

Spam – mor 21. století

KARIM IFRAH

Spam je tu již 30 let. Za tu dobu se bezesporu stal jedním z neaktuálnějších problémů síťové komunikace, hned vedle červů a bezpečnostních rizik. Spam je starý problém, který ale neustále přichází s novými triky, jejichž cílem je obelstít antispamové filtry a proklouznout do schránek uživatelů. Boj se spamem je nekončící a uspět v něm může jen ten, kdo používá komplexní a proaktivní metody.

Devizou spamu je, že ekonomicky bude spammerům vyhovovat do doby, kdy bude získána odpověď na každý dvacetimilionový e-mail. V klasickém podnikání s uvedenou úspěšností nelze přežít, odvětví spamu však lze považovat za určitý paradox. Jelikož škody vyvolané spamem stojí cca 75 miliard dolarů ročně, ale zisk spammerů je řádově o dvě nuly nižší. Jedná se o neefektivní ekonomickou činnost, která v klasickém ekonomickém prostředí nemá šanci na existenci. Síla spamu tkví právě v jeho atypičnosti.

Za vším hledej spam

Pokud se podíváte na vývoj spamu, lze si povšimnout, že to není jen neškodné reklamní sdělení, ale též zpráva rozeslaná s úmyslem poškodit příjemce finančně, tedy s cílem vylákat finanční prostředky. Jako příklad můžeme uvést tzv. nigerijské dopisy; podvodné zprávy s obsahem: „Mám 40 milionů dolarů a právě vy mi je můžete pomoci převést do Evropy, za zprostředkování nabízím provizi...“ Věřte, že rozeslání uvedeného typu e-mailu se vyplácí.

Spam ale může příjemce poškodit také technicky, a to devalvací jeho infrastruktury. Mezi takové druhy spamu patří zprávy, jejichž obsahem je speciální skript odkazující na infikované stránky s cílem nakazit počítač či podnikovou síť malwarem. Tento způsob využití spamu se označuje jako „Web Born Malware“ a boom zažívá právě v letošním roce.

Přestože na první pohled to není zřejmé, cíl tohoto druhu spamu bývá též finanční. Když se spammerovi podaří infikovat napadený stroj, tak se pokusí toto zombie (jak se označuje „počítač dvou pánů“) zapojit do různých botnetů a využít ho k páčání v lepším případě neetických aktivit, v horším případě nelegálních činnostech. Z výše uvedených příkladů je jasné, že spam je všechno jiné než neškodný a je třeba se proti němu chránit.

Důkazem všudypřítomnosti spamu a jeho adaptability vůči novým technologiím je fakt, že se začíná objevovat v prostředí instant messagingu. Pod názvem spam, tedy Spam Instant Messages, a též v prostředí internetové telefonie (s názvem spit, tedy Spam over Internet Telephony). O spamu v budoucnosti určitě ještě uslyšíme a ochrana proti němu není výsadou jen

velkých společností, ale nutností pro každou společnost, která využívá informační technologie.

Kladivo na spamery

V porovnání s dalšími bezpečnostními riziky je boj se spamem složitější, a to nejen z technického hlediska. Důvody této složitosti spočívají ve dvou oblastech:

1. Technicky je velmi obtížné odlišit spam od regulární pošty (nejsou stanovená jasná pravidla co je, a co není spam).
2. Spam je velmi úzce spjat s dalšími hrozbami typu virů, malware a phishingu.

Pro účinný boj uživatelé potřebují taková řešení, která dokáží jednak eliminovat všechny nežádoucí spam a jednak propustit všechny žádané a korektní e-maily.

Aby byl uvedený požadavek splněn, je nezbytné, aby řešení umožňovalo přizpůsobení parametrů hodnocení potřebám uživatelů. Vždy záleží na úhlu pohledu, jelikož to, co je pro technické oddělení spam, jím zdaleka není pro obchodní oddělení.

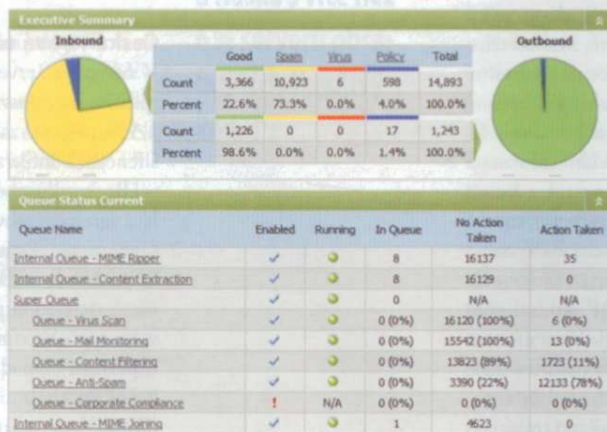
Dobrou zprávou je, že většina výrobců, které Gartner ve svém E-Mail Security Boundary Magic Quadrantu umístil do kvadrantu vedoucích firem (Leaders) a vyzývatelů (Challengers), plně splňují tento požadavek a dokonce umožňují přizpůsobení parametrů hodnocení jednotlivým uživatelům.

Mezi lídry trhu patří společnosti Cisco s řešením IronPort nebo Secure Computing s řešením IronMail, které má v sobě kromě „tradičních“ (11 metod) detekce spamu i detekci na základě reputací odesílatelů či reputací vnořených webových odkazů v rámci e-mailu a jež je napojeno na globální databázi kyberzločinců a spammerů TrustedSource.org.

Potřebnou funkcionalitou je též bezesporu rozšíření antispamových filtrů o ochranu před tzv. spam deriváty, tj. o ochrany před phishingem, viry a malwarem. Vzhledem k tomu, že spam je velmi často využíván k šíření těchto hrozeb, je prospěšné umožnit zákazníkům výběr antivirového enginu, a tím jim nabídnout možnost kombinovat různé AV enginy v síti s cílem zvýšit bezpečnost jejich sítí. Tyto funkcionality, především možnost výběru AV enginu, je výrobcem lehce opomíjena. Treba již zmíněný IronMail nabízí výběr mezi třemi AV enginy.

Vzhledem k tomu, že velká část společností má již schválenou svou vlastní bezpečnostní politiku, od moderní brány pro messaging by se měla očekávat schopnost vynutit od koncových uživatelů dodržování této politiky – ať už se jedná o šifrování, či o ochranu před únikem citlivých dat. Při výběru řešení je třeba dbát na to, aby bylo schopné tyto nároky zvládnout bez potřeby speciálních úprav stávající infrastruktury.

Autor je zaměstnancem společnosti ComGuard.



Report IronMail: Spamy dnes představují více než 70 % e-mailové komunikace