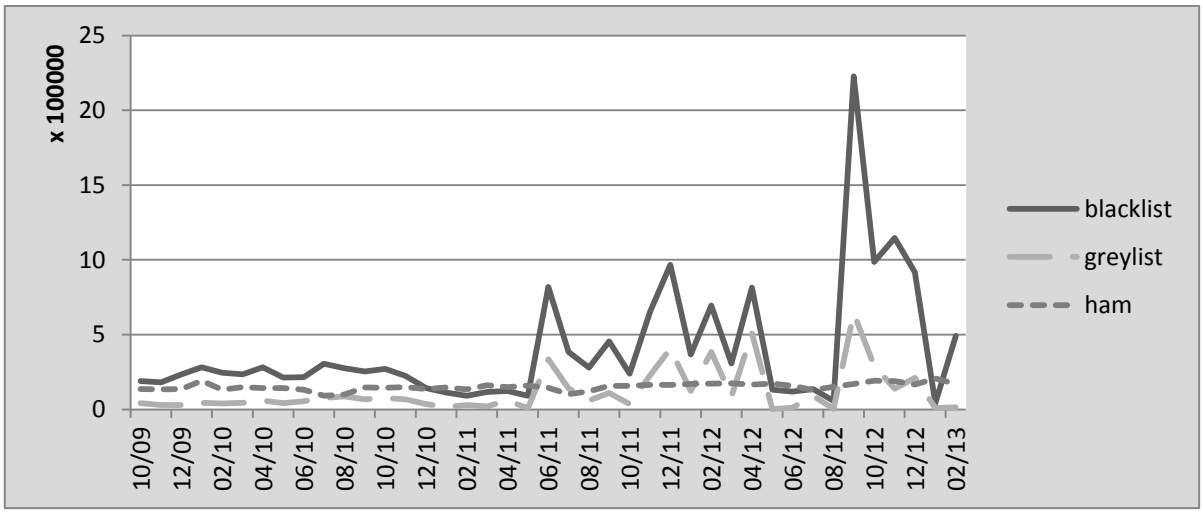
VYUŽITÍ MECHANISMU DNSBL

Michal Brož
m-broz@centrum.cz

Abstrakt

Jedním ze způsobů jak se chránit proti SPAMu je použití mechanismu blacklistů, který využívá DNS. Mechanismus blacklistů dostupných přes DNS se označuje DNSBL. Tomuto mechanismu se věnuje moje práce. Mechanismus DNSBL je kritizován pro vysokou chybovost, popřípadě že správci těchto blacklistů mají velkou moc, kterou mohou zneužít. Dotazy zda daná IP adresa zasílá spam či nikoliv jsou v případě OSU adresovány na spamhaus.org. Cílem této práce je seznámení s mechanismem DNSBL a následná analýza praktického využití na OSU. Podle výsledku provedené analýzy by mělo být rozhodnuto, zda je výhodné využívat tohoto mechanismu či nikoliv. Poté byla zjišťována slabá místa této ochrany a navrhnuty případné vylepšení.

Analýza příchozí pošty na OSU byla provedena z logů poštovního serveru od data, kdy se začal využívat mechanismus DNSBL, tzn. od října 2009 do února 2013. Odhaduje se, že více než 80% poslaných zpráv je spam [1]. Toto tvrzení se potvrdilo i na OSU. V analyzovaných měsících se někdy objevily velké výkyvy počtu obdržených spamů, viz obr. 1, což se odrazilo na poměru spamů k počtu regulérních zpráv (tzv. ham), avšak celkový poměr obdržených spamů, které byly odchyceny pomocí použití mechanismu DNSBL a nebo greylistingu byl okolo 80%. Počet IP adres, které zasílají na OSU spam, má klesající tendenci, avšak počet pokusů o doručení, které tyto adresy zašlou, má spíše vzrůstající tendenci. Překvapivým zjištěním bylo, že většina adres, ze kterých byl obdržen spam, zaslalo pouze jednu zprávu. Dalo by se totiž předpokládat, že boti budou zasílat spam na více mailů, které třeba ani nebudou regulérní. Dalším překvapivým zjištěním bylo, že okolo 10% obdržených spamů bylo adresováno na servery, které jsou sice ve vlastnictví OSU, ale nepředpokládá se, že by na ně byly adresovány maily. Tyto zprávy byly často adresovány na osu.eu.



Obr 1: Měsíční počty zadržených poštovních zpráv pomocí blacklistu a greylistingu v porovnání s počtem regulérních zpráv (ham)

Ve vybraných měsících byla provedena důkladnější analýza zpráv, které byly zablokovány díky mechanismu DNSBL. Byla ověřena životnost dotazů v těchto měsících, ale i životnost IP adres na blacklistu, aby se zjistil průběh doby, kdy uživatel případně požádá o vyřazení z blacklistu. V době jednoho měsíce od zaslání spamu by 5% zpráv prošlo kontrolou na spamhaus.org, po uplynutí dvou měsíců to už je 20%, a po uplynutí delší doby to je i okolo 30%. Průběh životnosti IP adres na blacklistu byl obdobný, ale maximální úbytek adres byl okolo 20%. Dá se říci, že čím více se blíží

počet milně zablokovaných dotazů k počtu milně zablokovaných adres, tím větší chybovost se očekává. Ve vybraných měsících byla chybovost mechanismu DNSBL zjišťována. Byly ověřovány maily, které podle domény měly být odeslány z ČR. Odhalování bylo značně ztíženo tím, že velký počet mailů, které byly zachyceny, mělo existujícího odesilatele i příjemce. Následné ověření IP adresy však ukázalo, že tyto maily nebyly zaslány z ČR, ale převážně z Ruska a Ukrajiny. Většina adres, o kterých lze tvrdit, že jim bylo zakázáno doručení regulérní zprávy, byly zprávy typu newsletter, u kterých se dá očekávat, že uživatelé se stali odběrateli těchto zpráv. Takovýchto zpráv bylo objeveno v daném období několik desítek. Výskyt mailů, které byly zablokovány a nebyly typu newsletter, byl mimořádný. Za celé období této důkladnější analýzy zpráv bylo takovýchto mailů odhaleno okolo desítky. Dá se tedy předpokládat, že chybovost blacklistu je opravdu minimální.

Dle výše uvedených údajů se využívání mechanismu DNSBL zcela určitě vyplácí. Zamezuje velkému množství spamu a chybovost je téměř nulová. Tato ochrana využívá výhody DNS, ale má i její nevýhody. V průběhu zpracování této práce byl spamhaus.org pod útoky hackerů, kteří jej chtěli shodit. Nelze vyvrátit, že by se jim to někdy mohlo podařit. Podvržení DNS záznamů je poměrně dosti nepravděpodobné, protože by to nemělo velké využití. Velký počet dotazů které jsou prováděny na spamhaus.org jsou zcela zbytečné z důvodu, že zprávy jsou adresovány na maily, které neexistují. Šlo by to teda do značné míry omezit provoz na spamhaus.org tím, že by prvně byla prováděna kontrola, zda příjemce mailu existuje.

Klíčová slova: *Spam, Blacklist, DNSBL*

Literatura

1. **Cisco Systems, Inc.** Global Spam Volume. *Cisco IronPort SenderBase Security Network.* [Online] [Citace: 4. Duben 2013.] http://www.senderbase.org/home/detail_spam_volume?displayed=last18months&action=&screen=&order