Борба срещу нежеланите съобщения (spam) с класически и съвременни средства

представени от Георги Чорбаджийски
georgi@unixsol.org
http://georgi.unixsol.org/

Асоциация за информационна сигурност
http://iseca.org/

Проблемът spam

- Нежелана комерсиална поща
- Други видове spam
  - comment spam
  - sms spam
  - IM spam (SPIM)
  - junk calls
  - voice message spam
  - windows messaging spam
  - spamdexing
- Защо се нарича „spam“?

Защо има spam?

- Причините са финансови
  - има глупави хора, които купуват от спамерите
  - дори при .01% успеваемост, спамерите печелят
- Сравнително лесно е да спамваш
  - продават се програми, които улесняват спамерите
  - продават се и адреси на потенциални „клиенти“
- По-принцип не е незаконно
  - това е на път да се промени, но не към добро :(

Как се изпраща spam?

- Чрез "spam friendly" ISPs
  - на думи всички са против, но на практика...
- През open email relays
- През отворени прокси сървъри
  - много админи не настройват коректно сървърите си
- През зомбирани MS Windows машини
  - дори и да не ползвате Windows, всички страдат заради заблудените му потребители
- През бъгави web приложения
  - основно скриптове за изпращане на поща
  - откриват се лесно с търсене в google
  - осигуряват анонимност на спамерите

Как ви "намират" спамерите?

- Купуват емайл адреса ви заедно с 50 милиона други накуп
  - предлагат се CD-та с такава информация т.н. „Millions CDs“
- Претърсват интернет страници за емайл адреси
- Претърсват news групи за емайл адреси
- Атакуват със списъци с често използвани имена (joe@xxx, john@xxx, georgi@xxx)
- Компании, чиито услуги ползвате продават данните за вас

Методи за борба със spam

- tarpitting
- филтри
- черни списъци
- бели списъци
- сиви списъци
- challenge/response
- bayesian филтри
- SPF (Sender Policy Framework)
- DNSBLs (DNS block lists)
- DCC (Distributed Checksum Clearinghouses)

Как да се пазят потребителите

- Не поддържайте спамерите като купувате от тях!!!
- Подсигурете си машината
- Не давайте емайл адреса си навсякъде
- Ползвайте throw away адреси за сайтове, на които не вярвате
- Внимавайте, когато четете поща
  - web bugs
- Филтрирайте пощата си
- Не отговаряйте на spam
- Не отваряйте адреси посочени в spam поща
- Не стойте безучастни!
  - оплаквайте се на ISP-то на изпращача на spam-а

Как да се пазят ISP-тата

- egress и ingress филтриране
- Четене и реагиране на abuse@example.isp
- Използване на комбинация от методите за защита обяснени преди малко
- AUP
  - изключване на заразени машини от мрежата
  - изключване на спамващи машини
  - недопускане на известни спамери в мрежата

Какво ползвам аз срещу spam?

- qmail + безброй пачове
  - tarpit
  - изискване за валиден домейн на изпращача
  - изискване за валиден MX на изпращача
  - черни списъци и регулярни изрази в badmailfrom
  - qmail qFilter с custom фрази и правила
- Няколко чужди DNSBLs
- Български DNSBL - cbl.iseca.org (http://cbl.iseca.org/)
- SPF
- Черен списък: http://web.greens.org/etc/r.txt

Връзки

- Anti spam portal
  - http://spamlinks.net/
- Spam Prevention Early Warning System
  - http://www.spews.org/
- spamassasin
  - http://spamassasin.org/
- DSPAM
  - http://dspam.nuclearelephant.com/
- Vipul's Razor
  - http://razor.sourceforge.net/
- Сайтът на вашия MTA :)

Благодаря за вниманието!

Имате ли въпроси?

ISECA
Association for Information Security