Unwanted Emails

An overview of the issues: technical, legal, social and economic

Information Security Interest Group

Thursday, 18 March 2004

Mark Suter, Miju Systems

<mark.suter@miju.com.au>

Copyright (C) 2004 Mark Suter

Slides @ http://zwitterion.org/talks/

Disclaimer

IANAL

YSSARL

A Few Good Definitions

Unwanted emails include:

- Unsolicited Bulk Email aka "spam"
- Viruses/Trojans/Worms aka "malware"
- Bounce messages for either of the two above

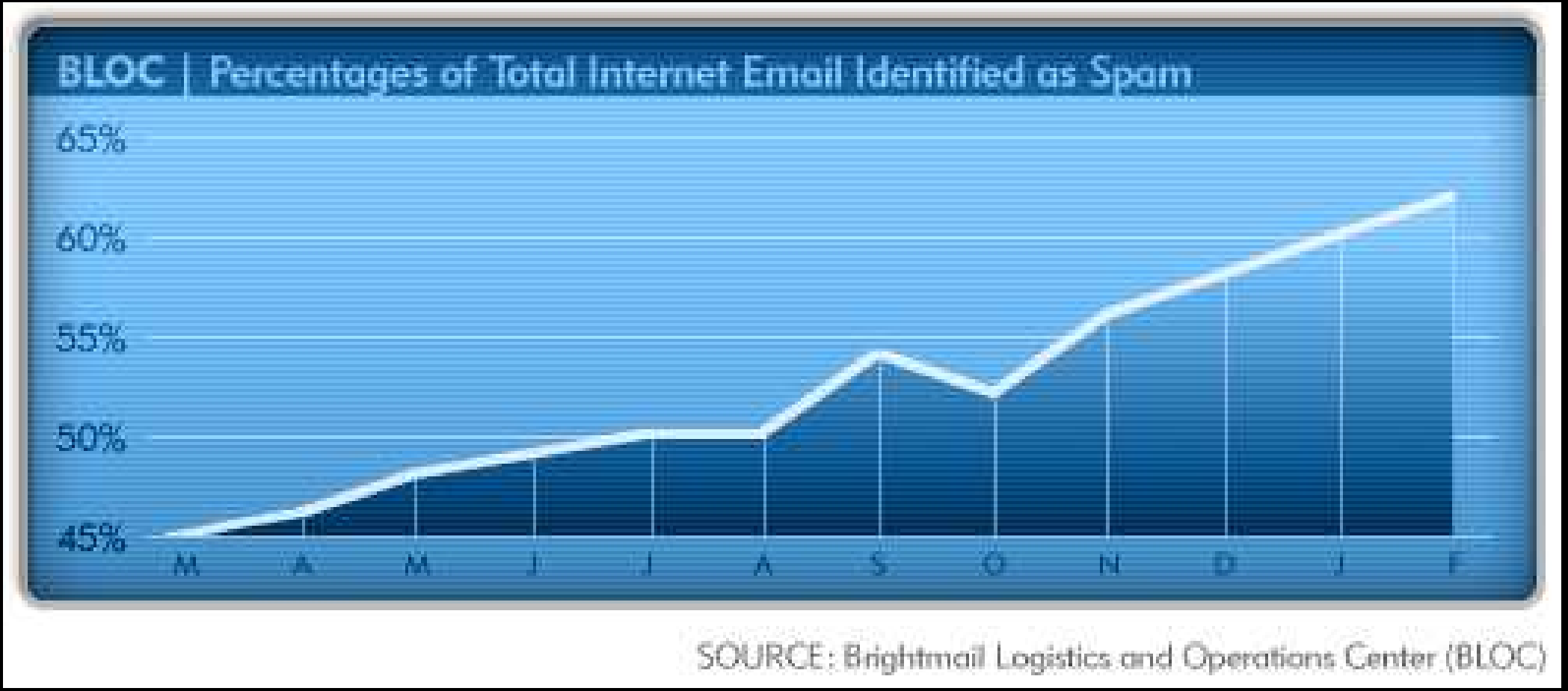
spam: CAUBE's definition

Spam is any electronic mail message that is:

- Transmitted to a large number of recipients; and
- Some or all of those recipients have not explicitly and knowingly requested those messages.

It does not matter what the content of the message is. It can be an advertisement for a commercial product, a solicitation for donations by a charity, or a religious pitch by somebody intent on saving your soul. If it meets the two criteria above, it is spam.

spam: The only way is up!



"spam levels hitting 60 percent of all email in January 2004, up from just 40 percent a year ago"

spam: What about SPAM(tm) cans ?

SPAM(tm) Luncheon Meat is a product of Hormel Foods:

- http://www.spam.com/ci.htm

Hormel Foods <publicrelations@hormel.com> denied my request to use a SPAM(tm) Luncheon Meat image from their media images website.

It took Hormel Foods sixty-five years to produce their six billionth can of SPAM(tm) meat (1937 - 2002).

spam: Economics

Great for the spammers:

- Low cost "advertising" for the spammer and their customer.
- Very low cost/message means low rates of return can be profitable.
- Nature of email means most of the cost is shifted to the recipients, unlike "junk mail".
- "I continue to be impressed by the agility of spammers." -- Dr Vinton G. Cerf

malware: What and Why?

The Viruses/Trojans/Worms filling our inboxes are changing. Once mostly harmless propagation, now also:

- Disrupt operations (ddos, zombie, etc)
- Send spam!
- Capture information (key-loggers, phishing, etc)

bounces: Why?

SMTP is a old protocol, designed in the early 70’s when security wasn’t an issue:

- "best-effort" delivery, either:
  - pass it on, or
  - send a bounce
- nothing to stop forgeries
- few controls for our security policy

bounces: Problems

Formerly correct behaviour is now a recipe for disaster, much like open relays.

- Bounce a forgery and you're sending the spam
- Bounce a virus (with body) and you're infecting someone
- Should we not send bounces / virus notifications?

Many of us have experienced the flood of bounces for emails we didn't send.

Soft costs

Unwanted emails

- Cost the recipient time
- Destroy the value of email
- Stifle other communications
- Weaken security

With time and groups of people, these costs quickly become significant.

solutions: where to act?

IMAP Internet Mail Access Protocol
LDA Local Delivery Agent
MTA Mail Transport Agent
MUA Mail User Agent
POP Post Office Protocol
SMTP Simple Mail Transfer Protocol

solutions: What Can We Do?

A wide range of solutions exist to implement our policies:

- IP Address blocks
- Reverse lookups
- Challenge-Response
- Cryptography
- Computational Challenge
- Content Filters
- The Law

Beware of the false-negative/false-positive issue.

solutions: Ethics of Filtering Email

Hopefully, fairly standard stuff:

- Breaks the gentleman’s agreement over email
- Have a written policy (often, just one page)
- Let it be known what you’re doing and why
- www.sage-au.org.au/ethics.html
- www.acm.org/constitution/code.html
- www.ieee.org/about/whatis/code.html
- www.isig.org.au/code_of_ethics.htm

solutions: IP Address blocks

One of the earliest methods, this continues to be popular.

- Getting the list
  - manually
  - rbls
  - honeypots
- Using the list
  - refuse connects
  - de-routing
- Updating the list

Many sites with large "black lists" are miss legitimate emails.

solutions: Reverse lookups

I mean this generally include many techniques to minimise forgeries:

- Reverse DNS checks
- Sender Policy Framework (and similar)
- Grey-listing (weakness in zombie SMTP engines)

Problems:

- smaller domains, vanity domains
- mobile users

solutions: Challenge-Response

The "confirm you're a human" challenges, sometimes using Interpretation Challenges.

Problems:

- mailing lists
- unexpected emails
- deadlock!
- unexpected and unsolicited, but not undesirable

solutions: Cryptography

Why not through some mathematics at the problem?

- By requiring signatures, unwanted emails can be discarded.
- Works within *limited* groups, or for special purposes
- Usability issues
- PKI anyone?

solutions: Computational Challenge

Require the sender to perform some work before you accept the email, for example, Microsoft Research’s Black Penny Project, often labeled "Postage".

Problems:

- Unequal taxation
- Mailing lists
- Robot armies (legal or zombie)

solutions: Content Filters

There are a lot of methods:

- Word lists
- Distributed Checksums
- Probabilistic systems (e.g. Bayesian networks)

Problems:

- Still sent, received and processed
- Arms race with spammers
- False-positives
- Need to review classifications

solutions: The Law

Australia’s Spam Bill 2004, effective from 10 April 2004:

- prohibits "unsolicited commercial electronic messages"
- requires accurate sender info
- requires functional unsubscribe
- prohibits "address harvesters" or list thus made
- covers email, SMS+MMS and IM
- doesn’t cover post, telemarketing and pop-ups
- doesn’t cover non-commercial spam

IANAL, YSSARL

Any more questions?

"Ask the next question"
Theodore Sturgeon (1918-1985)

Slides @ http://zwitterion.org/talks/