Spam a viry - smrtící symbióza

V době psaní tohoto článku otřásá světovým internetem vrchol infekce virem SoBig.F. Tento virus se od většiny předchozích liší tím, že byl napsán specificky za účelem podpory šíření nevyžádané komerční pošty (spamu).

Pro typického koncového uživatele internetu představují viry a spam pouze nepříjemnost: nutnost mazat z e-mailové schránky množství zpráv, případně platit za jejich stahování. Ovšem pro provozovatele e-mailových systémů, zejména těch velkých, představují viry a spam problém zcela zásadní. A vyhlídka na jejich vzájemnou podporu a symbiózu hrozí až problémy existenčními. Může se stát, že společnými silami viry a spam zahubí svého hostitele: e-mail, nejpoužívanější službu internetu na počátku 21. století.

Trocha historie

Standardy, které dnes používají téměř všechny internetové poštovní servery, loni oslavily dvacet let existence. Protokoly SMTP a formát poštovních zpráv vznikly v době, kdy nikdo neočekával, že by počet zasíťovaných počítačů a jejich uživatelů mohl dosahovat dnešních hodnot. A jakkoliv se bráním tomu, označit je za špatné, je to na nich vidět. Původní návrhy nepočítaly s posíláním jiného typu obsahu než prostého textu a počítaly s tím, že formát by měl být v zásadě "lidsky čitelný". Šlo v podstatě o drobné rozšíření unixové vnitřní pošty v rámci jednoho systému.

Zásadní změnu do elektronické pošty přinesl až formát MIME (Multipurpose Internet Mail Extensions), definovaný původně v RFC1341, nyní v RFC2045-RFC2049. Jeho omezení si byli vědomi i sami autoři, když napsali: "Některé z mechanismů popsaných v této sadě dokumentů mohou po prvním přečtení působit divně, až zbytečně přebujele. Je důležité poznamenat, že kompatibilita s existujícími standardy a soulad s praktikami používanými v současnosti (nestandardizovanými pozn. aut.) byly dvě nejvyšší priority, se kterými autoři tyto dokumenty vytvářeli. Jinak řečeno, vždy jsme upřednostňovali kompatibilitu před elegancí." Jako člověk, který prošel martyriem psaní odpovídajícího parseru, z celého srdce - a se zřetelně slyšitelným skřípěním zubů - souhlasím.

Standard MIME umožňuje posílání jiných než čistě textových dat - HTML formátovaných zpráv s vloženými obrázky, attachmentů a podobně. Vzhledem k implementační volnosti (na straně odesílatele) a složitosti (na straně příjemce) vytváří slušný prostor pro chyby, kterých využívala předchozí generace e-mailem se šířících virů.

Problém: viry

První generace e-mailem se šířících virů využívala hlouposti uživatele. Druhá generace využívala chyb v e-mailových klientech. Třetí se s úspěchem vrátila k osvědčené hlouposti, poučena poznáním, že je to spolehlivější.

Z hlediska správce poštovního serveru je vlastní projev viru (například smazání určitých souborů) nezajímavý: to je problém uživatele. Nicméně virus se snaží dále šířit, a to už pro správce problém je, protože jeho systém se musí vyrovnat s obrovským množstvím zpráv, které jest záhodno nějak zpracovat.

Antivirové programy

Poslední dobou začínám dospívat k závěru, že antivirové programy jsou spíše problémem než řešením - zejména v té "domácí" verzi, jsou-li nasazeny na počítači klienta. Dávají uživateli falešný pocit bezpečí: "Když to prošlo antivirem, je to v pořádku." Často ale nejsou schopny reagovat na virové nebezpečí dostatečně rychle (i v řádu jednotek hodin). Domácí uživatel není schopen si systém aktualizovat dostatečně často - jednou týdně, dokonce ani jednou denně nemusí stačit. Ale i v tom nejlepším případě jde pouze o částečné řešení: virus bude zneškodněn, ale až u uživatele. Předtím musí projít e-mailovým systémem a být celý stažen na klientský počítač.

Smysluplnější variantou, vyskytující se bohužel v současnosti téměř výhradně na serverech větších firem, je antivirový filtr přímo na serveru. Virové databáze takových filtrů bývají aktualizovány v podstatě v reálném čase, takže mají dobrou úspěšnost. Zavirovaný e-mail odmítnou ještě předtím, než se vůbec dostane k dalšímu zpracování. Ochrání tedy systém příjemce zprávy.

Případ viru SoBig.F ovšem dokázal, že antivirové systémy mohou způsobovat větší problémy než virus samotný. Naprostá většina jich totiž pošle na adresu uvedenou jako odesílatel zprávy poměrně obsáhlou zprávu o tom, že e-mail nebyl doručen, protože byl vyhodnocen jako zavirovaný. Některé obzvláště stupidní systémy k tomu přiloží i kompletní předmětnou zprávu. Takže zatímco mi nedorazila jediná kopie viru jako takového - ty odchytila moje vlastní content gateway -, byl jsem obšťastněn tisíci

zpráv o tom, že moje zpráva nemohla být doručena. Přitom všechny novější viry adresu odesílatele podvrhují, takže ten, kdo je jako odesílatel uveden, nemá se zprávou nic společného.

A jsme opět u protokolu SMTP, který nejen že umožňuje snadné podvržení adresy odesílatele, protože si ji žádným způsobem neověřuje, ale navíc ani nijak nekodifikuje formát chybových zpráv. Není tedy možné zajistit, aby uživatel dostával informace pouze o těch chybách, které se týkají zpráv, jež skutečně odeslal.

Problém: spam

Spam má s viry společné problémy, jež způsobuje: velké množství zpráv, které zahlcují poštovní servery, přenosové trasy a mailboxy uživatelů. Špatné je, že se podstatně hůře detekují a při jejich automatizované detekci je větší pravděpodobnost falešného poplachu. V současné době jsou nejefektivnějšími způsoby blokace spamu kombinace IP blacklistingu a heuristické analýzy.

IP blacklisting

Většina spamů je šířena prostřednictvím nedostatečně zabezpečených SMTP serverů - open relay. K tomu existuje několik systémů (např. www.ordb.org, www.spamcop.net), nazývaných RBL - Realtime Blackhole List. Do nich jsou zapisovány IP adresy serverů, které jsou nedostatečně zabezpečené nebo které již byly zneužity k posílání spamu. Přijímající mailserver si pak může ověřit, zda počítač, se kterým komunikuje, není na "blacklistu", a zachovat se podle toho. Některé poštovní servery mají tuto funkčnost vestavěnu přímo v sobě (např. XMail Server, www.cz.xmailserver.org), do jiných se dá pořídit patřičný plug-in, případně tyto databáze umějí využívat i některé antivirové programy a content gateways (např. Symantec AntiVirus for SMTP Gateways).

Výhodou blacklistingu je nízké procento falešných poplachů, nevýhodou to, že spameři nyní často používají sofistikovanější metody, jako například open proxy nebo různé trojany.

Heuristická analýza

Tato metoda je založena na syntaktické a sémantické analýze obsahu e-mailu: specializovaný program prohledává zprávu a hledá znaky, které by mohly naznačovat, že jde o spam (použití určitých slov, slovních obratů či technologií), nebo že tomu tak není (použití PGP signatury a podobně). Na základě těchto příznaků počítá skóre a při dosažení určité hodnoty zprávu označí za spam.

Pravděpodobně nejrozšířenějším zástupcem této technologie je open-source SpamAssassin. Obdobná technologie je implementována i v nové verzi MS Office Outlook 2003. Tato metoda má poměrně vysokou úspěšnost, ale je zde slušné nebezpečí, že i nevinné e-maily budou odmítnuty jako spam.

Smrtící symbióza: případ Sobig.f

Současnou hvězdou virové scény je virus Sobig. První varianta (Sobig.a) se objevila v lednu 2003. Smyslem existence tohoto viru je podpora šíření spamu: virus se snaží instalovat na napadené počítače trojského koně, který umožní použití počítače jako proxy pro šíření spamu. Podobné technologie vyřadí RBL sítě ze hry a bude záviset čistě na analýze obsahu.

V důsledku 11. září 2001 je dnes za "terorismus" označováno cokoliv nepohodlného. Ve světle možnosti řádového nárůstu obtížně filtrovatelných spamů kombinovaných s viry se začínám i já přiklánět k názoru, že označení "kyberterorismus" je pro tuto činnost více než na místě.

Řešením je změna

Jediným trvale udržitelným řešením situace s viry a spamem je podle mého názoru implementace novějšího a schopnějšího poštovního protokolu. Nástupce SMTP by měl řešit zejména tyto dva jeho hlavní problémy:

Zamezení nebo alespoň ztížení podvržení odesílatele e-mailu. Možností je implementace kryptografických technik na bázi elektronického podpisu, což bude ovšem narážet na problémy technologické i etické. Postačujícím řešením by bylo určit poštovní servery oprávněné odesílat poštu za danou doménu.

V současné době jsou pomocí MX záznamů v DNS definovány servery pro příjem pošty (mail exchangery). Pokud by bylo možno určit a ověřit servery, které mají oprávnění poštu za danou doménu odesílat, ztížilo by to možnost falšování adresy odesílatele.

Automatizované řešení problémových stavů. Protokol SMTP přenáší v maximální míře zodpovědnost za řešení problémových stavů na uživatele. Neexistence standardizovaných a počítačem zpracovatelných informací o chybách znamená, že nelze problémy s chybami řešit nějakou automatickou

nebo alespoň automatizovanou cestou. Není tedy možné zajistit ani tak triviální funkčnost, jakou je jisté navázání chybového hlášení na konkrétní zprávu. Nástupce protokolu SMTP by se mohl inspirovat například u X.400, který tyto stavy řeší celkem uspokojivě, byť za cenu podstatně vyšší složitosti.

Bohužel je velmi nepravděpodobné, že se takové změny dočkáme v brzké době. Firmy již investovaly do vybudování poštovní infrastruktury tak vysoké částky, že se nedá předpokládat, že by chtěly stávající řešení opustit a investovat do něčeho jiného. Dá se tedy očekávat, že elektronická pošta bude následovat příkladu IPv4, resp. nezavedeného IPv6: všichni vědí, že stávající technologie nestačí, ale nemají peníze na novou.

Michal A. Valášek, alt@ir.cz