není to až taková tragédie. "Malá" databáze obvykle obsahuje "pouze" asi 200 nejrozšířenějších virů. Testy na ní jsou neskonale přísnější a nenalezení jediného viru z této skupiny by se antivirovým programům nemělo promíjet.

Vyhledávání sekvencí je též možné provádět rezidentně. V takovém případě je známý virus vyhledáván v každém spouštěném programu a obvykle také v bootovacím sektoru každé diskety, s níž pracujete. Je možné zajistit i automatickou kontrolu každého otevíraného dokumentu. Zajímavou možnost nabízí program "Webscan": rezidentně kontroluje každý program stažený z Webu.

Metody obecné detekce virů

Metod obecné detekce virů je o poznání více než metod konkrétní detekce virů. Tyto metody umožňují vyhledání čehokoli, co jeví známky viru. Jedinou výhodou těchto metod je, že jsou schopny zachytit i virus, který byl v době návrhu těchto metod zcela neznámý. Tyto programy zachytí i např. špionážní "virus na míru" anebo obecně jakýkoli program, který by mohl poškodit informační systém. Přestože tedy není nutné tyto metody často aktualizovat, má jejich použití i několik nevýhod. Hlásí více či méně často falešné poplachy a některé (ne všechny) metody mohou naopak propustit zcela zjevný virus. Některé (opět ne všechny) metody jsou také schopné virus odhalit teprve v okamžiku, kdy infiltroval do systému a dostatečně se namnožil. A některé metody nepomáhají proti makrovirům.

Jednou z nejdůležitějších metod obecné detekce je "kontrolování integrity", které tvoří druhý stěžejní téměř všech antivirových systémů. Princip fungování této metody je jednoduchý: většina informací na disku – zejména pak obsah systémových oblastí a obsah spustitelných souborů – se často nemění. Jde tedy o mechanismus jednoduchý – při prvním spuštění si program zapíše informace (tj. nějaký druh kontrolních součtů) o systémových oblastech disku a o spustitelných souborech. Z důvodů většího komfortu se obvykle ukládají také atributy, délka a datum poslední aktualizace. Při dalších spuštěních pak program porovnává tyto uložené informace se skutečností. Případné změny mohou znamenat virovou infekci a měly by být dále analyzovány.

Tato metoda musí být nasazena dříve, než je systém virem infikován. Jde bohužel také o jedinou metodu schopnou virus odhalit až v okamžiku, kdy infiltroval do systému. Pomocí návazných metod je možné též neznámé (i známé) viry odstraňovat. Tato metoda patří mezi středně rychlé metody a ne každý její nálezný je možné kvalifikovat jako virus. V zásadě lze tuto metodu aplikovat i na dokumenty, které mohou obsahovat makroviry. Jelikož se však některé dokumenty často mění, musíte počítat s velkým množstvím falešných poplachů.

Antivirové programy si obvykle ukládají do databáze celé (či skoro celé) kopie bootovacích sektorů a MBR, neboť tyto oblasti nejsou příliš dlouhé a informace v nich jsou velice cenné. Některé antivirové programy též ukládají do databáze i "hlavičky" souborů (určitý počet bajtů od začátku), neboť tyto informace mohou také zjednodušit obnovování souborů (viz dále). Přestože to nemá v praxi příliš velké opodstatnění, i kontrolu integrity je možné provádět rezidentně. V takovém případě je obvykle kontrolována integrita každého spouštěného programu.

Další metodou, která se do jisté míry stala fenoménem několika posledních let, je "heuristická analýza". Metoda spočívá v procházení instrukcí programového kódu a ve vyhledávání různých podezřelých činností – např. vyhledávání souborů, instalace rezidentní rutiny apod. Takto se obvykle krokuje určitý začátek programu (určitý počet instrukcí od začátku programu). Čím více instrukcí se projde, tím je větší spolehlivost této metody, ale trvá déle a zvyšuje se možnost falešného poplachu. Viry se tomuto krokování brání tím, že umísťují do svého těla různé "pastičky", které nebudou tyto analyzátoři schopny interpretovat správně. Této metodě by jistě dělaly problémy i viry psané ve vyšších programovacích jazycích, neboť ty by bylo nutné krokovat opravdu do značné hloubky. Heuristickou analýzu je v zásadě možné uplatnit i na MBR, bootovací sektory, na obsah paměti a nebo na vektory přerušení, čehož také některé programy využívají. Problém je v tom, že pro kód uložený na těchto místech je nutné použít úplně jiné hodnocení než na běžný kód v souborech (např. není překvapující, když kód v boot sektoru používá přímé čtení pomocí BIOS). Též by bylo možné heuristicky

vyhledávat makroviry, ale v jejich případě by nešlo v pravém smyslu o "heuristickou analýzu".

Tato metoda umožňuje najít neznámé viry, ale může také propustit zcela zjevný virus. Virus může být také odhalen ještě před jeho infiltrací do systému. Její nevýhodou je naopak přílišná pomalost a poměrně veliké procento falešných poplachů. Je třeba k ní přistupovat jako k metodě, která hlásí velké procento falešných poplachů. Cena "vážně pojatého" falešného poplachu totiž v rozsáhlé organizaci může snadno převýšit i škody napáchané vlastním virem.

Heuristická analýza je nepochybně zajímavou metodou, která může přinést mnoho zajímavých výsledků. Neměla by se přeceňovat a zatím by měla být používána jako doplňková – tedy ne jako hlavní metoda detekce virů. Nehledě na to, že bylo dokázáno, že není možné v reálném čase provést dostatečně podrobnou analýzu. Je možné ji provádět také rezidentně. V takovém případě se obvykle analyzuje každý spouštěný program.

Monitorování podezřelých činností se provádí pomocí rezidentních programů: monitorují všechny důležité činnosti typické pro viry, které mohou nějak ohrozit bezpečnost systému. Zejména takové činnosti, jako je zápis do spustitelných souborů COM a EXE, přímý přístup na disk, pokus o formátování a pokusy o přejmenování či smazání souboru COM a EXE. Zdaleka ne každý zachycený pokus však znamená činnost viru – spíše naopak. Jelikož je při použití této metody nutné nad každým zachyceným pokusem přemýšlet, zda jde o pokus oprávněný, je to metoda vhodná pouze pro zkušené uživatele.

Touto metodou můžete nejen zachytit neznámý virus, ale i pokusy trojských koňů a případně i vlastní omyly. Zachytíte tak virus ještě před jeho infiltrací do systému. V zásadě by těmito metodám neměla uniknout činnost žádného viru. Lze je zaměřit i proti makrovirům. Měli byste si však uvědomit, že v takovém případě budete vídat varovnou hlášku při každém pokusu o uložení dokumentu.

Speciální metody detekce virů

Existuje ještě několik technik, které se dají použít k detekci virů. Zajímavá jen jedna metoda – detekce přítomnosti rezidentních souborových virů pomocí "udiček". Při testu pomocí udiček jsou na disku vytvořeny soubory COM a (nebo) EXE. Jsou s nimi potom prováděny rozličné operace, jako je spouštění, zápis do nich, kopírování apod. Pokud se po těchto operacích změní jejich obsah, je velice pravděpodobné, že systém napadl nějaký rezidentní virus. Je také možné použít jako udičku pro detekci rezidentního bootovacího viru disketu. Program nejdříve na disketu zapíše standardní bootovací sektor. Poté provádí s disketou různé operace, a je-li po těchto operacích jiný bootovací sektor, než byl na začátku, je pravděpodobně na počítači přítomen bootovací virus.

Tato metoda je schopna detekovat pouze rezidentní programový virus, resp. rezidentní bootovací virus, který je už přítomný v systému. Pokud však test udiček dopadne negativně, není možné z toho usuzovat, že počítač je prostý virů! Nejenže určitá nemalá část souborových virů není rezidentní, ale ne každý virus se množí vždy. Viry se mohou množit za rozličných podmínek – ať už jde o podmínky vázané na čas a datum nebo na délku souboru, zaplnění diskety, určitý čas a datum u souboru, anebo jsou prostě náhodné. Teoreticky by bylo možné na podobném principu detekovat i makroviry, ty je však snazší detekovat jinak.

Stealth techniky

Stealth viry svého času antivirovým firmám pěkně zamotaly hlavy. Připomeňme si, že jde o speciální skupinu rezidentních virů, které při žádosti programu (i antivirového) o zjištění údajů, které by vedly k odhalení viru, vrátí původní údaje. Otřepaným příkladem stealth techniky je, že si virus zálohuje původní podobu bootovacího sektoru (resp. MBR). Při žádosti nějakého programu o obsah bootovacího sektoru je tato žádost přesměrována – vrácena je pak původní kopie bootovacího sektoru. Obdobně je souborový virus schopen "odinstalovat" se ze souboru, který se nějaký program snaží otevřít. Po uzavření souboru je soubor opětovně infikován. (Proto se paradoxně některé stealth viry ze souborů "odinstalují", když se je snažíte zkomprimovat do nějakého archivu, např. programem ZIP). Mohou tak unikat jak konkrétním, tak i obecným antivirovým technikám. V paměti se však stealth viry příliš skrývat nemohou, a proto je tam mohou konkrétní (i některé obecné) antivirové techniky odhalit. Stealth techniky není také možné používat na všech operačních systémech. Je třeba ještě zdůraznit, že stealth viry se mohou takto skrývat jen v okamžiku, kdy jsou samy přítomny v paměti. V okamžiku, kdy nejsou v paměti přítomny, je možné je detekovat stejně "snadno" jako jiné viry.

Antivirové firmy se snažily proti stealth virům bojovat různým způsobem – a nutno podotknout, že na tomto poli ještě antivirové firmy značnou převahu nezískaly. Obecně se snaží antivirové programy pomocí technik "tunelování" zjistit původní (BIOS) rutiny pro manipulaci s pevným diskem (zejména přerušeni 13h). Pro načítání skutečných informací o disku se pak používají tyto původní detekované rutiny, které nemohou být ovlivněny virem. Čím úspěšněji antivirové programy odolávají virům a čím lépe jsou schopny se tunelovat, tím jsou naopak méně kompatibilní a mohou způsobovat problémy. Další cestou je použití přímého přístupu k řadiči disku, ale opět narážíme na problémy s kompatibilitou různých řadičů disků.

Nejlepší (v podstatě dokonalou) antistealth technikou je tedy odstranění stealth viru z paměti před provedením antivirového testu. To se provede nejlépe tzv. "tvrdým resetováním" (Ctrl-Alt-Del nemusí na všechny viry platit) a nabooteváním z čisté systémové diskety. Bohužel – s příchodem nových operačních systémů začíná být bootování z disket komplikovanější a u některých systémů už bootování z diskety není možné vůbec. Konkrétně není možné nabootevat z diskety Windows NT a při bootování do DOS a použití souborového systému NTFS se nedostanete na pevný disk.

Antivirový hardware

Protože se software dá softwarem vždy (a často poměrně dobře) obejít, nabízí se myšlenka chránit počítač pomocí kombinace hardwaru a softwaru. Většinou jde o "karty", které se zasouvají do hlavní desky počítače. Tyto produkty nejsou určeny speciálně proti virům – obvykle jsou určeny obecně k ochraně dat i před nechtěným nebo neúmyslným poškozením. Cílem těchto produktů je zabránit zápisu na disk (mimo vymezené oblasti). Tyto oblasti mohou být vymezeny jako části disku, ale chytřejší systémy mohou chránit i jednotlivé soubory podle jejich příslušnosti k adresáři anebo podle jejich typu. Tyto produkty obvykle vyžadují autentizaci uživatele a podle toho mu přidělí pravomoci, neboť na systému musí vždy existovat nějaký "administrátor" s neomezenými pravomocemi. Některá z těchto řešení umožňují i takové ochrany, jako je znepřístupnění disketových jednotek, šifrování, zaznamenávání činností jednotlivých uživatelů apod.

Jejich výhodou je, že jsou aktivní už v okamžiku zavádění operačního systému – tedy dříve, než je zaveden jakýkoli software. Objektívni výhodou těchto řešení je, že se běžné viry nebudou schopny v takovém prostředí (při zachování určitých pravidel) nekontrolovaně šířit a škodit.

Největším problémem antivirového hardwaru je jeho cena. Při velkém nasazení (díky multilicenčním slevám) může často i mnohonásobně přesáhnout cenu softwaru. Nehledě na to, že tyto prostředky často brání počítač tak důkladně, že znesnadňují jeho používání. Některé programy, které přímo zapisují do svého těla, potom nejsou schopny na takovém počítači pracovat. Jejich další obecnou nevýhodou je značná závislost na použitém operačním systému. A nakonec – téměř každou hardwarově-softwarovou ochranu lze (se znalostí o její konstrukci) obejít; onu magickou 100% jistotu vám stejně nepřinese (zatím jsem viděl pouze jediný prostředek, u něhož si nedovedu představit, jak by se dal "obejít"). Dosud se nenašel žádný virus, který by se snažil některou z takovýchto ochranných opatření obejít.

Většina nových BIOS obsahuje i ochranný prvek z této kategorie – zvaný často "Boot Sector Virus Protection". Tato ochrana chrání uživatele před zápisem do bootovacího sektoru. Jak konkrétně se BIOS zachová při pokusu o zápis do bootovacího sektoru, však závisí na typu použitého BIOS (obvykle se BIOS snaží uživatele zeptat). Tuto ochranu je v zásadě možné používat (pracuje-li korektně), ale před každým větším zásahem na disk (např. instalaci nového operačního systému) je třeba tuto ochranu vypnout. Ostatně často je možné tuto ochranu programově obejít přímým zápisem na řadič disku.

Odstraňování virů

Nyní bych si dovolil čtenáře varovat. Nezkušení uživatelé často při odstraňování virů nadělají více škody než užitku a jejich řádění je pak pro počítač horší pohromou než řádění viru. Proto si na viry zavolejte raději odborníka (anebo se s ním alespoň poraďte), aby nevzniklo více škod, než kolik je nezbytně nutné. Před odstraňováním viru je také nanejvýš vhodné, abyste si zjistili, zda nejde o falešný poplach. Odborníka volejte i v případě, kdy vám antivirový program nabízí odstranění viru. Při nešetrném odstraňování viru z disku (buď antivirovým programem) může totiž dojít i ke katastrofě, jakou je ztráta dat na disku. Kdo se setkal s virem "One Half", ví o čem mluvím.

Pro méně zkušené uživatele by se dal postup odstraňování virů shrnout takto: přesně opsat (vytisknout) hlášku antivirového programu, korektně ukončit všechny aplikace, vypnout počítač a zavolat odborníka.

Je třeba, aby si uživatel uvědomil, že před každým odstraňováním viru musí nejdříve odstranit virus z paměti (je-li rezidentní). Teprve potom může odstraňovat viry z bootovacího sektoru anebo ze souborů. Obecně musí pro odstranění každého viru z paměti fungovat postup "tvrdého resetování" pomocí tlačítka "Reset" (není-li toto tlačítko, použijte vypnutí a zapnutí počítače). Potom je nutné zavést operační systém z neinfikované systémové diskety.

Možnosti odstraňovacích programů

Bootovací viry (případně viry v MBR) lze poměrně dobře odstraňovat automaticky. Nejlepší je, má-li antivirový program někde zálohovanou kopii těchto objektů a při odstraňování ji použije k náhradě. Ani vygenerování čistého bootovacího sektoru disket by nemělo činit antivirovým programům problém ("zálohování" čistých bootovacích sektorů disket je sice možné, ale je to trochu zbytečný luxus). Jisté nebezpečí při generickém odstraňování virů (obecném odstraňování bez znalosti konkrétních vlastností viru) šifrujících obsah počítače zde však je. Pokud by byla v antivirovém programu chyba anebo byste použili pro rekonstrukci kopii MBR (boot sektoru) jiného disku, mohli byste o svá data přijít.

Viry z programových souborů lze automaticky odstranit trojím způsobem (za čtvrtý můžeme považovat smazání celého souboru i s virem). Prvním způsobem je "léčení podle známých vlastností konkrétního viru". Některé viry je možné ze souboru bezzbytku odstranit a soubor uvést do původního stavu, jiné viry nikoli. Takovým virem "nabořený" program může provádět nedefinovatelné činnosti. Tuto metodu je možné použít jen u některých, a to známých virů. Druhou cestou je "heuristické odstranění virů". To znamená heuristické nalezení těla viru v programu a jeho odstranění. Jde o cestu sice zajímavou a lze ji využít i na neznámé viry, ale není příliš bezpečná. Takto "částečně vyléčený soubor" se může jevit antivirovým programům jako zcela zdravý, ale zbytky těla viru mohou provádět "zajímavé věci". Jelikož tyto dvě metody nejsou v žádném případě bezpečné, důrazně se jim doporučuji vyhnout a používat je jen jako poslední možnost v okamžiku, kdy nejsou k dispozici záložní kopie. Třetí možnost, která je uspokojivě bezpečná, je rekonstrukce souboru na základě informací uložených při testu integrity. Pokud se antivirovému programu nepodaří z dostupných informací soubor zcela rekonstruovat, rekonstrukci vůbec neprovede. Tato metoda "léčení" je také nabízena všemi seriózními programy a má velkou šanci zcela uvést soubor do původního stavu (běžně se uvádí více než 50% – záleží na antivirovém programu a viru). Dobře jdou ze souborů odstraňovat makroviry. Makrovirus může být ze souboru zcela odstraněn či pouze znehodnocen tak, že bude příslušnými programy ignorován.

Odstraň si sám...

Pokud antivirovým programům nedůvěřujete, máte možnost odstranit některé viry sami. Některých virů se tak můžete zbavit, i když nemáte po ruce žádný antivirový program. Některé postupy zde ve stručnosti popíši.

Bootovací viry lze odstranit poměrně snadno a spolehlivě ručně. Dovolím si zde však zopakovat varování před odstraňováním šifrujících virů (např. viru One Half), neboť po jejich odstranění se už nemusíte dostat k datům. Popíši zde ve stručnosti postupy, jak odstranit virus podle toho, kde přesně je umístěn:

MBR pevného disku: Z MBR pevného disku je možné virus odstranit poměrně bezpečně pomocí příkazu MS-DOS "fdisk /mbr" (od verze 5.0). Tento příkaz přepíše řídicí program v MBR a tím odstraní z MBR virus.

Bootovací sektor diskety: Z bootovacího sektoru diskety je možné virus odstranit přeformátováním diskety. Data je možné z diskety zachránit prostým zkopírováním veškerého obsahu na disk před vlastním formátováním. Pro formátování pod DOS je nutné použít "poctivé" formátování s přepínačem "/u"!!! (U systémové diskety stačí znovu zkopírovat systém – v DOS příkazem "sys a:").

Bootovací sektor pevného disku: V bootovacím sektoru pevného disku se viry neobjevují příliš často. Z bootovacího sektoru logického disku s operačním systémem je možné virus odstranit opětovným zkopírováním operačního systému na disk. To se v případě DOS nebo Windows 95 provede příkazem "sys c:" (v případě Windows 95 je nutno mít nabootováno ze záchranné diskety pro Windows 95). Z bootovacího sektoru disku, na němž není operační systém, je možné virus ručně a dokonale odstranit pouze přeformátováním (s parametrem "/u"). Jelikož je tato metoda příliš drastická, je možné na disk zkopírovat např. operační systém DOS a poté z takového disku odstranit systémové soubory *io.sys*, *msdos.sys*, *command.com* a případně další, které si systém přinesl. Tato metoda není sice "čistá", ale uspokojivě funkční.

Ruční odstranění souborových virů je věc téměř nemožná. Proto v takovém případě nezbyvá než začít hledat v záložních kopiích a obnovovat...

Jelikož makroviry mohou pracovat na mnoha různých principech, těžko lze popsat obecný popis na odstranění libovolného makroviru. Odstranění makroviru spočívá v odstranění všech maker (kromě těch, které znáte a o nichž víte, že nepatří k viru) ze všech (infikovaných) dokumentů a šablon. Mezi šablonami má zvláštní postavení šablona "normal.dot" ("Normální", resp. "Prázdný dokument"); je předkem všech ostatních šablon a dokumentů a její makra mohou používat všechny dokumenty (proto je také obvykle hlavním hostitelem makroviru). Základní problém však spočívá v tom, odkud makra odstranit nejdříve – odstraníte-li nejdříve makra z "normal.dot", zůstane šablona po otevření prvního infikovaného dokumentu infikována. Při opačném postupu (tj. odstranění maker nejdříve z dokumentů) mohou makra z šablony "normal.dot" takto vyčištěný soubor před uložením ještě infikovat. Jeden z postupů je, že se odstraní makra z dokumentů i ze šablon najednou. Druhý možný postup spočívá ve vyčištění "normal.dot" a jeho ochránění proti zápisu – např. atributem "pouze čtení" (read-only) – a následném čištění souborů.

Jak vybírat antivirový program

Důležitým kritériem při výběru je rozsah funkcí. Jaké funkce by měl určitě každý antivirový program poskytovat, by mělo vyplývat z tohoto článku. Dalším kritériem by měla být snadnost obsluhy a kvalita dokumentace. Jelikož databáze virových sekvencí poměrně rychle zastarává, zajímejte se také, jakým způsobem a za jaké poplatky je možné získávat aktualizované databáze.

Pokud jste při práci s počítačem odkázáni pouze sami na sebe, zajímejte se také o snadnost instalace a konfigurace programu a o možnosti technické podpory. Rozhodně nemá cenu pátrat po tom, kolik virů je který program schopen detekovat. A to nejen kvůli minule popsanému pravidlu 99/1, ale i kvůli tomu, že některé firmy počítají každou variantu viru jako nový virus a jiné ne.

Nezapomeňte také, že většina antivirových programů je na internetu k dispozici zdarma v nějaké "omezené" verzi.

Atlas virů

Jestliže se hodláte zabývat virovou a antivirovou problematikou podrobněji, bude vás jistě zajímat program VSUM. Obsahuje totiž v hypertextové podobě popisy mnoha různých virů. V tomto popisu naleznete kromě strohých technických údajů i různé zajímavosti o viru – podmínky aktivace škodlivé činnosti, vedlejší účinky, země původu apod. Viry jsou zde zařazeny podle mnoha různých kategorií – jednak abecedně podle jména, dále podle dne aktivace, země původu, délky (o niž prodlužují programy) a ještě dalších kategorií. V českém jazyce jsou některé viry popsány v programu AVG, v dokumentaci k programu AVAST! (a AVAST32) anebo v některé dále uvedené literatuře.

Závěrem

Účelem tohoto dvoudílného seriálu nebylo zastrašit čtenáře ani zvýšit obrat antivirových firem. Účelem bylo upozornit čtenáře na možnosti a nebezpečí, která tato problematika skýtá. Účelem bylo poučit čtenáře, že proti virům není v žádném případě bezbranný a že proti virům se mů- že účinně bránit. A navíc by měl čtenář vzít v úvahu, že ochrana dat je sice nákladná, ale vyplatí se.

Martin Beran

Literatura:

1. Baudiš P., Zelenka J.: Antivirová ochrana, Plus 1996.
2. Atestační středisko Relsie: Metodika pro testování antivirových programů, 2. verze, 1996.
3. Látal I.: Ochrana informací, dat a počítačových systémů, Eurounion 1996.

Autor:

Martin Beran

Rubrika:

Magazín

Vydání:

729329 - 729358