Stopping Spam: Five Years in the Trenches

Jonathan M. Bresler

jmb@FreeBSD.org

Oct 20, 1999

Stopping Spam: Five Years in the Trenches

Jonathan M. Bresler

jmb@FreeBSD.org

Oct 20, 1999

Spam...worse than junk mail

- Junk mail is slow (time based cost of entry).
- Junk mailers pay (at least printing and nominal mailing cost).
- Postal Service laws and regulations eliminate whole classes of junk mail...these do appear as spam email.
- Junk mail is has fewer sources.
- Spam email is too fast, too cheap, too easy.

Spam Sources–in order of frequency

- Greed: get rich quick; stock tips; pyramid schemes.
- Lust: images; live(?) shows; Pamela Anderson videos.
- Fear and neighborliness: "Happy Times" warning messages.
- Politics (rare): East Timor and Iraq.
- cluelessness...mail loops.

Spam Control

- Prevention: at point of origin (ISPs, ASPs, Mail Hosting Services)
- Mitigation: at relays points and the destination http://www.mail-abuse.org/
- Retaliation: directed at the source or path

Spam Control at the MTA

- MTA based
  - DNS must contain PTR records
  - SMTP HELO hostname must have a DNS record
  - IP address must be match RBL, DUL, or RSS
  - Domainname must not appear in spammers list

Spam Control at the Mailing List

- Mailing List Software based
  - Closed lists with few approved senders
  - Headers must be RFC "friendly"
  - Headers must not contain spam identifiers
  - Body must not contain spam identifiers

Database Lookups (external)

- DNS: valid PTR records
- RBL: special case of PTR records
  http://maps.vix.com/rbl
- DUL: special case of PTR records
  http://maps.vix.com/dul
- RSS: special case of PTR records
  http://maps.vix.com/rss

Database Lookups (local)

- Domain names

xoticfantasies.com	bighits.com
investorsprofit.com	host4u.com
banneradvantage.com	byteme.com

- IP address ranges

199.4.121.93	204.137.220.

Header Filtering (correctness)

- missing headers: "Message-Id:"
- incorrect, illegal per RFCs: "Message-Id:"
- excessively long: "To:" "Cc:" "Bcc:"

Header Filtering (content)

- We have 80 header triggers
- infamous: "To: Friend@..."
- X-UIDL: POP protocol violation
- Spam mailer tag lines

Trench Coat Mailer	MailKing
Emailer Platinum	Mail-Gear
CyberCreek Avalanche	MailWorkZ

Content Filtering

- We use 60 content triggers
- Common spam phrases

CALL TO ORDER	NO OBLIGATION
EMAIL MARKETING	WE OFFER
WORLD RECORD SEX	EMAILS FOR SALE

- Others

Not for mail	BSB-Publishing
X-Loop: FreeBSD.org	news2mail

Monitor the Results

- Divert all content filtered mail into a file for review.
- Review content filtered mail daily.
- Each time a new spam appears, examine it for characteristics that can be triggers for your filters.
- Ask your users to forward you a copy of spam received...with all the headers.

Check List

- DNS–Spammers tend to be misconfigured.
- Whois–Consider an embargo of all domains owned by the spammers.
- RBL, DUL, RSS–stop spam at your door.
- Adcomplain–report spam, encourage ISPs to act.
- TcpWrappers–Decide who sends you mail.
- Procmail–both personal and site spam filtering.
- SpamBouncer & JunkFilter–procmail recipes

Changes in Spam

- Both Mailer and Content tag lines have largely disappeared
- Headers are mostly compliant
- Addressed, not broadcast
- Foreign (non-US) spam
- Spammers still can not figure out DNS

The Road not Taken

- Procmail all incoming mail
- Expunging email addresses from the mail
- Moderation of the mailing lists
- Certain databases (ORBS)
- Active/Reactive/Proactive Measures

A Possible Future

- Marketers will not voluntarily stop.
- Recipient will continue to pay the costs of spam.
- Spam will come to resemble email.
- The growth markets are outside the US–both spammers and recipients.
- Spam will be with us always,
- We can control, not eliminate, the infestation.