

Security and unwanted e-mail

Networkshop 31, York
April 2003

Rodney Tillotson
JANET-CERT
R.Tillotson@ukerna.ac.uk

Security and unwanted e-mail

- „ UBE
- „ Countermeasures
- „ APM

UBE

- Unsolicited
- Bulk
- E-mail

What?

- „ Advance fee fraud
- „ Dubious US mortgages
- „ Pornography
- „ Medication and treatments

- „ Not a content issue

Who?

- „ Mostly US
- „ Full-time contract bulk mailers
- „ Integral to a business
- „ Opportunist bulk mailers
 - Gullible or greedy marketers

Why?

- „ Because they can
- „ Very low marginal cost
- „ Response rate is minute

How?

- Exploit weaknesses of Internet mail
 - promiscuous protocol
 - recipient consent not considered
 - poor system administration practice
 - insecure systems
- Open mail relays
- Open proxies (Web etc)

Good mail

- SMTP
 - RFC 2821
- Header
 - RFC 2822
- Trace
- Relay

SMTP

- " HELO
- " MAIL FROM:
- " RCPT TO:
- " DATA

SMTP (2)

- HELO arien.ukerna.ac.uk.but.testing
- MAIL FROM:<spam-alert@ukerna.ac.uk>
 - Return-Path:
- RCPT TO:<victim@victim.domain>
- DATA
 - Not examined, includes header lines

Header

- From:
 - (same as MAIL FROM: in good mail)
- To:
 - (same as RCPT TO: in good mail)
- Date:
- Header lines take no part in message delivery

Trace

- Header lines Received:
 - added by each transferring mailer
- Received: from HELO-name
(PTR-name [connection-IP])
by own-name ...;
timestamp
- Message-ID: <arbitrary@own-name>
 - added if not present

Relay

- Message passed from mailer to mailer
 - within originating network
 - within recipient network
 - possibly between service providers
- Relaying useful or necessary
 - multiple hubs within a network
 - roaming users

Recipient view

- Header line From:
- Header line To:

- Took no part in message delivery

Good mail (reprise)

- SMTP
- Header
- Trace
- Relay

Bad mail

- „ Disregard of recipient wishes
 - UBE is unpopular
- „ Stealth and misrepresentation
- „ Theft of ISP resources
 - open relays
 - open proxies

Stealth

- „ Misrepresent source to recipient
 - header line From:
- „ Arrange to implicate another network
 - exploit open relays and proxies
- „ Confuse header readers
 - spurious Received: lines
 - find relays that write poor trace

Open relays

- Accept messages for other domains
- Typically misconfigured mail products
 - eg default installation

Open proxy

- Accept non-mail connections, make onward mail transfers
 - initiating the mail path
- Typically misconfigured Web products
 - eg Web servers and caches, SOCKS

Dedicated networks

- Some bulk mailers buy fast links
- They still misrepresent origin
 - MAIL FROM: to deflect bounces
 - From: to deflect complaints

Address lists

- „ Of very poor quality
 - invalid addresses
 - dictionary runs
- „ No incentive to improve
 - marginal cost close to zero
- „ Lists are traded

Security and unwanted e-mail

- (UBE)
- Countermeasures
- APM

Countermeasures

- Self-defence
 - Filtering by recipient or mailer
 - Blocking at recipient mailer
 - Both supported by community services
- Business pressure on perpetrators

Defensive

- „ Filtering on content
 - Sophisticated
 - Blacklists and signature services
- „ Blocking by origin
- „ Demanded by recipients
- „ Makes UBE survivable
- „ Increases aggression of bulkers

Pressure on perpetrators

- „ Identified from content
 - URLs etc
- „ Blocking by origin
- „ Complaints to service providers
 - some are ambivalent

Applying pressure (2)

- Community services
 - MAPS, ROKSO
- Hard work
 - pain before gain
- What can JANET do?

Legislation

- „ Much in place
 - US states, EU countries
- „ Ineffective across borders

ISP consensus

- BCP
 - LINX, RIPE

Whitelisting

- „ Default deny
- „ Allow certain source IP addresses
- „ Allow certain recipients
 - identified cryptographically
 - and other categories

ASRG

- „ Anti-spam Research Group (IRTF)
- „ Many old and new ideas
- „ Cryptographic payment schemes
- „ Replacements for SMTP
- „ Tweaks to SMTP, DNS etc
 - Designated Sender RR

Security and unwanted e-mail

- (UBE)
- (Countermeasures)
- APM

Assured Path Messaging

- A parallel universe
 - coexists with promiscuous mail
 - people might want two addresses
- No new technology
 - SMTP mailers with default deny
 - can use any emergent transport
- Bilateral links between providers
 - with relaying as necessary

Minimal central coordination

- „ Publish and maintain statement of standards
- „ Publish and maintain agreement template
- „ Maintain configuration advice for mail products in widespread use
- „ Occasionally broker between APMPs

Business case

- „ Can sell a quality mail service
- „ The service is cheap to run
 - UBE and other mail abuse are absent

Critical mass

- „ 'First telephone' problem
- „ Depends on adoption by big players
- „ Will need APMPs of last resort
 - at least at first

Outline requirements

- „ No UBE
 - spell out as necessary
- „ No support for UBE operators
- „ No messages illegal at either end
- „ Maintain and respect privacy of APM users
- „ Good practice in list management

- „ Document to be explicit

Outline agreement

- „ All mail across the APM link will conform to the requirements.
- „ No mail that is not APM will be introduced to the APM link.
- „ Parties publish their procedures for dealing with any abuse once identified.
- „ Parties will accept arbitration by the body managing the central APM facility.

Outline agreement (2)

- „ Relaying will be by agreement.
- „ A charge may be made for APM relayed to another party, on any basis acceptable to the two parties.

Steps needed

- „ Get international consensus on the two key documents
- „ Find an organization to provide the central facilities and promote the scheme widely
- „ Find an organization to provide initial relaying between APMs with no direct agreement

Could JANET do this?

- Does it help?

References

- Spamhaus
 - <http://www.spamhaus.org/rokso/>
- MailScanner
 - <http://www.sng.ecs.soton.ac.uk/mailscanner/>
- SpamAssassin
 - <http://spamassassin.org/>
- Bayesian filtering
 - <http://spambayes.sourceforge.net>