Jemný úvod do (anti)virové problematiky

Petr Holub, ÚVT MU

Hned na začátek se sluší poznamenat, že i mistr tesař se někdy utne a počítačovému specialistovi se také může stát, že nějakým nešťastným počinem podpoří šíření virové infekce. Na druhou stranu pravděpodobnost, že se něco podobného stane osobě poučené, je výrazně nižší než u osoby nepoučené. V tomto článku se pokusíme shrnout informace o různých virech a jak se před nimi chránit a snížit tak alespoň o něco množství osob nepoučených.

Tento článek se snaží podat obecný úvod do problematiky, konkrétní aplikace jsou pak probírány v jiných článcích v tomto čísle Zpravodaje.

1 Viry, červi, trojští koně a jiná havět

Co znamenají termíny počítačové viry, červi a podobné termíny? Většinou označují kód, který běží na počítači uživatele bez jeho vědomí a z tohoto počítače se pak šíří dále. Často zahrnují také kód, který může modifikovat či ničit uživatelova data, případně jeho dokumenty, které mohou být přísně soukromého charakteru, rozesílat do Internetu.

1.1 Rozdělení

Co se pod jednotlivými termíny skrývá? Proč bychom mezi nimi měli rozlišovat? Ze stejného důvodu, jako se v běžném životě rozlišuje mezi infekcí virovou a bakteriální – na čistě virovou infekci nemá cenu nasazovat antibiotika. Obdobně je tomu i v případě počítačových infekcí: různé infekce mají různé způsoby „léčby“.

Trojský kůň. Jedná se o program, který se na první pohled zdá být užitečným programem. Ať už něco užitečného skutečně provádí či nikoli, jeho vedlejší úlohou jsou činnosti, o nichž uživatel netuší a které mohou být velmi nepříjemné (mazání souborů, otevření zadních vrátek do počítače připojeného k síti apod.). Co trojského koně odlišuje od zbylých dvou skupin, je jeho neschopnost šířit se samovolně na další počítače. Často se můžeme například setkat s trojskými koňmi maskovanými za spořiče obrazovky.

Virus. Tímto pojmem se označuje kód, který sám sebe replikuje a vkládá do jiných programů. V okamžiku, kdy je infikovaný program spuštěn, dojde také k aktivaci viru. Viry kromě svých schopností šíření také často obsahují kód na destrukci dat uživatele, případně na jejich kompromitaci (například otevřením zadních vrátek). Tento kód nemusí být spouštěn při každé aktivaci viru, ale třeba pouze k zadanému datu, což umožňuje viru fungovat skrytě, aniž by nějak uživatele upozornil na svoji přítomnost v infikovaném systému.

Makrovirus. Jde o specifickou skupinu virů, o jejíž existenci se před šesti, sedmi lety vůbec neuvažovalo. S příchodem textových editorů, které v sobě uměly spouštět uživatelem specifikovaný kód (tzv. *makra*), se však staly poměrně nepříjemnou hrozbou právě proto, že si uživatelé nebyli dostatečně vědomi tohoto nebezpečí.

Červ. Tento termín označuje kód, který se také šíří mezi počítači, ale buď běží pouze v operační paměti počítače, nebo se ukládá na disk do samostatných souborů, jejichž spuštění při startu počítače si zajistí vhodnou modifikací souborů řídících start počítače. Od viru jej odlišuje neschopnost vkládat se do jiných programů.

Hoax. V tomto významu bychom slovo hoax mohli přeložit jako podvodný poplach. Nejedná se tedy o program, ovšem jeho důsledky mohou být stejně nepříjemné. Objevily se například dopisy vyzývající uživatele ke smazáni souboru, v němž je prý uložen červ – ve skutečnosti se však jednalo o soubor životně důležitý pro chod operačního systému. Takové zprávy by běžný uživatel měl brát na vědomí pouze v případě, že mu přišly od správce jeho počítače či sítě, v níž je jeho počítač zapojen. Navíc by tomu mělo předcházet ověření, že dopis přišel skutečně od správce a nejedná se o falzifikát. Dopisy tohoto druhu z jiných zrojů by měl uživatel smazat.

1.2 Způsoby aktivace

K nejobvyklejším způsobům aktivace virů patřilo a patří spuštění infikovaného spustitelného (*executable*) souboru. Dalším způsobem používaným hlavně u starších virů byla nákaza v tzv. *bootovacím sektoru*, čímž se zajišťovalo automatické spouštění viru při samotném startu počítače z daného disku či diskety[1].

S příchodem makrovirů se podobně nebezpečnými staly ty dokumenty, z nichž aplikace umožňuje spouštět programový kód (typicky např. makra v případě nástrojů Office firmy Microsoft). Tyto aplikace navíc často umožňují spouštět kód automaticky hned při otevření daného dokumentu (jak tomuto nebezpečí předcházet se zmíníme níže).

Dalším způsobem šíření je využívání chyb v programech. Náchylnost programů na bezpečnostní chyby je obzvláště nebezpečná v případě síťových programů. Tímto způsobem jsou často zneužívány webové servery, poštovní servery či poštovní klienti.

S rozvojem Internetu nastal také obrovský rozvoj červů a virů, kteří se šíří za pomoci elektronické pošty. Někteří zástupci této kategorie využívají pouze metod tzv. sociálního inženýrství, tedy například psychického tlaku na uživatele textem dopisu. Klasickým příkladem jsou červi, jejichž průvodní dopis obsahuje text, že po kliknutí na přílohu se dostanou k obrázkům nějaké slavné celebrity. Je až k neuvěření, kolik lidí dokáže tak primitivní hříčce podlehnout. Na druhou stranu existují i mnohem rafinovanější dopisy, které vypadají jako dopisy softwarových společností, které v příloze údajně obsahují důležitou bezpečnostní aktualizaci softwaru[2]. Jiní červi využívají chyb v poštovních klientech, které např. umožňují spuštění kódu už jen při pouhém otevření náhledu na došlou zprávu (vzhledem k tomu, že většina uživatelů má nastavený automatický náhled na zprávy, dojde ke spuštění takového kód ihned při běžném procházení pošty za předpokladu, že aplikace tuto chybu obsahuje).

1.3 Způsoby šíření

Klasickým způsobem šíření virů byla infekce spustitelných souborů a případně též bootovacího sektoru na počítači uživatele. Při předávání souborů mezi uživateli pak snadno došlo k přenosu nákazy. V síťovém prostředí pak nákaza probíhá testováním okolních strojů a serverů, zda jsou zranitelné, a také infekcí souborů na síťových discích.

V případě e-mailových virů probíhá šíření rozesíláním dopisů dalším uživatelům. Aplikace obvykle použije seznam adres získaných buď z uživatelova adresáře, případně též projde přijatou poštu a vybere osoby, od nichž uživatel nějaký dopis v minulosti dostal. Poté virus pod jménem daného uživatele rozešle dopisy buď s použitím některého z poštovních serverů, které má uživatel nadefinován, nebo k šíření použije vlastní poštovní server. Jako tělo dopisu se použije buď nějaký pevně definovaný text, nebo některé rafinovanější viry používají úryvky z uživatelovy korespondence či z dokumentů uložených na disku, což může mít velmi nepříjemné následky, jedná-li se o důvěrné materiály. Svoji kopii pak k dopisu připojí jako přílohu.

1.4 Zlovolné činnosti

Jaké nepříjemné činnosti nám může zlovolný program dělat pod rukama? Jedná se o poměrně bohatý repertoár, kombinující často více možností z následujících:

- modifikace či mazání dat
- kompromitace důvěrných materiálů jejich rozesláním třetím osobám
- zneužívání uživatelova počítače k útokům na další počítače[3]

[1] K oblíbeným mýtům o virech patřilo, že již pouhé vložení diskety s infikovaným bootovacím sektorem do počítače či vypsání adresáře na takové disketě způsobí infekci počítače. Za předpokladu, že v systému a systémových programech není nějaký zásadní bezpečnostní nedostatek, takto počítač infikovat nelze. Pro infikování je třeba počítač z diskety nastartovat, neboť teprve tehdy dochází ke spuštění kódu uloženého v bootovacím sektoru

[2] Takové dopisy je nejlépe hned smazat, protože firmy sice skutečně posílají informace o bezpečnostních aktualizacích pomocí e-mailu, ovšem v žádném případě k němu samotnou záplatu nepřipojují a pouze vybídnou uživatele k jejímu stažení z webu či FTP dané společnosti.

[3] Zde nemáme nutně na mysli šíření virů dále, ale například útoky typu Denial of Service (při takovém útoku je

– kompromitace uživatelových hesel
– vytvoření „zadních vrátek“ k počítači
– ohrožení funkce počítače na hardwarové úrovni[4].

Z předchozího popisu je vidět, že infekce počítačovým virem či červem může mít *velmi* nepříjemné následky. Jak proti případné infekci můžeme bojovat? Je třeba využít kombinace dvou strategií: softwarovou ochranu a zásady bezpečného chování, které si nyní podrobněji probereme.

2 Softwarová ochrana

2.1 Aktualizace programového vybavení

Vzhledem k obvyklým metodám vývoje programů je bohužel časté, že programy obsahují mnoho chyb, z nichž některé mohou mít velmi nepříjemné bezpečnostní následky. Většina producentů software se v případě objevení bezpečnostní chyby snaží vydat co nejrychleji „záplatu“, kterou by měli uživatelé aplikovat (slušní výrobci dávají tyto bezpečnostní záplaty zdarma).

Je na zodpovědnosti každého správce počítače (tedy uživatele za předpokladu, že uživatel je zároveň i správcem svého počítače) tyto záplaty co nejdříve nainstalovat. Správce by proto měl pravidelně sledovat seznam dostupných záplat pro software nainstalovaný na počítačích, které spravuje. Zvláště důležité je to v případě, že stroje a sítě jsou přímo připojeny do Internetu, a to i v době nepřítomnosti uživatele počítače. Problém totiž spočívá v tom, že v poslední době se již krátce po objevení bezpečnostního nedostatku začínají objevovat první červi, kteří procházejí stroje dostupné na Internetu a testují, zda jsou k danému problému náchylné, a pokud ano, tak stroj infikují. Dalším problémem je, že pokud virus pronikne do počítače bezpečnostní dírou v nějakém programu, snižuje se pravděpodobnost, že bude zachycen systémem antivirové ochrany (viz níže).

Často se člověk může setkat s názorem, že k těmto problémům jsou náchylné jen produkty firmy Microsoft. To samozřejmě není pravda a o bezpečnostní aktualizace je třeba se starat i v případě všech jiných operačních systémů a aplikací.

2.2 Antivirové programy

Antivirové programy jsou programy na detekci a ve většině případů i odstranění virové infekce. Tyto programy mohou běžet jak na počítačích běžných uživatelů, tak i na serverech. Často jsou umísťovány na poštovní servery, kde procházejí poštu proudící přes daný server a zachycují virovou infekci.

V případě operačních systémů Windows je velmi vhodné mít na každém takovém počítači nainstalován kvalitní antivirový program, který je třeba pravidelně aktualizovat. Vzhledem k frekvenci vzniku nových virů by interval mezi aktualizacemi neměl být delší než jeden týden. Program by měl být zkonfigurován tak, aby se startoval zároveň se startem operačního systému a aby měl zprovozněn tzv. on-access scanner, tj. aby kontroloval všechny soubory před tím, než se s nimi začne pracovat.

V případě antivirových programů je třeba mít na paměti, že tyto programy jsou schopny zachytit prakticky všechny viry a červy, ale totéž obvykle zdaleka neplatí o trojských koních, pokud se nejedná o ty nejznámější (uvědomme si, že v tom případě by antivirový program musel neustále analyzovat veškerou činnost všech programů a při tom spolehlivě rozhodovat, která činnost patří řádnému programu a která trojskému koni).

Další problematická kapitola zahrnuje průniky přes bezpečnostní chyby v programech pracujících se sítí. Antivirové programy obvykle sledují

počítač zahlcen například nesmyslnými požadavky tak, že nemůže poskytovat běžné služby, které poskytovat má). Tyto útoky vedené z akademického prostředí do prostředí komerčního mohou být obzvláště nepříjemné, neboť akademická komunita často disponuje mnohem větší šířkou pásma než je přípojná šířka pásma komerčních institucí a není proto problém saturovat útokem zcela jejich připojení.

[4] Často se tvrdí, že virus nemůže zničit počítač na hardwarové úrovni. Problém ovšem je, že například virus CIH známý též jako Černobyl dokáže přepsat FlashBIOS počítače, bez něhož počítač nemůže nastartovat. Z pohledu běžného uživatele se pak jedná o hardwarové poškození, neboť tento problém není možné odstranit reinstalací softwaru na počítači.

práci s diskem a předpokládají, že program je uložen před tím, než je spuštěn. Pokud je ovšem program spuštěn bez předchozích uložení například tak, že je přímo ze sítě umístěn do operační paměti a je mu předáno řízení, pak má antivirová ochrana jen malou šanci jej zachytit. Zde má nezastupitelnou roli aktualizace programového vybavení na počítačích.

2.3 Další metody

Do této kategorie patří na prvním místě *zálohování*. Jak říká jedno oblíbené pravidlo: zálohy oceníme obvykle teprve v okamžiku, kdy je nemáme a nutně potřebujeme. Kdykoli se můžeme dostat do situace, kdy nám nezbude nic jiného než obnova souborů ze zálohy – nemusí se jednat jen o virovou infekci, ale třeba o hardwarovou poruchu pevného disku.

Důležitým prvkem ochrany je také vypnutí podpory maker v aplikacích typu Office a jejich selektivní zapínání pouze v případě, že jsme si naprosto jisti, že daný soubor virus neobsahuje (například po prověření antivirovým programem), a pouze pokud jsou makra nezbytná pro správné zobrazení dokumentu.

Poznámka pro pokročilé uživatele: Existuje řada programů na posílení soukromí a bezpečnosti, o jejichž nasazení je možno uvažovat: osobní firewally (např. ZoneAlarm) či systémy detekce průniku (např. BlackICE, snort, tripwire). Dále existují systémy pro šifrování dat, které mohou pomoci snížit pravděpodobnost jejich kompromitace (např. PGP).

3 Základy bezpečného chování

Bezpečné chování uživatele je opět velmi důležité hlavně v prostředí, kdy je jeho počítač připojen k Internetu. To ovšem neznamená, že by se tomuto tématu neměla věnovat pozornost i na počítačích od Internetu odpojených.

3.1 Práce s elektronickou poštou

V naší poštovní schránce se objevil nový dopis, který:

- je napsán v jazyce, kterému nerozumíme případně obsahuje podivné znaky
- netušíme, proč bychom takový mail měli dostat
- má v předmětu slova jako „happy day“, „birthday“, „how are you“, „love“, „erotic“ apod.
- je v cizím jazyce, ačkoli jej nám posílá někdo známý, který by pro to mohl těžko mít nějaký důvod, či dopis obsahuje text, který nijak rozumně neodkazuje na odesílatele ani adresáta
- obsahuje několik nesouvisejících částí – vět či odstavců (některé viry konstruují tělo dopisu tak, že procházejí dokumenty na disku uživatele a náhodně z nich vybírají věty či odstavce)
- obsahuje podezřelou přílohu a ještě jsme v textu dopisu vybízeni k jejímu otevření; v souvislosti s odesílatelem ani adresátem nám však příloha nic neříká.

Takový dopis je nejlépe *okamžitě smazat*. Za žádných okolností však nemanipulujeme s přílohou takového dopisu s výjimkou jejího smazání.

V případě, že nám od nějakého známého či kolegy přijde spolu se srozumitelným dopisem také příloha, u níž si nejsme úplně jisti, zda je v pořádku, je lépe si *před* jakoukoli manipulací s takovou přílohou (ukládání, otevírání) ověřit, zda je vše v pořádku (např. kontrolním dopisem či telefonicky). *To, že dopis přijde od osoby, kterou známe, ještě neznamená, že takový dopis lze považovat za bezpečný*[5].

V případě práce s přílohou je nejbezpečnější strategií její uložení na disk s následnou kontrolou antivirovým programem před otevřením takové přílohy.

Umožňuje-li náš poštovní klient automatickou aktivaci JavaScriptu, ActiveX komponent či maker, je velmi rozumné tyto vlastnosti vypnout!

3.2 Práce s dalšími službami Internetu

Po elektronické poště je dalším potenciálně nebezpečným nástrojem služba WWW. Internet je sice takřka neomezeným zdrojem různých zajímavých programů a utilit, ale zároveň je třeba mít na paměti, že je i zdrojem lecjakých trojských koní a virů. Není tedy vhodné stahovat a

[5] Jako ilustraci problému důvěryhodných zdrojů lze uvést příklad, kdy jedna známá firma nešťastnou náhodou distribuovala zavirovaný program na instalačním CD.

instalovat každý zajímavý program, na který narazíme. Totéž se týká i posílání souborů přes IRC.

Dalším zdrojem problémů jsou webové stránky, které obsahují kód využívající bezpečnostních děr v prohlížečích. V každém případě je dobré utužit bezpečnostní nastavení v prohlížeči na nejvyšší míru, která nás ještě nebude výrazně omezovat při práci.

V případě, že jeden počítač sdílí více lidí, je třeba dbát na to, aby všichni používali tutéž míru zabezpečení.

4 Co dělat v případě nákazy?

Prvním krokem při podezření na virovou nákazu by měla být kontrola, zda jde skutečně o virovou nákazu. To, že nějaký program nefunguje tak, jak má, většinou pramení z chybné konfigurace a ne z nákazy virem. Prvotní kontrolu je nejlépe provést aktualizovaným antivirovým programem.

Pokud se infekce potvrdí, je nejlépe postupovat dle pokynů, které antivirový vypíše. Většina velkých antivirových společností také udržuje na svých webových stránkách popisy virů včetně způsobu jejich odstranění.

V případě, že si na odstranění netroufáme sami, je třeba neprodleně kontaktovat správce, který má daný stroj na starosti. V každém případě však naší prvořadou a jedinou aktivitou okamžitě po zjištění infekce musí snaha o zamezení jejího šíření a její odstranění. Musíme také *neprodleně odpojit počítač od počítačové sítě*, aby virus nemohl využít svých schopností šířit se po síti. Čekáme-li s odstraněním nákazy na správce systému, je lépe počítač dočasně vypnout.

5 Závěrečné poznámky

Virová problematika je samozřejmě mnohem složitější, než jsme mohli v tomto souhrnném článku uvést. Počítačoví odborníci by měli mít mnohem hlubší znalosti a podrobnější informace. Pro běžného uživatele však snad poskytl alespoň přehled problematiky a základní informace o tom, jak by se měl chovat, aby nezavdal zbytečně příčinu ke vzniku problémů.

6 Odkazy

Další odkazy lze najít na řadě míst v Internetu, například

- weby antivirových společností
  - `http://www.norman.com/`
  - `http://www.europe.f-secure.com/`
- diskusní skupiny zaměřené na viry (informace v nich obsažené je však třeba ověřovat, protože mohou ale nemusí být důvěryhodné)
  - <news:comp.virus>
  - <news:alt.comp.virus> □