Spam včera, dnes, a bohužel asi i zítra

Jan Kasprzak

`http://www.fi.muni.cz/~kas/`

Obsah přednášky

- **Úvod –** co je spam, historie.
- **Elektronická pošta –** SMTP, formát zpráv, vrácené zprávy, DNS, relaying.
- **Spam –** principy fungování, způsoby rozesílání.
- **Protiopatření.**
- **Praktické rady –** jak postupovat, abychom měli spamu co nejméně; jak postupovat, abychom neomezovali uživatele.

Historie

- **Co je spam? –** nevyžádaná komerční hromadně rozesílaná pošta (UCE/UBE).
- **První spam –** 1. května 1978, pozvánka na prezentaci firmy Digital Equipment. Zpráva napsaná ručně, včetně všech adresátů. RMS prohlašuje, že toto využití pošty může být do budoucna zajímavé.
- **První komerční spam –** 5. března 1994, nabídka právních služeb („Green card spam“).

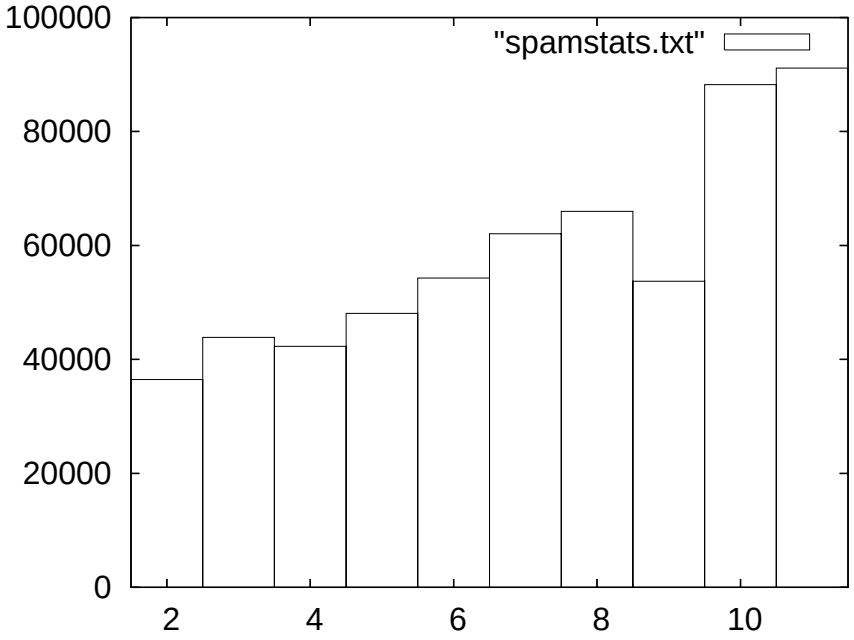
Název

- **SPAM –** zkratka z „Hormel *sp*iced h*am*“.
- Ochranná známka, Hormel povoluje užití slova spam nebo Spam pro hromadně rozesílanou nevyžádanou poštu.
- **Monty Python SPAM sketch**

Hormel's SPAM

Současný stav

- **Spam pro autora –** jen co zachytil spamový filtr.



- **Viditelný nárůst v cca posledních dvou měsících.**
- **91132 spamů za listopad –** více než dva spamy za minutu.

Formát zpráv

- **RFC 822**, novela RFC 2822.
- **Hlavičky, tělo –** oddělené prázdným řádkem.
- **Hlavičky –** jen US-ASCII.
- **Tělo –** jen US-ASCII, není-li v hlavičce řečeno jinak.

MIME

- **Interpretace těla zprávy**
- **Jednoduché typy –** `text/plain`, `image/jpeg`, `aplication/vnd.x-msword`, ...
- **Složené typy –** `multipart/alternative`, `/mixed`, `/parallel` ...
- **Stromová struktura –** složený typ může mít části také složeného typu.

```
From lenbar@fi.muni.cz  Mon Dec  4 10:30:39 2006
Return-Path: <lenbar@fi.muni.cz>
Received: from tajem1.fi.muni.cz [147.251.48.144]
        by anxur.fi.muni.cz (Postfix)
        for <fi@fi.muni.cz>
Date: Mon, 04 Dec 2006 10:30:25 +0100
From: Lenka Bartoskova <lenbar@fi.muni.cz>
MIME-Version: 1.0
To:  fi@fi.muni.cz
Subject: Vanoce prichazeji
Content-Type: text/plain; charset=iso-8859-2
Content-Transfer-Encoding: 8bit
X-CRM114-Status: Good  ( pR: 5.8600 )
X-Bogosity: Ham, spamicity=0.000000
X-Spam-Status: No, score=-106.5 required=5.0

Vážení a milí,
vánoce jsou opět "za dveřmi" a s nimi i naše[...]
```

Protokol SMTP

- **RFC 821**, novela RFC 2821.
- **Zasílání zpráv.**
- **Obálka** – odesílatel, adresáti.
- **Zpráva** – hlavičky, tělo. Pozor – hlavičky $\neq$ obálka!

```
$ telnet mail.muni.cz smtp
Trying 147.251.49.9...
Connected to mail.muni.cz.
Escape character is '^]'.
220 arethusa1.fi.muni.cz ESMTP NO UCE NO SPAM
EHLO linux.cz
250-arethusa1.fi.muni.cz
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
```

```
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
MAIL FROM:<kas@linux.cz>
250 2.1.0 Ok
RCPT TO:<kas@mail.muni.cz>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: test

pokus
.
250 2.0.0 Ok: queued as 08220595087
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

SMTP – pokračování

- **Nedoručitelnost** – vygeneruje se zpráva o nedoručitelnosti (bounce).
- **Adresát bounce** – obálkový odesílatel původní zprávy.
- **Odesílatel bounce** – prázdný (<>).
- **Double bounce** – někdy se zasílá postmasterovi.

Problémy SMTP

- **Identita odesílajícího stroje** se neověřuje.
- **Informace z obálky** se nikde neověřují.
- **Bounce** – může jít na nesouvisející (podvrženou) adresu.
- **Bounce** – někteří zoufalci posílají na adresy z hlaviček :–(
- **Doménové koše** – často nezachovaná obálková adresa. Problém při dalším rozposílání (`fetchmail`).

DNS a relaying

- **Tolerance k výpadku –** nasazení záložních poštovních serverů.
- **DNS –** směrování pošty pro doménové jméno.
- **MX záznam –** (priorita, hostname) – pošta se posílá na stroj podle priority (best MX).
- **bez MX –** pošta se posílá na A záznam.
- **Relay –** přeposílající poštovní server (záložní MX, stroj v DMZ, ale i jiné případy).
- **Open relay –** je ochotna přeposlat jakoukoli poštu.

Spam – principy fungování

- **Nízká cena** – náklady nesou z velké části adresáti.
- **Velký rozsah** – k rentabilitě stačí malé procento úspěšných obchodů.

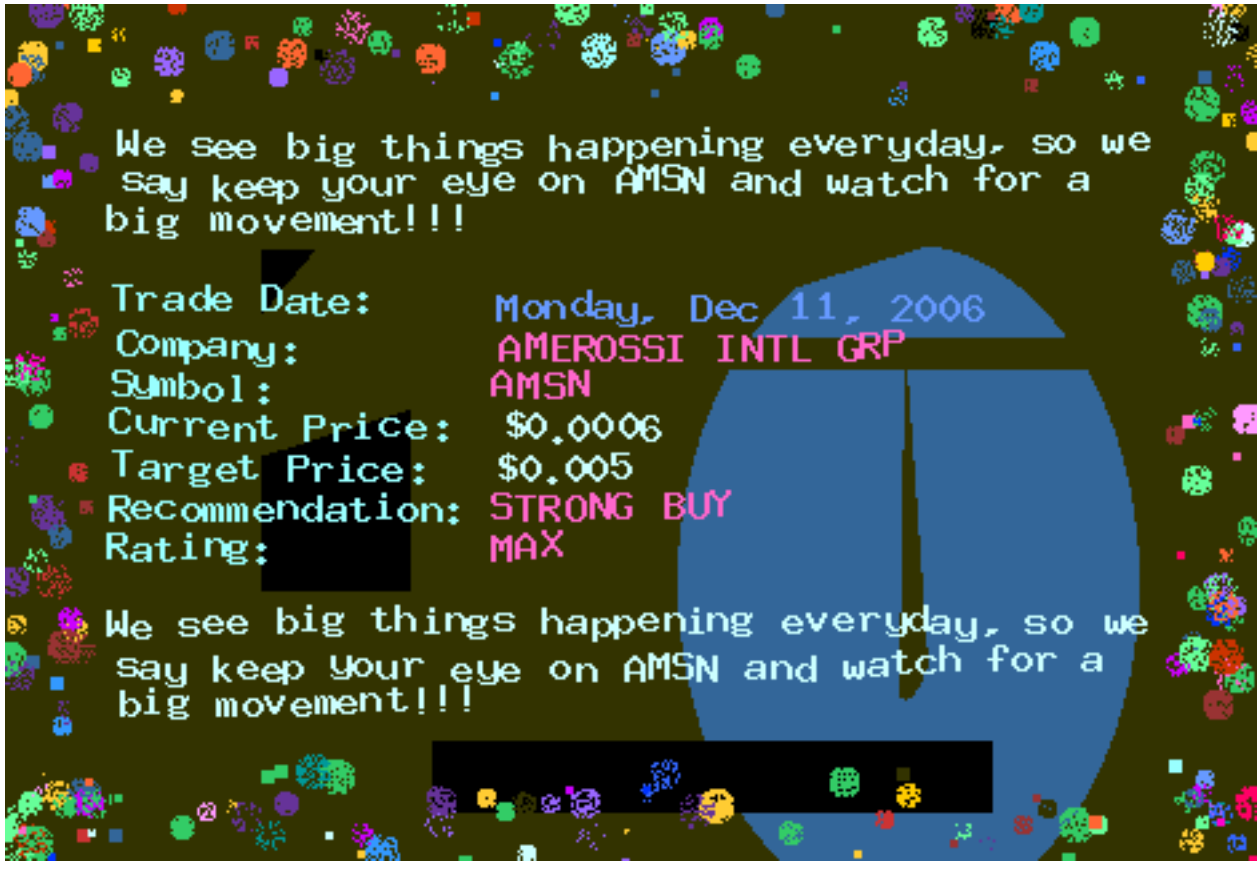
Jak se spam rozesílá?

- **Open relaye** – starší metoda, dnes v menšině.
- **Zombie** – napadené nezabezpečené stroje s Wind*ws, na nich běžící klientské rozesílací programy, centrálně řízené.

Dnešní spam

- **Personalizace** – snaha potvrdit si existenci adresy (unikátní kusy URL, externí obrázky v HTML, JavaScript, ...).
- **Zpráva v obrázku** – okolní text je naprosto nevinný. Obrázek konstruovaný pro ztížení strojového rozpoznání.
- **Adresy** – nalezené na WWW stránkách, slovníkové útoky, zneužití seznamu kontaktů v napadeném počítači, ...

Obrázkový spam



Metody obrany proti spamu

- **Pravidlo číslo 1 –** *nikdy* nekupujte zboží nabízené pomocí spamu.

Blacklisty/Whitelisty

- **Seznam serverů,** ze kterých šel v poslední době spam, open relaye, atd.
- **Ručně hlášené problémy,** často i skryté pasti (honey-poty).
- **Distribuce seznamu –** přes TXT záznamy v DNS.
- **Příklady:** SORBS, SpamHaus.org, SpamCop.net.

Problémy:

- **Na blacklist se může dostat i běžný server.**
- **Správce serveru musí sledovat, na kterých blacklistech se ocitl.**
- **Doporučení:** nepoužívat jako absolutní kritérium.

Kontrolní součty zpráv

- Zprávu už někdo jiný identifikoval jako spam.

Vipul's Razor

- **Kontrolní součty spamů.**
- **Přibližná kontrola –** snaha obejít některé odchylky ve formátování.
- **PyZor –** open source reimplementace, Python.

DCC

- **Distributed Checksum Clearinghouse.**
- **Kontrolní součty všech zpráv.**
- **Počet výskytů kontrolního součtu –** překročí-li limit, jde o hromadně rozesílaný mail.

Doporučení:

- Možno použít jako doplňující informace, ale pozor na false positives (mailing listy atp.).

Greylisting

- **Dočasné pozdržení zprávy.**
- **Zombie se už neozve.**
- **Klient se v mezičase dostane na blacklist.**
- **Kontrolní součet zprávy se v mezičase projeví jinde.**

- **SMTP server** – vyslechne si obálku, odpoví „451 dočasná chyba“.
- **Klíč** – IP adresa serveru, obálkový odesílatel a adresát. Pro tuto trojici zablokován přístup na 5–10 minut.
- **Běžný SMTP klient** – zkusí po hodině znovu. Ozve-li se do dvou dnů, přidat trojici na whitelist.
- **Zombie** – nemá frontu, už se neozve. Po dvou dnech přidat IP adresu na blacklist.
- **Whitelist** – projde-li IP adresa několikrát za sebou úspěšně greylistingem.

Greylisting II.

- **Rozhodně použít.**
- **Statistika –** u 91% (!) zpráv se SMTP klient se už neozval.
- **Pozor na relaye a záložní MX.**
- **Zatím funguje,** ale spammeři se časem přizpůsobí.

Hash cash

- **Zaplaťte strojovým časem.**
- **Inverze jednocestné funkce –** parametr závislý na obálkovém adresátovi (a případně obsahu zprávy).
- **Výpočetně náročné –** řádově vteřiny běžného CPU.
- **Princip funkce –** pro spammera náročné na generování ve velkém.
- **Problém –** mailing listy.

Identifikace odesílatele

- **Problém SMTP –** obálkový odesílatel může být podvržený.
- **Snaha identifikovat odesílatele.**
- **Seznam adres,** oprávněných odesílat poštu z dané domény.

SPF

- **Sender Policy Framework**
- **Seznam IP adres**
- **Implementace –** TXT záznam (fuj!) v DNS dané domény.

Domain keys

- **Kryptografický podpis zprávy** odesílajícím SMTP serverem.
- **Veřejný klíč SMTP serveru –** v DNS.

Problém:

Neřeší problém spamu, jen identifikace odesílatele.

Bayesovské filtry

- **Bayesův vzorec –** podmíněná pravděpodobnost.
- **Paul Graham:** A Plan For Spam.
- **Využití –** pravděpodobnost toho že mail je spam za podmínky, že obsahuje určitá slova (jejichž pravděpodobnost výskytu ve spamech a nespamech známe).
- **Strojové učení –** stačí poskytovat nové (chybně rozpoznané) instance spamu a nespamu.

Metody učení

- **Train only errors –** lepší odezva na chyby, ale delší proces učení.
- **Train until no errors –** vylepšení téhož. Nutno držet korpus spamu a nespamu.
- **Train everything –** doporučované pro bayesovské filtry.
- **Automatické učení –** zprávy určitého stupně jistoty.

Bayesovské filtry II.

Implementace

- **Bogofilter**
- **SpamAssassin bayes**
- **SpamBayes**
- **SpamProbe**

Výhody

- **Individuální naučení –** spammer předem neví, co projde.
- **Přizpůsobení se trendům.**
- **Reaguje na úmyslné překlepy –** V1agra, porrnn, ...

Nevýhody

- **Obrázkový spam –** neúčinný; často doplněno textem pro zkažení učícího se filtru.

Další učící se filtry

CRM114

- **Bayesovská klasifikace.**
- **Markovovské řetězce.**
- **Další experimentální metody.**
- **Zkušenost:** dobré výsledky s TOE nebo TUNE. Lepší tolerance k degradaci přiloženými texty.

DSPAM

- **Bayesovská klasifikace –** i přes dvojice slov.
- **Databáze zpráv –** možnost později překlasifikovat zprávu podle ID.
- **Pro větší instalace –** DB backend, klient-server, různé způsoby filtrování.

Heuristiky – SpamAssassin

- **Sady pravidel –** je mail v HTML? Obsahuje neexistující adresu v hlavičce? Má chybně zakódované hlavičky? ...
- **Váhy pravidel** – dávají celkové skóre zprávy.
- **Hranice skóre** – zahození mailu.
- **Whitelist/blacklist** – ručně zadaný.
- **Auto whitelist** – na základě předchozí historie.
- **Uživatelská pravidla** – možná návaznost na jiné antispamové systémy.
- **Bayesovský filtr.**
- **Klient-server.**

Problém:

- **Globální nastavení –** je jednoduché ověřit, jestli mail „typickou“ instalací projde.

Best practices – doporučení

- **Použijte greylisting –** dokud ještě funguje.
- **Kontrolujte uvnitř SMTP spojení –** test existence obou adres v obálce (reverzní SMTP dotaz), zjevné spamy odmítat rovnou, kontrolovat nepovolený pipelining, ...
- **Použijte statistický filtr** nebo lépe:
- **... použijte dva různé statistické filtry –** nižší riziko false positive.
- **Použijte SpamAssassin** pro celkové vyhodnocení dostupných informací.
- **a hlavně ... vymyslete si vlastní řešení –** v rozmanitosti je síla.

Worst practices – co nedělat

- **Nedávejte adresy na web** (antiuživatelské opatření).
- **Nepoužívejte Qmail.**
- **Relaye jsou zlo.**
- **Záložní MX jsou zlo** – nastavte aspoň best MX = worst MX.
- **Negenerujte bounces** – nebo aspoň ne mimo svoji doménu.
- **Neupozorňujte automaticky na příchozí spam a viry.**

Spam tady bude stále

- **Obecná dostupnost služby –** cílem je mít dostupnou adresu/schránku, kam může zprávu poslat úplně kdokoli.
- **Vylepšování spamu –** obtížněji rozeznatelné obrázky, opisné formulace v textu, ...
- **Roste počet lidí s e-mailovou schránkou –** bude stačit i nižší rentabilita.

Možný vývoj obrany

- **Statistické filtry se závislostmi –** spam je obvykle spam, ale běžná pošta může být dost rozdílná. Filtrování např. podle zdroje.
- **Filtry nad částmi zprávy –** např. `Subject` a `From`.

Dotazy?

- Egg and bacon
- Egg, sausage and bacon
- Egg and spam
- Egg, bacon and spam
- Egg, bacon, sausage and spam
- Spam, bacon, sausage and spam
- Spam, egg, spam, spam, bacon and spam
- Spam, sausage, spam, spam, spam, bacon, spam, tomato and spam
- Spam, spam, spam, egg, and spam
- Spam, spam, spam, spam, spam, spam, baked beans, spam, spam, spam and spam
- Lobster thermidor aux crevettes with a Mornay sauce served in the Provençale manner with shallots and aubergines, garnished with truffle paté, brandy and with a fried egg on top and spam