Neúčinné antispamové filtry

Obranné prostředky proti spamům ztrácejí v poslední době na síle

VOJTĚCH BEDNÁŘ

Problém nevyžádané pošty je jedním z největších problémů, se kterými se současný IT svět musí prát. Ještě nedávno se zdálo, že ochrana uživatelů vítězí. Nyní se však karty začínají obracet.

SPAM, neboli nevyžádaná pošta jsou reklamní, propagační, ale také třeba podvodné e-maily rozesílané v milionech exemplářů na e-mailové adresy, jejichž majitelé takové zprávy nechtěli a které tyto zprávy obtěžují. Odesilatelé využívají speciální software, který jim umožňuje získat seznamy mnoha adres z veřejných služeb, z webových prezentací, z konferencí a dalších míst. Pak posílají své nevyžádané zprávy na tyto adresy. Jejich majitele poškozují jednak přímo – na čase, který musí u třídění takovéhoto odpadu strávit, než jej identifikují a oddělí od skutečně hodnotné pošty, či vlákáním do podvodu. Mimo to však SPAM poškozuje IT infrastrukturu nepřímo. Využívá mnoho jejích systémových prostředků, narušuje její fungování, komplikuje transakce nevyhnutelné k přenosu autorizované pošty. Jinými slovy, SPAM patří k hlavním problémům a ten, kdo by vymyslel ideální řešení proti němu, řešení, které by bylo stoprocentní, by si zřejmě zajistil velmi pěkné živobytí i nekonečné uznání až do konce života.

Proti nevyžádané poště existují již nyní desítky různých obranných prostředků. Mezi nejjednodušší patří blokování adres, z nichž je tato pošta odesílána. Děje se tak buďto na serverech, nebo v klientech elektronické pošty. Kromě toho je možné blokovat i přímo počítače, z nichž se odesílání děje, nebo analyzovat strukturu zpráv technikou podobnou heuristické analýze v antivirových systémech a na základě této analýzy se rozhodovat, máme-li co do činění s vyžádanou, nebo nevyžádanou poštou. Kromě toho existuje mnoho dalších možností odstranění nevyžádané pošty. Některé z nich se minoritně využívají, jiné jsou ve stadiu teorie, další jsou upotřebitelné pouze v měřítku uzavřených nebo neveřejných sítí, další se nakonec ukáží jako nefunkční nebo nepoužitelné.

Velkou změnu na poli boje proti nevyžádané poště přinesly v uplynulém roce dvě věci. První z nich bylo vytvoření inteligentního a přitom uzavřeného heuristického filtru. Tento filtr je schopen s vysokou přesností rozlišit nevyžádanou poštu na základě analýzy jejího obsahu. Neváže se na konkrétní text – ten totiž může být velice proměnlivý – ale vyhodnocuje zprávu na základě souběžného výskytu mnoha znaků indikujících spam. Druhým objevem pak byla integrace takového filtru do serveru elektronické pošty. Nevyžádané zprávy je díky němu možné odstranit z e-mailové schránky předtím, než se k nim uživatel vůbec dostane. To mu ušetří čas, práci, a navrátí dávný komfort nakládání s elektronickou poštou známý z dob, kdy nás nevyžádané zprávy v takovém měřítku jako dnes ještě netrápily.

Protože serverový filtr není možné mít nastavený na maximální citlivost, stává se, že pouští, již ze svého principu, část nevyžádané pošty dál. Je to proto, že maximální stupeň ochrany před nevyžádanou poštou by v jeho případě vedl k odchytávání také regulérních zpráv jako spamu a k jejich likvidaci, nebo přesouvání do k tomu určených složek. Zprávy, u nichž si serverový filtr není jistý, si klienti mají možnost buďto prohlédnout (což ale nechceme), nebo stáhnout klientskými aplikacemi do počítačů nebo jiných zařízení.

Aby bylo čištění pošty od spamu dokonalé, objevily se i inteligentní filtry integrované do čtecích programů, nebo závislé na využití určitého protokolu. Pravděpodobně nejznámější aplikací s obsaženým filtrováním nevyžádané pošty je nejpoužívanější klient, aplikace Microsoft Outlook 2003. Kromě něj však existují i další programy, podporující odstraňování nevyžádaných zpráv (Mozilla Mail), nebo také samostatné aplikace, které analyzují chování na portech poštovních protokolů a jsou schopny eliminovat nevyžádané zprávy – přenosy – přímo na nich.

Tato dvojkombinace serverové – klientské ochrany před nevyžádanou poštou, spolu s aktivní a aktuální ochranou před konvenčními červy představovala donedávna takřka spolehlivou ochranu. Šťastný uživatel, v českých podmínkách například velmi dobře chráněného, Seznam Mailu v kombinaci s Outlookem 2003 a aktuálním antivirovým systémem jiným než Nod32 (který je součástí Seznamu), se mohl cítit takřka úplně v bezpečí. Problém nevyžádané pošty se jej netýkal prostě proto, že přes velmi silnou vrstvu ochrany se k němu žádná nedostala.

Začínají problémy

V posledních několika měsících zveřejnil Microsoft prostřednictvím své služby Office Update, která (analogicky s Windows Update) slouží k aktualizaci produktů jeho kancelářského balíku, již dvě aktualizace antispamového filtru aplikace Outlook. Kromě toho někteří uživatelé začali pozorovat nápadné zvýšení množství nevyžádané pošty, která se třeba i přes dvojitou ochranu dostala až do jejich složky doručené pošty. Původní řešení, jež se k filtraci spamu používala, tedy především vytvoření seznamu nedůvěryhodných (blacklist) a naopak důvěryhodných (whitelist) adres, jejichž korespondence byla automaticky mazána, respektive explicitně přepouštěna přes filtr, jsou v současné době zcela nepoužitelná a aplikace které jsou založeny na tomto filtrování, obzvláště na blacklistech, již svou úlohu antispamového řešení neplní. Whitelisty jsou zase po praktické stránce použitelné pouze v omezené míře, jejich absolutní nasazení by totiž znamenalo znemožnit uživatelům e-mailu komunikaci s kýmkoliv, koho neznají, což zajisté není účelem.

Nárůst spamu v doručených složkách i těch klientů, jež byly donedávna proti nevyžádané poště efektivně chráněny, má jedno nepříjemné, avšak jednoduché vysvětlení. Spameři rozesílali nevyžádanou poštu, analyzovali filtry, a podařilo se jim najít způsob, kterak jejich působení obejít. Filtry tak začaly nevyžádanou poštu považovat za regulérní korespondenci a propouštět ji k uživateli, čímž rovněž začaly ztrácet svůj smysl.

Výrobci filtrů si tohoto jevu pochopitelně všimli, a do svých produktů začlenili ochranu proti novým trikům obtížného internetového hmyzu. Nemůžeme sice odhadovat, co se děje s filtry na serverech, ale potřeba aktualizovat Outlook z Office Updatu hovoří za všechno. I přes tyto aktualizace se ovšem spamerům stále daří. Navíc se zdá, že za použití jednoduchých fint.

Finty spamerů

Heuristické filtry jsou konstruovány v drtivé většině případů pro anglický jazyk – protože většina nevyžádané pošty je právě anglicky. Pokud si mají poradit s e-maily v jiných jazycích, nebo třeba jen jazykových sadách, mají potíže a mohou se orientovat prakticky jen podle některých všeobecných znaků odlišujících nevyžádanou poštu od běžné korespondence. Tedy se sníženou přesností. Spam, ačkoliv je rozesílán anglicky, může obsahovat řetězce v jazykových sadách evropských jazyků, čímž uvádí tento druh filtrů do stavu mírné nejistoty. Dalším elementem je využívání foneticky stejných, ale graficky odlišných slov. Pokud se například v nevyžádaném e-mailu vyskytuje čtyřikrát za sebou slovo „Viagra" a dotyčný e-mail navíc nese další znaky Spamu, je nekompromisně vyřazen. Stačí ale Viagru nahradit jinak stejnou Viiaagrou, a efekt rozpoznání je tentam, nebo se mu filtr bude přinejlepším mnohem hůře přizpůsobovat. Další, méně známou věcí je vkládání znaků, které antispamový filtr považuje za známku důvěryhodnosti. Takové řetězce jsou na koncích zpráv nebo jsou do nich umístěny tak, že je uživatel přinejlepším neuvidí. Vrcholem drzosti je pak to, když spameři své skutečné adresy (které uvádějí v těle zprávy) maskují v hlavičce e-mailu adresami z národních domén shodných s doménami příjemců. To totiž dokáže heuristické fitry znejistět ještě více. Vyjma toho existuje ještě několik dalších „fíglů". Na některé z nich již došlo, na některé ještě ne.

Najde se řešení?

V důsledku uvedených skutečností přestávají současná antispamová řešení postupně fungovat, respektive začínají markantně ztrácet na účinnosti. Jejich dosavadní aktualizace vedou pouze k částečnému zlepšení, brzy jsou zase autory Spamu odhaleny a nějakým způsobem obejity. Spolehlivý způsob rozpoznání, podobně jako třeba u virů, neexistuje a vypadá to, že ani není na spadnutí. Majitelé slabě zasažených schránek jsou poměrně dobře chráněni, avšak chudáci, v jejichž poště denně přistává stovka nevyžádaných mailů, na tom ani zdaleka tak dobře nejsou. Jediné, co lze ze strany vývojářů s tímto stavem udělat, je zdokonalovat a zdokonalovat, především naučit filtry „hovořit" národními jazyky a rozpoznávat text jiný než anglický či homofony. Uživateli pak nezbývá nic jiného, než si zachovat s nevyžádanou poštou, přesněji s jejím nedokonalým rozpoznáním určitou trpělivost, na nevyžádané maily neodpovídat – a především, nešířit je dál. Jedině tak se elektronickou poštu může podařit udržet jako užitečnou technologii, a ne jako něco, z čeho nás za pár měsíců nebo let bude všechny bolet hlava. 4 0299/FEL ❑

Tři typy e-mailů

Ne všechny e-mailové adresy jsou nevyžádanou poštou zahlceny stejně. V zásadě se dá říci, že na internetu v současné době existují tři typy adres – e-mailových schránek. První typ představují ty, jichž se problém nevyžádané pošty týká jen v minimálním měřítku – jsou zasahovány maximálně jednotkami nevyžádaných zpráv denně. Druhý typ představuje řekněme střední stupeň zamoření. Do takových schránek chodí řádově jednotky až desítky e-mailů denně. Třetí stupeň představují silně zamořené schránky, bombardované obrovským množstvím desítek, někdy až stovek zpráv denně. Zejména takové schránky jsou bez efektivní dvoufaktorové filtrace nepoužitelné. Je obtížné odhadovat, na čem je množství zamoření e-mailů závislé – v zásadě se dá říct, že faktorů je více. Třeba nakolik se dotyčná e-mailová schránka nachází ve veřejných adresářových službách, v konferencích, na webových stránkách, ve strojově čitelné podobě, v databázích spamerů. Jak často a kým je využívána, jak je aktivní a na spoustě dalších vlastností, které spolu málokdy souvisí, až právě na skutečnost, že ovlivňují spam. Všeobecně se dá říci, že efektivní obrana proti němu by měla v důsledku snižovat i množství nevyžádané pošty, a dobře chráněná schránka by tak časem mohla přestat být e-maily bombardována. Nakolik ale toto pravidlo platí, je spornou záležitostí.

▲ **Seznam Mail je velmi dobře chráněný antivirovým systémem NOD 32**

▲ **Informace ohledně spamu hledejte na serveru Antispamu (www.antispam.cz)**

▲ **I přes aktualizace z webu Office Update Microsoftu se zatím spamerům stále daří**