

Ochrana proti počítačovým virům a spamu

Datum: 8.1.2004

Vypracoval: Kamil Gric, třída 7.A

Ochrana proti počítačovým virům a spamu.....	1
Krátký úvod.....	1
Počítačové viry obecně.....	1
Druhy virů.....	2
Boot viry	2
Souborové viry	2
Multipartitní viry	2
Makroviry	2
Stealth viry	2
Polymorfní viry	2
Rezidentní viry	2
Trojské koně.....	2
Destruktivní trojani.....	3
Password-stealing trojani.....	3
Drooper	3
Backdoor.....	3
Červi.....	3
Speciální případy.....	3
Ochrana před viry.....	3
Techniky „stopování“ viru.....	3
Vyhledání v databázi.....	3
Heuristická analýza.....	3
Kontrola integrity.....	4
Rezidentní sledování	4
Konkrétní tipy na zajímavé antiviry.....	4
Spam.....	4
Co je to?.....	4
Jak se bránit?.....	5
Prevence!.....	5
Pasivní ochrana.....	5
Aktivní ochrana.....	5
Závěrem.....	5
Zdroj informací.....	5

Krátký úvod

Jak jsem zmiňoval v prvním projektu zabývajícím se bezpečností PC, druhů nebezpečí, která našim plechovým miláčkům hrozí, je velké množství - a právě za obecně nejobávanější považujeme (bezpochyby oprávněně) počítačové viry. Ochrana proti nim však může být mnohem jednodušší, než v případě klasických hackerských útoků. Moje dnešní seminární práce tak pojednává o jejich nebezpečí i způsobech ochrany. Velká část je pak také věnována spamu, tedy nevyžádané poště, která se s rozmachem internetu stává stále ožehavějším tématem.

Počítačové viry obecně

Není pochyb o tom, že viry jsou v současné době zřejmě největší hrozbou internetu. Jejich minulost však sahá již do dob, kdy byl internet (tak, jak ho známe v dnešní době) pouze v plenkách. Název virů vznikl podle shodně pojmenovaných biologických organismů – stejně jako ony jsou i některé počítačové viry schopny snadné sebe-replikace a vlastního množení – nejen v tom však tkví jejich nebezpečí. Zatímco v minulosti byly počítačové viry v běžných domácnostech přenášeny pomocí disket „z počítače na počítač“, s rozšiřujícím se propojením PC do sítí i jejich připojení na internet jejich hrozba i útoky sílí. V následujících odstavcích rozebírám nejčastější typy virů a později také možnost ochrany proti nim, za pomoci nejdostupnějších a nejužnávanejších prostředků.

Druhy virů

Rozdělení virů do několika velkých skupin je možná složitější, než se na první pohled zdá – já proto použiji jedno z uznávaných dělení na klasické počítačové viry, trojské koně, backdoor aplikace, červy a zbylé případy.

Viry

Nejznámější oblast, která zahrnuje viry, se kterými se běžně setkal snad každý z nás – její historie sahá až do roku 1986, který je všeobecně označován za období vzniku prvního viru.

Boot viry

Známy druh virů, který nenapadá konkrétní soubor, nýbrž systémové (boot) oblasti disku. Jedná se o jeden z nejčastějších druhů virů, které se v minulosti šířily zejména jako součást klasických disket. Šíří se jednoduchým způsobem – po restartu počítače a zavádění systému z disketové mechaniky se vir sám spustí a napadne systémové oblasti. K jeho spuštění však musí být zaveden start systému z diskety, tohoto nastavení se lze jednoduchou změnou BIOSu zbavit.

Souborové viry

Jak již napovídá jejich název, napadají konkrétní soubory – přesněji programy, tedy soubory obsahující prováděný kód. Právě tento kód přepíše svou vlastní částí, mohou změnit jeho velikost i chování a aktivovat operace, v nichž tkví jejich nebezpečí – například smazání části disku atd., samozřejmě v závislosti na konkrétním viru.

Multipartitní viry

Kombinace obou předcházejících možností, tyto viry tedy napadají soubory i systémové oblasti disku a těží z výhod tohoto spojení.

Makroviry

I když jejich jméno mnohým nemusí nic říkat, makroviry jsou dnes nejrozšířenějšími viry vůbec. Mohou totiž tvořit součást datových souborů a využívají tak faktu, že tyto soubory (typicky dokumenty) obsahují také makra. Makroviry jsou často šířeným druhem virů na internetu, dokáží se snadno dále šířit a využívají „důvěřivosti“ lidí – zajímavý popis emailu dokáže mnohého přesvědčit k otevření smrtící přílohy. Více už konkrétní příklad, nalezený v literatuře:

Možnosti jazyka Visual Basic for Applications, ve kterém jsou psána makra v MS Office 97, jsou velmi rozsáhlé a bezpečnost je minimální. V nedávné době se o tom mohly přesvědčit oběti viru W97M Melissa, který při své aktivaci použije dokument, na němž uživatel zrovna pracuje, infikuje jej a rozešle elektronickou poštou na 50 náhodně vybraných adres z uživatelova adresáře. Následky takové akce pravděpodobně nebudou fatální, ale podobný makrovirus může například vykrádat z vašeho počítače důvěrné informace, pracovat s vašimi soubory, spouštět aplikace.

Stealth viry

Typ virů, který dbá na svou „bezpečnost“ a snaží se pomocí stealth technik obelstít antiviry – pokud je v paměti, snaží se ovládat a ovlivňovat práci systému a tím překládat antiviru nesprávná data, která znesnadňují jeho objevení.

Polymorfní viry

Specifický druh virů, který se od ostatních liší schopností měnit vlastní kód a tím znesnadnit antivirovým programům jeho detekci.

Rezidentní viry

Typicky viry, které po svém spuštění zůstávají přítomny v paměti.

Trojské koně

Na rozdíl od virů nejsou tyto viry schopny sebe-replikace, čímž částečně mizí jejich nebezpečí – je tomu však pouze na první pohled. Trojský kůň se v praxi nejčastěji tváří coby samostatný spustitelný EXE program, který však nemá žádnou funkci a za užitečnou aplikaci se pouze vydává – v minulosti se objevily trojské koně v podobě některých antivirových i dalších programů. Trojské koně jsou příkladem škodlivého softwaru (malwaru) a pokud jde o bezpečnost dat, jsou často škodlivější, i když ne tak rozšířené jako viry. Rozlišujeme také několik typů trojských koní:

Destruktivní trojani

Základní a klasická forma trojanů, jejímž cílem je likvidace dat na pevném disku.

Password-stealing trojani

Typicky se jedná o programy kontrolující a zapisující údaje o veškerých stisknutých klávesách na PC, informace pak odesílají svému tvůrci. Šikovný uživatel z nich dokáže vyčíst hodnotná hesla a další údaje.

Drooper

Funguje pouze jako prostředník, kdy po svém aktivování vypouští do PC jiný vir.

Backdoor

Speciální skupina trojských koní, od jejich kategorie se však oddělila především svým nebezpečím. Jedná se o klient-server aplikace, které samy o sobě nemusí být škodlivé – záleží samozřejmě na konkrétním případě, jako vždy však jejich schopností využili lidé také k šíření nebezpečných virů.

Zvláštním typem jsou backdoory, které komunikují s uživatelem za pomoci otevřeného kanálu IRC.

Červi

Vznik pojmu červ se datuje do roku 1989, kdy byl takto označen vůbec první virus tohoto typu. Červi bývají často zaměňovány s viry, ale je mezi nimi diametrální rozdíl. Na rozdíl od nich využívají červi síťových paketů a dále se šíří na další, doposud neinfikované počítače v síti či internetu. Jejich základní ideologií se tak stává využití bezpečnostních chyb v programech (například MySQL) i systému, kterých (jak dobře víme) obsahuje každá verze operačního systému Windows nespočet. Účinnou ochranou tak zůstává pravidelné stahování a instalování všech bezpečnostních záplat pro programy, které aktivně spoluprací se sítí.

Speciální případy

Kromě všech zmiňovaných druhů virů rozlišujeme také několik specifických případů, které se od výše zmiňovaných virů v mnohém liší – přesto, stejně jako ony, představují pro uživatele jasné nebezpečí. Protože důkladnější popis není potřeba (otázku spyware jsem rozebíral v předchozí práci), následuje jen jejich letmé vyjmenování:

- **Spyware**
- **Hoax**
- **Dialer**

Ochrana před viry

Myslím, že výše naznačené způsoby šíření virů i jejich škodlivosti dokazují, o jak ožehavé téma se v případě počítačových virů jedná. Proto věnuji následující kapitolu popisu ochrany před tímto moderním nebezpečím. Základem se samozřejmě stávají antivirové programy, které jsou pro boj s viry primárně určeny a kterým se také v následujícím textu věnuji. Jeho první část je však vyplněna popisem technik, které dokáží vir v systému odhalit, další jsem věnoval popisu zajímavých programů (antivirů), kterými se před nimi můžeme chránit.

Techniky „stopování“ viru

Stejně jako veškeré jiné programy, i antiviry využívají mnoha technik pro odhalení přítomnosti virů v PC. My si je nyní projdeme postupně:

Vyhledání v databázi

Základní metoda, která je založena na speciální databázi virů, které obsahuje každý antivir. Program při kontrole systému prohledává zadané soubory a testuje je na výskyt určité posloupnosti bytů, která identifikuje vir z databáze. Porovnání s databází je stále nejrozšířenějším a nejspolehlivějším způsobem kontroly, který však s sebou nese jistá rizika – databáze musí být pravidelně aktualizována, jinak celý proces kontroly systému ztrácí smysl. V případě kvalitnějších antivirových programů (například AVG) však update probíhá minimálně dvakrát do měsíce, což by mělo pro ochranu PC před nejnovějšími viry alespoň částečně postačit.

Heuristická analýza

Tato metoda využívá analýzy kódu souboru, hledá v něm tak odlišnosti od standardních souborů, které jsou typické pro viry. Podobný způsob kontroly PC však spolu nese výhody i nevýhody – předností je možnost odhalení doposud do databáze nezanesených virů, spolehlivost heuristické analýzy však není stoprocentní a mnohdy dokáže za vir označit i nenapadený soubor.

Kontrola integrity

Sledování změn v systému, kdy si program po svém prvním spuštění vytvoří databázi souborů na disku – po dalším spuštění kontroluje aktuální stav souborů a využívá faktu, že uložením viru do některého souboru dojde ke změně souboru, kterou je možné detekovat – program však při nalezení změny nedokáže určit, zda-li ji způsobil vir, což může být poměrně velkou nevýhodou. Stejně jako v případě heuristické analýzy, i tato metoda dokáže odhalit doposud neanalyzované a neznámé viry.

Rezidentní sledování

Proces antivirového programu, který průběžně kontroluje prováděné operace na PC a je vždy funkční na pozadí systému. Antivir tak dokáže důsledně upozornit uživatele na spuštění souboru, který je infikován virem a tento proces včas přerušit. Rezidentní štít některých antivirů sleduje také pokusy o zápis do bootovací tabulky PC, podezřelé operace přeruší či dá uživateli na výběr, zda-li zápis do boot sektoru povolí.

Konkrétní tipy na zajímavé antiviry

Bránit se proti virům můžeme samozřejmě prevencí (neotevíráme přílohy u cizích emailů, neinstalujeme žádné podezřelé programy z internetu, vždy kontrolujeme od kamaráda přinesené disky a CD atd.), základní a nejrozšířenější metodou je však využití specializovaných programů, tzv. antivirů.

Antiviry samozřejmě kombinují všechny výše zmíněné metody kontroly systémů na přítomnost virů, některé využívají všech funkcí, jiné méně. Mezi nejzajímavější programy této kategorie se však bezpochyby řadí následující produkty:

- **AVG** – český výrobek
- **avast!** – český výrobek
- **Kaspersky Antivirus**
- **Norton Antivirus**
- **McAfee VirusScan**

Spam

Spam – pojem, který před pár lety nikdo neznal, dnes se s ním důvěrně seznámil každý častější uživatel internetu. Nejprve tedy k jeho popisu a poté také k formě ochrany před tímto novodobým problémem.

Co je to?

Spam je v jednoduchém překladu „nevyžádanou poštou.“ Jedná se tedy o takové emailové zprávy, které vás obtěžují, mají reklamní charakter a obecně splňují ze zákona stanovené podmínky. Jak totiž znalejší z řad uživatelů internetu jistě ví, i u nás je spam nelegální! A co nám zákon týkající se spamu říká vpraxi?

V následujících řádcích jsem vycházel z názorů právníka a dostupných informací. Podle § 2 odst. 1 písm. e) zákona č. 138/2002 Sb. platí následující:

"Zakazuje se šíření nevyžádané reklamy, pokud vede k výdajům adresáta nebo pokud adresáta obtěžuje."

Zákaz tak platí pouze při splnění všech následujících podmínek:

1. *musí jít o reklamu*
2. *tato reklama musí být nevyžádaná*
3. *musí dojít k obtěžování adresáta*
4. *nebo k výdajům adresáta*

Jak je vidno, již samotné definování spamu ze zákona poskytuje jeho původci mnoho prostoru – nevyžádanou poštou totiž není chápán email (například v miliónu kopií), kterým se uživatel rozhodl prezentovat odlišný názor na aktuální politické dění, rozhodnutí našich vrcholných představitelů atd. V případě druhého bodu je řešení také nasnadě – „reklama musí být nevyžádaná“, přičemž tuto podmínku lze snadno obejít – stačí do emailu umístit informaci, podle které můžete v budoucnu rozesílání reklamních emailů zabránit jednoduchým odhlášením svého jména z databáze. Zdá se to možná směšné, podle právníků však rozhodně postačující.

Zákon pak také vymezuje sankce, které mohou být rozesílateli a původci podobně nevyžádané pošty uloženy:

Podle § 8 odstavec 1 písm. a) zákona o regulaci reklamy platí, že orgán dozoru uloží zadavateli, zpracovateli nebo šířiteli reklamy, která je v rozporu s tímto zákonem, pokutu až do výše 2 000 000 Kč podle závažnosti porušení povinnosti, a to i opakovaně.

Bohužel, zákon je jedna věc (a v našem případě ještě mnohdy děravá), realita jiná. Skutečnost hovoří za vše – spam je stále nedílnou součástí naší každodenní pošty a situace se v budoucnu jen těžko změní.

Jak se bránit?

Ze zákona je spam nelegální, pro uživatele to však nic neřeší a podceňovat jeho obtěžující funkci není radno. Podle údajů provozovatelů emailových schránek totiž dorazí do emailů jejich zákazníků denně kromě klasických zpráv také téměř dvojnásobek těch nevyžádaných. Právě proto je základem ochrany antispam na straně serveru, který se o odstranění nevyžádané pošty stará. Bohužel, ani tato služba není dostačující a tak se uživatelé musí bránit především sami!

Prevence!

Tkví v několika zásadách, kterými bychom se měli řídit!

- 1) Emailovou adresu nezveřejňujeme na internetu, není-li to nezbytné. Nejčastějším zdrojem funkčních emailových schránek jsou právě webové stránky.
- 2) Používáme speciální formu zápisu emailové adresy – místo znaků jako je „@“ použijeme jednoduše „(zavináč)“ – jednoduchý příklad v praxi: „kamil(tečka)gric(zavináč)doupe(tečka)cz“

Pasivní ochrana

Tkví ve využití speciálních programů a spamových filtrů, které se snaží nevyžádanou poštu rozeznat a odstranit – mažou ji či přesunou do speciálních složek

Aktivní ochrana

Na první pohled nejatraktivnější forma – tkví totiž v pokusu o potrestání spamera, k čemuž je pak potřeba dohledat počítač, ze kterého byl spam odeslán a stěžovat si u správce sítě. Kdo z nás však má na něco podobného čas, peníze i energii?

Závěrem

Doufám, že má celá práce dostatečně prezentovala veškerá úskalí i nebezpečí počítačových virů a také spamu. Jedná se o častý zdroj problémů s PC a v obou případech se nejedná pouze o otázku minulosti, ale především budoucnosti, kdy můžou viry (a svým způsobem také nevyžádaná pošta) působit mnohem větší nebezpečí. Snad se tak nestane.

Zdroj informací:

- Igor Hák, <http://www.viry.cz/>;
- Infosystém PřF UK, <http://info.natur.cuni.cz/pocitace/viry/>;
- Šotola Petr, <http://www.sotolapc.cz/>;
- Živě.cz, internetový server, <http://www.zive.cz/>;
- CDR.cz, internetový server, <http://www.cdr.cz>