TVORBA PROTIVIROVÝCH PROGRAMŮ A OCHRANA PROTI VIRŮM

Ing. Belaban

1. Počítačové viry

Vzhledem k velkému rozšíření počítačů standardu IBM PC XT/AT u nás, dochází zde, pochopitelně, i k velkému oběhu počítačových programů. A tato cirkulace programů přináší zcela nevyhnutelný důsledek - velké šíření počítačových virů. A navíc je zde patrná nedostatečná informovanost uživatelů výpočetní techniky o možných následcích činnosti virů a z toho pramenící podceňování nebezpečí nákazy.

Zcela obecně lze říci, že počítačový vir je program, část programu nebo upravená součástka počítače. Cílem počítačového viru je škodit. Lze odlišit viry, které škodí minimálně, např. po obrazovce občas přeběhne nahulatá mlečna, a viry, které ničí programy, data, ale i součástky počítače.

2. Historie a rozdělení počítačových virů

Myšlenky o počítačových virech jsou pravděpodobně stejně staré jako počítače. První počítačové viry na velkých počítačích se vyskytly v USA okolo roku 1972, první publikace o těchto virech jsou z let 1973 - 1974. Ale teprve rozšíření počítačů standardu IBM PC přineslo velký rozmach virů, protože tyto počítače jsou pro šíření virů takřka ideální. První viry byly jednoduché, ale v posledních letech se objevují velice důkladné viry. Taktéž lze říci, že okolo roku 1986 vznikají první Hardviry (viry, poškozující součástky počítače).

V dnešní době je natolik dobrá dokumentace o počítačích, že není problémem napsat nový nebo modifikovat starý vir ani pro člověka bez hlubších programátorských znalostí.

Počítačové viry lze rozdělovat podle několika hledisek. Pro naše účely je rozdělíme do několika skupin.

2.1 Rozdělení virů podle původu

Rozdělení virů dle původu znamená, že viry budou rozděleny do skupin, s přihlédnutím k okolnostem jejich vzniku.

Viry "Hardware"

Tyto viry jsou novinka. Spočívají v tom, že je upravená součástka počítače - např. paměť typu EPROM, takže při výskytu náhodné události dojde ke škodám.

Viry "Ochranné"

Viry, kterými si programátorské firmy samy nakazí svoje meziprodukty - dosud nehotové verze programů apod. Tyto programy, ilegálně okopírované, mohou, zpravidla po nějakém datu, škodit.

Viry "Pirátská kopie"

Viry, které se šíří z ilegálně okopírovaných programů. Tyto viry jsou sice v některých zemích zakázány (např. NSR), ale jsou běžně rozšířené.

Viry "Nešťastné"

Jedná se o programy, kde došlo nějakým nešťastným způsobem ke změně kódu, takže program za určitých okolností škodí.

Viry "Klasické"

Nejčastější viry, vyrobené za účelem, aby škodily nebo pobavily a dokázaly autorovi viru, jak je dobrý.

2.2 Rozdělení virů podle způsobu šíření

Základní vlastností virů je šíření. Bez této vlastnosti by viry nemohly existovat.

Viry "Hardware"

Viry, šířící se poškozenými součástkami počítače. V ČSSR dosud nebyly popsány.

Viry "Souborové"

Viry, šířící se tím, že se "přilepí" k souboru a šíří se spolu s nějakým souborem. Tyto viry jsou zároveň zpravidla i "Rezidentní" a jsou nejrozšířenější.

Viry "Diskové"

Viry, které jsou uloženy v nějaké formě na disku a šíří se pomocí disků. Tyto viry jsou zároveň zpravidla i "Rezidentní".

Viry "Síťové"

Šíří se v počítačových sítích. Vzhledem k minimálnímu počtu sítí v ČSSR a ještě menšímu počtu propojených pracovišť u nás zatím nejsou poppsány. Tyto viry jsou zároveň zpravidla i "Rezidentní" i "Souborové" nebo "Diskové".

Viry "Rezidentní"

Jedná se výše popsané viry, které se usadí v paměti a rozmnožují se nějakým způsobem - např. nakazí spouštěný program, nakazí disketu apod.

Viry "Trójský kůň"

Jde o zcela speciální skupinu virů. Oproti jiným virům mají zcela specifickou vlastnost - nešíří se nebo se šíří až jejich potomci. V podstatě jde o to, že program je napadený nebo je už vyroben jako zavirovaný. Virus v něm se dlouhé týdny, měsíce a často i roky neprojevuje. Až po dlouhé době může (ale nemusí) nakazit některý další program svou modifikací. A ještě po delší době začne škodit - třeba smaže několik stop pevného disku. Programy takto napadené se velice těžko vyhledávají, většinou se nedojde k žádnému výsledku.

2.3 Rozdělení virů dle způsobených škod

Viry se odlišují především svými škodlivými účinky. Zároveň platí, že jeden vir může škodit více způsoby a hlavně to, že může škodit pouze někdy. U některých typů virů lze hovořit o výjimečném působení. Viry škodí buď pouze u příležitosti některého data, při nějaké jiné příležitosti (dvacáté zavedení viru, spuštěná virem v jeho kódu apod.) nebo zcela libovolně. Viry mohou škodit na různých typu počítače.

Viry "Neškodné"

Viry, které způsobují naprosto nepostřehnutelné změny počítače - občas více přeběhne po obrazovce monitoru, občas počítač zapípá, systémová hlášení je nahrazena humorným textem, občas může počítač chrčet, abychom mu dali svačinu. Jakmile ji dostane (například SUŠENKA), pokračuje dál. Rovněž sem patří viry, které zpomalují běh programů nebo občas způsobí zhroucení systému (kterému příznak je přeplněný systémový zásobník).

Viry "Soft-ware"

Viry, poškozující nebo zcela mažící soubory, ať už s daty nebo kódem.

Viry "Diskové"

Poškozují zavaděč, přidělení tabulky, adresáře, označují bloky disku jako vadné apod.

Viry "Hardware"

Viry, poškozující součástky počítače. Např. zničí monitor, vyjíždí s hlavou mechaniky z vodících tyček, poškodí obvody v/v, vydá povel ke zpětným krokům v tiskárně - značkaný papír, opakují několikrát přístupy na disk - opotřebení disku, rozkmitají hlavy pevného disku tak, že klepnou o povrch a tím zničí disk atd.

3. Podmínky, které mohou vyžadovat viry pro svoji činnost

Většina virů pochopitelně vyžaduje určitý operační systém počítače a viry, které přímo používají porty, vyžadují i jistou kompatibilitu s originálem IBM PC. Většina virů na PC vyžaduje systém MS-DOS, verzi zpravidla vyšší jak 2.0, resp. 3.0. Některé se ale nemohou šířit ani pracovat ve verzi např. 4.1 (vir, nazvaný 3k), protože systém používá přerušení, jaké vyžaduje vir a z pohledu viru je tedy systém neustále zavirovaný. Viry, které osahávají přímo hardware počítače, nemohou fungovat v počítačích odlišné stavby jak originální IBM PC. Např. vir, který monitoruje port klávesnice nebude fungovat na prvních počítačích TNS - AT, protože u těchto starších PC je pro klávesnici užit port 60h, nikoli jak u novějších počítačů port 64h.

Obecně lze říci, že proti šíření viru se lze chránit pouze zalepením otvoru na disketě nebo hardwarovou úpravou pevného disku (vyvedení signálu k zápisu na vypínač).

4. Ochrana proti virům a její význam

Dokonalá ochrana před počítačovými viry je jenom jedna - počítač nekupovat. Pokud ho už máme koupený, prodat ho. Ale vážně - dokonalá ochrana neexistuje. Ochrana disket je pouze zalepený otvor proti nahrávání. Tím je hardwarově zabezpečeno, že na disketu nelze zapisovat. Ochrana pevného disku je pouze vyvedení signálu k zápisu na vypínač. Toto jsou druhy absolutní ochrany. Další metody lze rozdělit na tři druhy - ochrana při šíření, po šíření a karanténním počítačem a samozřejmě opatrnou instalací - viz další kapitoly.

4.1 Ochrana při šíření a činnosti viru

Tato ochrana spočívá v tom, že hlídáme změnu přerušovacích vektorů, monitorujeme některé činnosti, máme vlastní COMMAND.COM, který hlídá přístupy na disk atd. Výhodou tohoto pří-

stupu je to, že odhalí vir ještě před rozšířením, takřka okamžitě. Jeho nevýhodami je především nekorektnost k rezidentním programům (ale i jiným) a především nedokonalost. Pokud je vir "chytrý" a užívá přímo portů, není možno ho chytit, nepřeprogramujeme-li řadič disku.

4.2. Ochrana po šíření

Tato ochrana spočívá v kontrole souborů, ale i zaváděčů disků pomocí mnoha existujících programů. Patřím mezi zastánce této metody. Sice se virus může rozšířit, ale pomocí kontrolních programů se zjistí a pomocí toho, že víme, který program byl napaden, můžeme si nechat vytvořit nebo napsat protivirový program, čímž můžeme ničit viry kdykoli, pokud se objeví, neboť nemusíme vždy vědět, který z programů je program typu trójský kůň. Je zde jisté riziko, že program začne ničit ještě než bude nalezen, ale vzhledem k tomu, že většina virů se šíří okamžitě, přijdeme na něho při dalším volání kontrolního programu, zpravidla druhý den.

4.3 Ochrana pomocí karanténního počítače

Tato ochrana spočívá v tom, že veškeré nové programy nejprve instalujeme na jednom počítači, kde se s ním intenzívně pracuje - zpravidla po nějakou lhůtu. Pokud nedojde v této době k nějaké závadné činnosti počítače, předpokládáme, že je program nezávadný a instalujeme ho i na ostatních počítačích. Tento postup je zárukou, že většina virů se "nachytá" a začne se alespoň šířit - poznáme prodlužování nebo poškozování souborů. Doba, kdy se program testuje, by měla být dostatečně dlouhá, aby se vir mohl projevit a zároveň co nejkratší, protože je samozřejmě škoda nechávat nové kvalitní programy ležet na karanténním počítači. Já se přimlouvám za dobu 14 dnů až 1 měsíce. Delší nemá smysl, není-li alespoň jeden rok, což je samozřejmě neúnosné. A pokud máme rafinovaný program typu "Trójský kůň", stejně

se projeví přinejmenším za rok od svého vzniku (samozřejmě některé i okamžitě). Lze říci, že pokud je dodržován určitý režim (přenášet soubory pouze ve zdrojovém tvaru, nejlépe nepřenášet nebo přenášet pouze na zalepených disketách směrem do karanténního počítače), jde o poměrně dobrou ochranu.

4.4 Ochrana pomocí imunizace

Tato ochrana spočívá v tom, že využijeme vlastnosti virů - každý vir zpravidla má nějakou "značku" na souboru, který už nakazil, aby ho nenakazil víckrát. Např. nastaví čas na nějakou hodnotu apod. Tuto ochranu já osobně nesnáším a zavrhuji, neboť má jenom jednu a krátkodobu výhodu - imunizovaný soubor nelze nakazit příslušným virem. To nám ale nezaručuje, že zavirovaný soubor nepřežívá v nějakém souboru a projeví se až v nejméně vhodném okamžiku. A předáme-li někomu takto "ověřený" program, u kterého se změní datum, má vir v počítači a netuší odkud.

4.5 Pravidla pro zmenšení rizika nákazy

1. Každý program, než ho instalujeme, nejprve prohlédneme, zda není nakažen některým virem.
2. Programy vždy přebíráme od někoho, koho dobře známe a kdo nám úmyslně nedá zavirovaný program.
3. Pokud je to možné, soubory denně kontrolujeme pomocí některého kontrolního programu.
4. Mezi počítači a pracovišti přenášíme pokud možno pouze zdrojové soubory na zalepených disketách.
5. Důkladně archivujeme veškeré důležité soubory.
6. Máme-li velice důležitá data, je nutno je zálohovat systémem sudá - lichá, tj. máme vždy dva archivní soubory - poslední a předposlední, přičemž je nutno je kontrolovat. (Pozn. lze doporučit větší počet kopií, zpravidla 4 - 6.)
7. Při jakékoli změně nebo podezřelém chování vyrozumíme někoho se znalostí protivirové problematiky. Počítač vypneme a nezapínáme!

5. Jak poznáme zavirovaný počítač

Základní problém zní - jak poznáme, že máme v našem počítači vir. Obecně platí, že každý vir je jiný a má i jiné příznaky, takže nelze přesně napsat, že když se stane to a to, je zcela určitě v počítači vir. Vir zpravidla způsobí řadu různých problémů. Je důležité odlišit, co mohla udělat chyba počítače a co mohl udělat vir. Tady platí, že více nezávislých příznaků tvoří příznak viru - např. chyba počítače určitě neprodlouží soubor typu .COM a současně nezničí FAT na disketě. Mezi nejtypičtější příznaky patří :

a) Programy běží pomaleji, než je obvyklé.
b) Programy se zavádějí déle, než obvykle.
c) Systém se snaží o přístup na zalepenou disketu, přestože nemá zapisovat na disk.
d) Bezdůvodně se pracuje s diskem.
e) Nepracují nebo pracují s chybami rezidentní programy.
f) Je méně volné paměti než je obvyklé.
g) Prodlužují se soubory.
h) Nepracují některé programy, které dříve pracovaly.
i) Jsou poškozeny záznamy na disku nebo jejich části.
j) Poškozené soubory.
k) Nesmyslné hlášení systémů nebo programů.
l) Neobvyklá činnost programů nebo počítače.
m) Ubývají nebo přibývají soubory.
n) Kontrolní programy hlásí chyby.
o) Přibývá chyb na discích.
p) Zvětšuje se počet vadných sektorů na discích.
q) Ubývá volného místa na disku, ačkoli se nezvětšuje počet ani velikost souborů.

Takže lze říci, že když se objeví více jak jeden příznak nebo se objeví jeden vícekrát, jedná se s největší pravděpodobností o vir. V tomto případě doporučují okamžitě vypnout počítač a konzultovat s někym, kdo se vyzná ve virové problematice.

Pro větší odborníky navrhuji tento postup :

a. Provedu RESET počítače a nahraji URČITĚ nezavirovaný systém.
b. Snažím se zjistit, který soubor je zavirovaný (je nositelem viru). Zkontroluji především COMMAND.COM (např. u MS-DOS 3.30 má délku 25 308 byte). Není-li změna, provedu kontrolu souborů v adresáři, který byl v okamžiku projevu příznaku aktuální, dále provedu kontrolu hlavního adresáře a systémového adresáře. Není-li nikde změna, postupuji zpravidla dle konkrétních okolností.
c. Zpravidla tímto způsobem (je-li opravdu v počítači vir) odhalím soubor, jež je delší, tj. je zavirovaný. Tento soubor si přehraji na disk, řádně označím a další kroky už dělám na počítači bez pevného disku.
d. Pokusím se program spustit. Pokud běží - je vyhráno, vir je chycen.
e. Nahraji do adresáře známé krabší soubory obou typů a sleduji množení viru - to jen pro pořádek.
f. Začnu prohlížet napadený program programy AFDPRO nebo SYMDEB a.l. Opíšu si úvodní sekvenci (v hexadec. kódu). Tím získám typickou úvodní sekvenci. Toto provedu u více programů - můžou být různé výsledky (např. vir 2000). Při tvorbě protivirového programu potom budu testovat např. 24 byte a povolím max. 4 rozdíly.

   a 2. Hledám typickou dekódovací smyčku, tj. místo, kde se dekóduje (ale nemusí) původní část programu. Tato leží zpravidla v místě, kam přijde program po testu na verzi MS-DOSu, pokud mu předhodíme verzi patřičně nízkou (1.0). Ale jsou viry (2000), kde se k této smyčce musím prokousat skoro celým programem, a to ještě přes přerušení 0. Program totiž na sebe přesměruje přerušení 0 a potom vyvolá dělení nulou, takže předá řízení další své proceduře.
g. Napíšu odvirovací program, který řádně vyzkouším na několika místech a několika různých programech.

6. Budoucnost a viry

Je jisté, že se virů nikdy zcela nezbavíme. Bude zřejmě nutno naučit se pracovat tak opatrně, abychom viry nešířili sami

nebyli ohrožení jejich činností. To znamená důsledná kontrola všech programů, programy kontrolních součtů atd.

Přesto jsem optimista a domnívám se, že se opatrnou prací dají důsledky virů potlačit natolik, že nedojde ke škodám na programech ani datech.