Opensource antispamová ochrana

Jiří Ráž

Plzeň 31. října 2013

CESNET z.s.p.o.

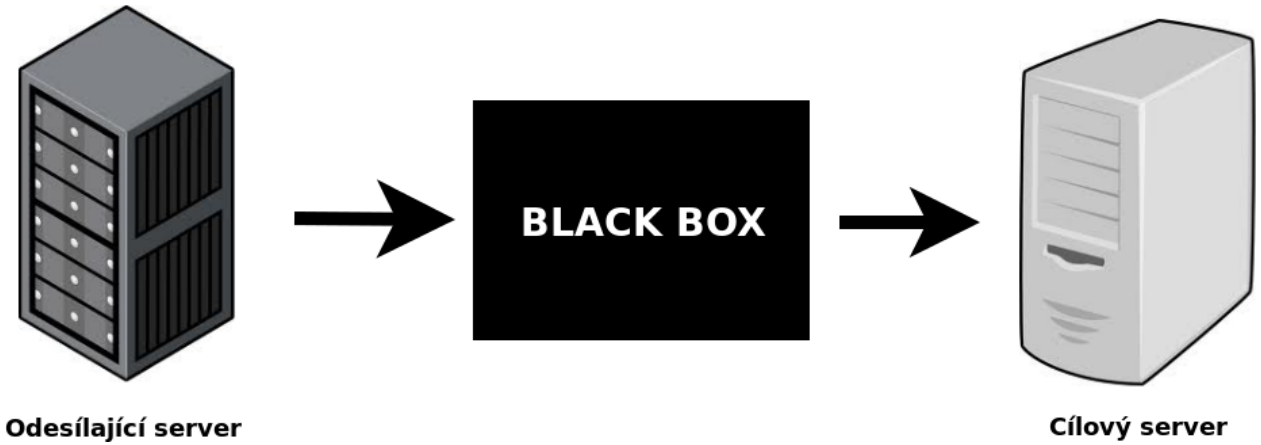
- Založen v roce 1996
- 25 českých univerzit + Akademie věd České republiky
- Hlavní cíle (připojit se může každý, kdo těmto bodům vyhoví)
  Provoz a rozvoj sítě CESNET2
  Podpora vědy a výzkumu v oblasti pokročilých síťových technologií a aplikací
  Podpora a šíření vzdělanosti, kultury a poznání
- Připojené organizace:
  Univerzity, CAS Státní správa, městské úřady Střední školy, knihovny, muzea apod.

Spam, spam, spam, ...

- Nevyžádaná pošta
- Pravděpodobně první byl rozeslán 1. května 1978 v ARPANETu
- Zpočátku jen jako reklamní, později zneužíván k phishingu
- Objem spamu přesahuje 90% veškerého provozu
- Poměrně jednoduché, levné a těžko postihnutelné
- K šíření se s oblibou využívá botnetů a open relay serverů
- Uživatelé jsou obecně velmi náchylní ke kompromitaci počítače e-mailem, často zaměnují vyžádanou komerční zprávu za spam a naopak

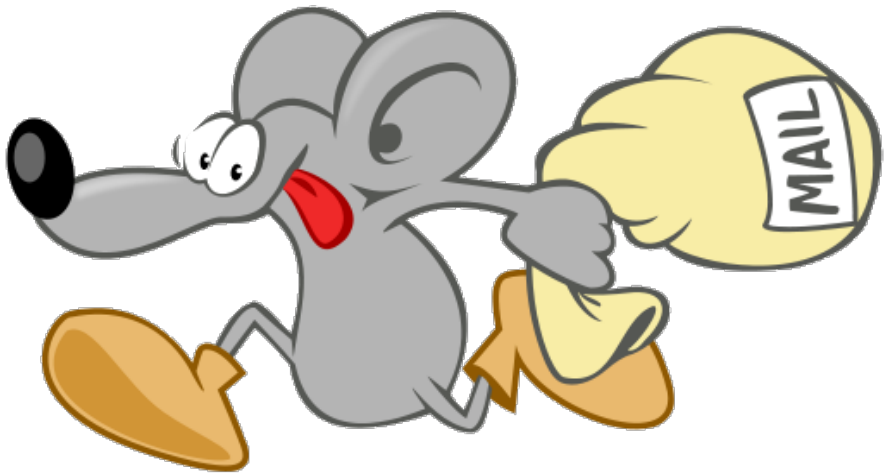
Filtrování pošty – komerční řešení

- Předáváme poštu, seznam uživatelů třetí straně
- Nemáme kontrolu nad nastavením
- Prakticky nelze vytvářet vlastní vyjímky, pravidla
- Težko napojitelné na interní databázi
- Služba může běžet v jiné zemi, pod odlišnou jurisdikcí
- Cena se většinou odvíjí od počtu uživatelů
- Naopak ideální řešení pro malé firmy



Omezení na úrovni MTA – Postfix

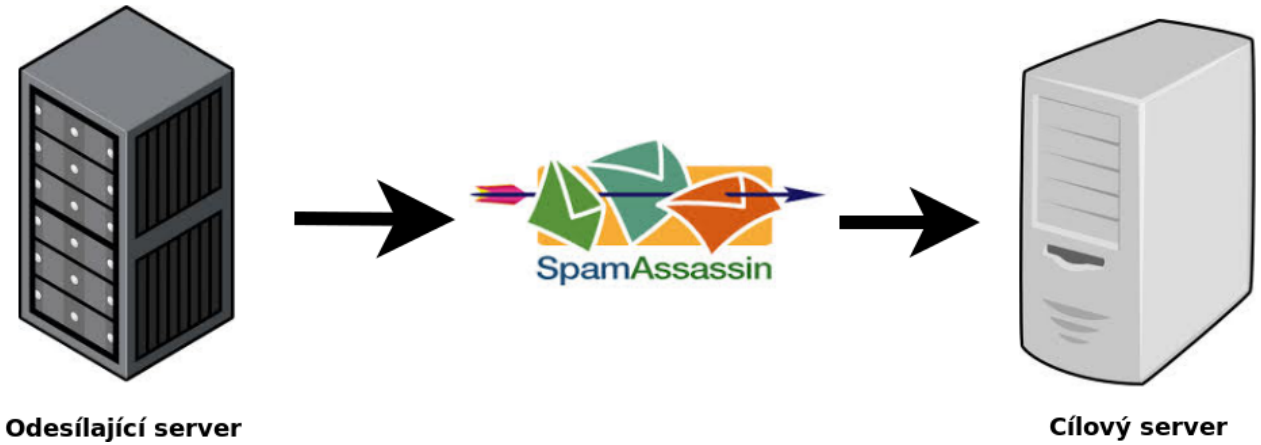
- Přijímáme pouze korektní e-mailové adresy
- Přijímáme pouze existující domény
- Vyžadujeme korektní pozdrav serveru EHLO
- Přijímáme poštu pouze pro povolené domény, existující uživatele



CESNET

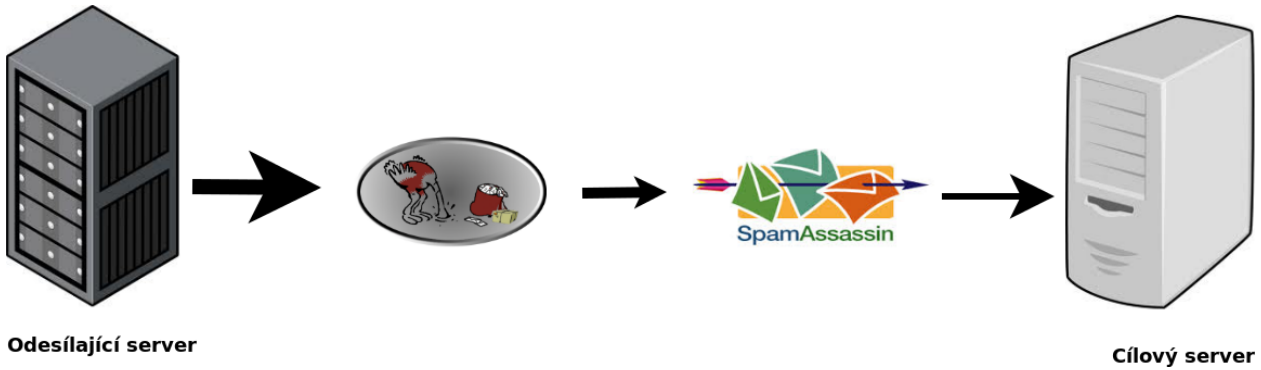
Antispamový filtr – Spamassassin

- Filtr obsahu zpráv od Apache Foundation
- Provádí rozličné testy a podle výsledku hodnotí zprávu
- Poměrně spolehlivé řešení, ovšem náročné na výkon serveru
- Kontrolována je veškerá příchozí pošta
- V případě velkého zatížení dochází ke zpoždění
- Můžeme vytvářet vlastní pravidla, vyjímky
- Umí spolupracovat s antivirem ClamAV



Greylisting – SQLgrey

- Využívá lenosti spamujících strojů
- Při prvním pokusu o doručení poštu odmítne
- Vetšina spamujících strojů se o další pokus nepokusí
- Spožďuje legitimní poštu, občas i o desítky minut
- Umístěním před Spamassassin snížíme zatížení serveru



Nolisting

- Obdobně jako greylisting využívá lenosti spamerů
- Nasměrování MX záznamu na adresu, kde nic nebeží
- Lepší varianta je konfigurace postfixu, která poštu jen odmítá
- Máme přehled o odmítnuté poště
- Težko lze prokázat účinnost tohoto řešení

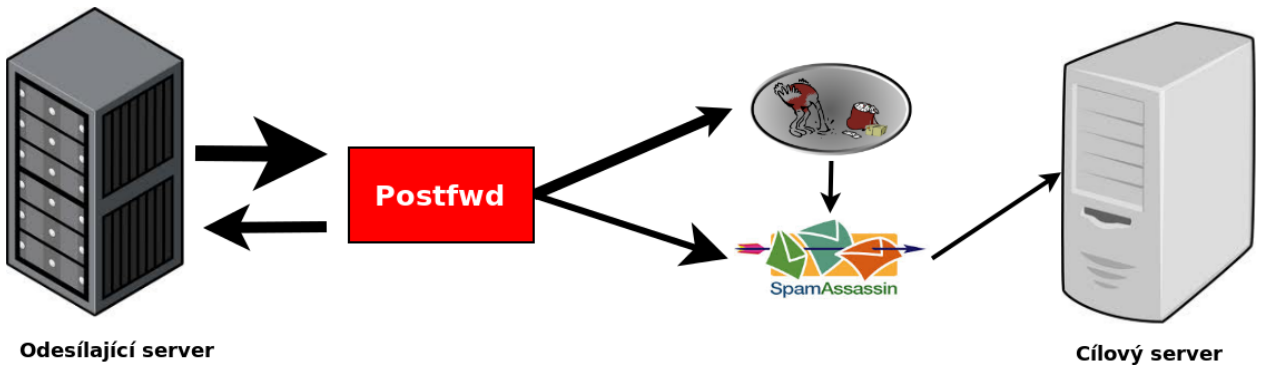
Blacklisty a whitelisty

- Seznamy spamujících IP adres
- Podmínky zařazení na blacklist se různí podle provozovatele
- Pro dotazy se využívá protokolu DNS
- Odmítat poštu na základě jednoho blacklistu je riskantní
- Kombinace více blacklistů přímo v MTA je komplikovaná
- Většinou bezplatné pokud nepřekročíte určenou hranici dotazů
- Velkým problémem jsou sítě s dynamicky přidělovanými adresami

CESNET

Krotíme blacklisty – Postfwd

- Postfix firewall daemon
- Vytváření filtrovacích pravidel na základě, IP adresy, odesílatele a příjemce
- Hodnocení odesílatele z více blacklistů a smtp spojení
- Umožňuje různá omezení podle získaného hodnocení
- Citelně sníží zatížení serveru
- Postfwd si výsledky testů ukládá do paměti
- Zprávy nemusíme jen odmítat, můžeme aplikovat limity

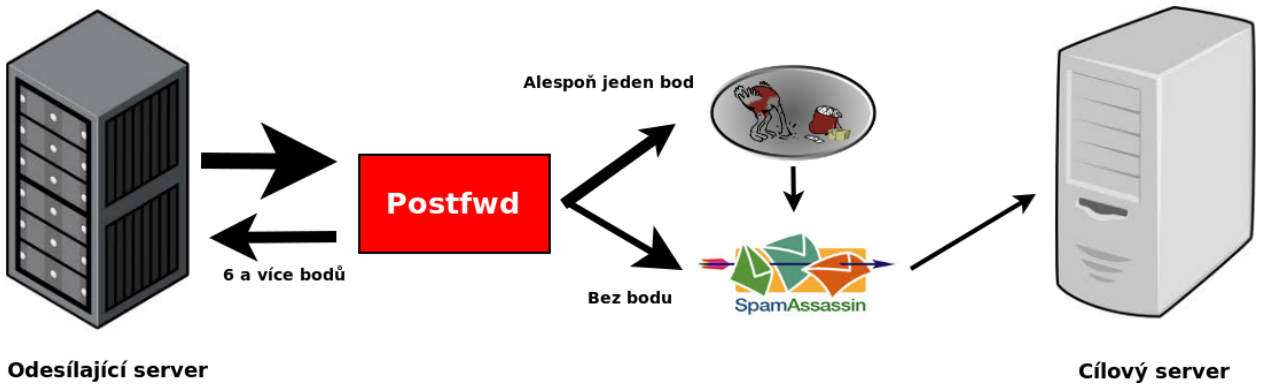


Příklad konfigurace – Postfwd

- Má adresa korektní reverzní záznam?
- Je reverzní záznam stejný jako EHLO?
- Vyskytuje se IP na jednom z pěti blacklistů?
- Vyskytuje se IP na whitelistu?

- Za každý prohřešek získá odesílající server 1 bod

- V případě 0 bodů pošleme poštu přímo spamassassinu
- V případě 1-5 bodů pošleme přes sqlgrey
- V případě 6 a více bodů zprávu odmítneme
- Do zprávy o odmítnutí můžeme vkládat vlastní text i výsledky testů



Vytváření pravidel – Postfwd

- Název pravidla
  - Slouží k identifikaci a vytváření statistik
- Samotné pravidlo
  - Popisuje samotnou kontrolu, může obsahovat makra
  - Například: *client_name = !! $$helo_name*
- Akce
  - Co se provede při nalezení shody
  - Nastavení čítače, přechod na jiné pravidlo
  - Návrat do postfixu s nějakou třídou omezení
  - Návrat do postfixu s výsledkem, OK, REJECT...
- Například:
  id=SET_NAME;
  client_name = !! $$helo_name;
  action=set(HIT_helo=1)

ClamAV

- Filtr škodlivého kódu nejen pro linux
- Kontroluje zprávu, přilohy i archivy
- Použití v kombinaci se spamassassinem jako modul
  Přidává pouze bodové ohodnocení a případně hlavičku
- Může fungovat i jako samostatný filtr pošty
- Pravidleně aktualizovaná databáze vzorků
- Kontrola, je náročná na výkon systému

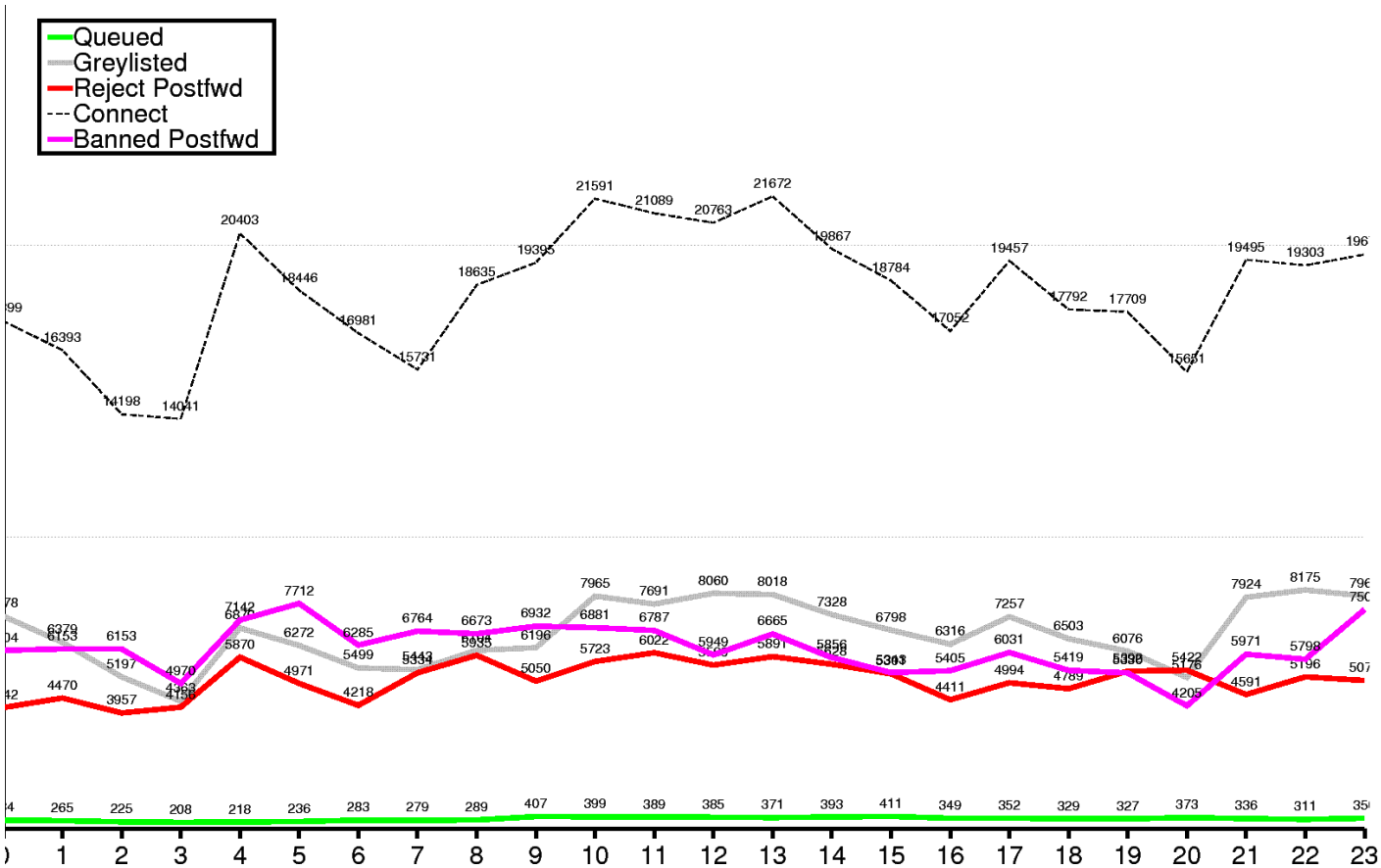
Fail2ban

- Aby toho nebylo málo, můžeme vytvářet vlastní seznamy škodících adres
- Postfwd umí číst data z externího souboru
- Fail2ban generuje seznam, například podle neúspěšnosti odesílatele (550)
- Následně jako první pravidlo pro Postfwd přidáme kontrolu na tento seznam
- Získáme operativní blokování adres, které se ještě nevyskytují na blacklistech
- Fail2ban zajistí po nastavené době odblokování
- Oproti blokování na úrovni iptables máme přehled o odmítnutých zprávách

CESNET

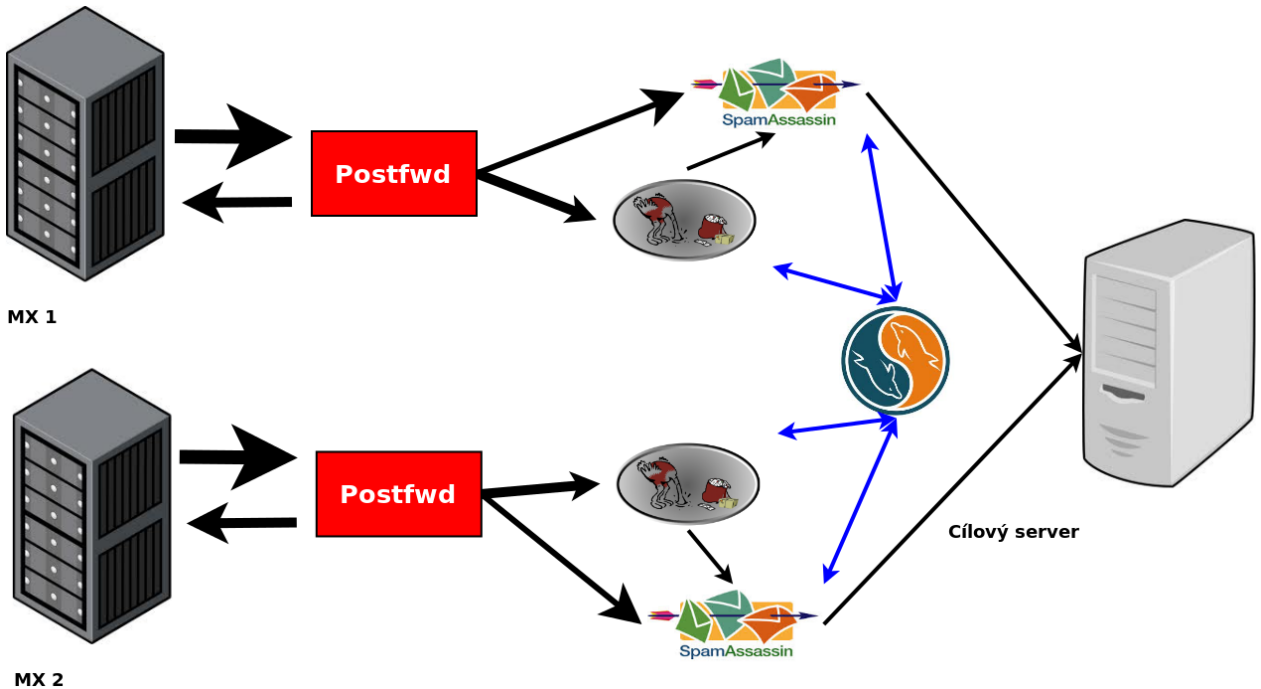
Ukázka z provozu

- Jeden den provozu 25. září 2013



Robustní řešení mailového systému

- Pokud používáme spamassassin s podporou MySQL a SQLgrey můžeme postavit redundantní řešení se sdílenou databází
- SQLgrey má k dispozici stejné záznamy na obou serverech
- Spamassassin má k dispozici stejné vzorky
- Databáze je obousměrně replikovaná
- Servery mohou být v rozdílných lokalitách, na různých distribucích



Záludnosti sdílené databáze

- Spamassassin je třeba upravit pro práci se sdílenou databází
- V modulu *Mail/SpamAssassin/BayesStore/SQL.pm* je třeba vyměnit veškeré příkazy INSERT za INSERT IGNORE
- Jinak dojde ke zkolabování replikace, pokud již záznam v databázi existuje

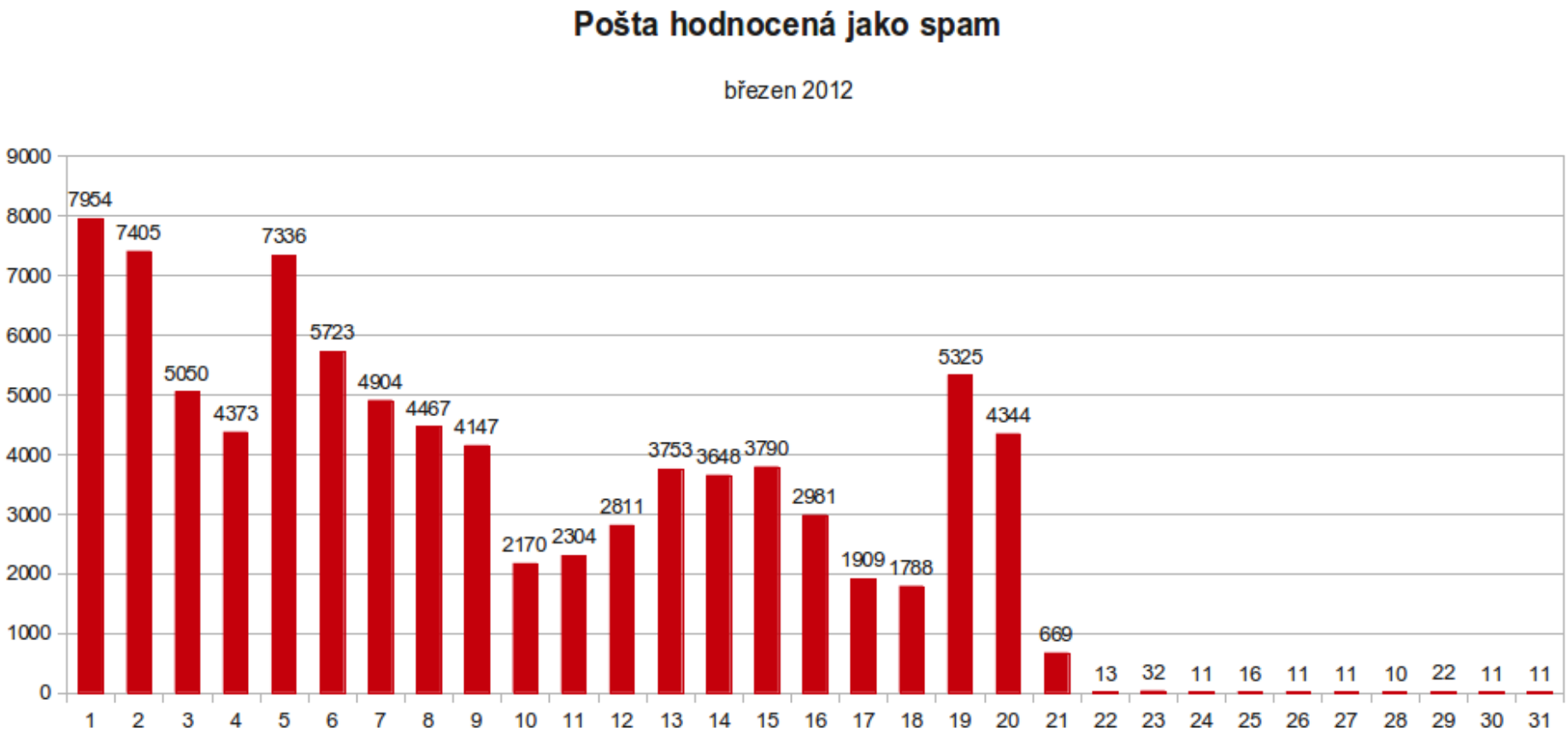
- Pokud používáte AutoWhitelist je třeba upravit modul:

Mail/SpamAssassin/SQLBasedAddrList.pm

```
my $sql = sprintf("INSERT INTO %s (%s) VALUES (%s) ON DUPLICATE
KEY UPDATE count = count + 1, totscore = totscore + %s",
$self->tablename, join(',', @fields), join(',', ('?') x @fields), '?'); my $sth =
$self->dbh->prepare($sql);
```

- v podstatě se jedná o přidání funkce ON DUPLICATE KEY UPDATE

Úbytek spamu po nasazení



Zdroje

- http://www.postfix.org/
- http://spamassassin.apache.org/
- http://sqlgrey.sourceforge.net/
- http://postfwd.org/
- http://www.mysql.com/
- http://www.apache.org/
- http://www.clamav.net/

Závěr

Děkuji za pozornost