Spam, Security and SORBS v2.0

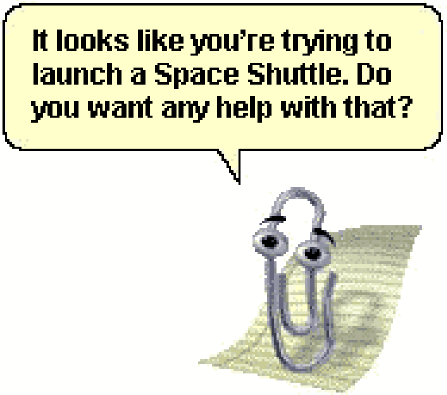
Michelle Sullivan
Engineering Director, GFI Software Ltd
Creator, Spam and Open Relay Blocking System (SORBS)
Email: michelle@sorbs.net
Tel: +356 79 543115

About this Presentation

- Provoking discussion.
- What is Spam?
- “Legal Speak”.
- The technical issue.
- The Network Security Problem.
- SORBS v1 / SORBS v2.0

Provoking Discussion

- My purpose is to provoke discussions.
  - and introduce you to SORBS v2.0
- Microsoft bashing.
- ISP bashing.
- Sales and Marketing bashing.


It looks like you're trying to launch a Space Shuttle. Do you want any help with that?

SORBS

What is Spam?

- Penis Enlargement Pill/Device Email?
- Bank Scams?
- Unsolicited Bulk Email (UBE)?
- Unsolicited Commercial Email (UCE)?
- All Unsolicited Email?
- All Advertising Email?
- All Email I don’t want?

SORBS Definitions

- SORBS Defines spam as:
  - Unsolicited Commercial Email
  - Unsolicited Bulk Email
- Some of the SORBS fallout:
  - Mailing lists that use their signup email for advertising, are spamming.
  - Opt-Out (Non Opt-In) mailing lists, get listed from time to time.

“Legal Speak”

- Australian Spam Act 2003
- The Privacy and Electronic Communications (EC Directive) Regulations 2003
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (2003) (aka “you CAN-SPAM from 2003”)

Consent and Inferred Consent

- Consent
  - I Give you permission to mail me…
    - » Is it really me…?
    - » Proof could be needed.
    - » Confirmed/Closed Loop Opt In
- Inferred Consent
  - I have a business relationship with you.
    - » Still need to know if it’s really me…?
    - » Better safe than sorry…

The Technical Issue

- How to stop spam..
  - Blacklisting
  - Greylisting
  - Whitelisting
  - Standards Enforcement.
  - Heuristics
  - AI type tests.

The Technical Issue

- How not to stop spam
  - Challenge Response
  - Accept then bounce
  - Delete/Drop/Silent Discard
  - Callout Verification
  - ‘Spam Folders’

Black / Block Listing

- Blacklisting
    - SORBS
    - Spamhaus
    - CBL
    - Spamcop
    - AHBL
    - NJABL
  - Advantages
    - Quick and simple checks.
  - Disadvantages
    - Sledgehammer where a scalpel is needed.

Greylisting

- Block senders/IPs by default.
    - Temporary Failures.
    - Unblock the IP/Sender automatically.
    - Servers retry every X period.
  - Advantages
    - Spammers don’t want to wait, they give up.
    - Bots don’t really care, they just retry (sometimes forever.)
  - Disadvantages
    - Mail is delayed.
    - Some servers don’t retry at all (eg: Yahoo!).

Whitelisting

- Useful in conjunction with Blacklists
- Useful in conjunction with Greylisting
- Block all, allow known good?
    - The principle of the firewall.
    - The principle of the SORBS Spam Firewall

Standards Enforcement

- RFC821/2821/1153 states:
  - HELO command must have a FQDN
    - » Address literals may be used.
  - HELO command must contain certain chars.
  - FQDN must resolve to an A record
  - <> (NULL) must be supported as a return path.
- RFC822/2822 states:
  - A valid From address must be supplied.

Heuristics

- Rules
- Patterns
- Scoring
- Accuracy

AI Type Tests

- Artificial Intelligence
  - Is there such a thing?
  - Learning Engines
    - Support Vector Machines
      - Kernel Hilbert Spaces and Hyper dimensional Planes

Challenge - Response

- Incoming message.
  - Test known/unknown
    - Known: Allow
    - Unknown: Send ‘Challenge’ and wait for ‘Response’
  - Advantages
    - Effective with most mail.
  - Disadvantages
    - Challenge Loops
    - Innocent People get spammed

Accept then Bounce “Backscatter”

- RFC 2821 states that if you accept a message you accept responsibility for delivery.
- Spammers, Viruses, Trojans routinely use fake addresses.
- SORBS produces and uses patched MTAs
    - Postfix patched for LibClamAV Integration
    - Postfix now uses libmilter and milter-clamav
    - Postfix can use grey-milter
    - Reject, don’t bounce.

Delete/Drop/Silent Discard

- RFC 2821 states that if you accept a message you accept responsibility for delivery.
- Rejects and Notification messages are there for a reason.
  - If you can’t reject, and you accept you must deliver.
  - Failure to deliver or notify results in perceived failure of email systems and data loss.

Callout Verification

- Sometimes called ‘Sender Verification’
    - Will connect to the MX of the domain in the ‘From’ address, and issues VRFY or RCPT TO commands to see if the email address used is valid.
  - Advantages
    - Ensures made up addresses cannot be used.
  - Disadvantages
    - Off loads spam prevention to innocent people.
    - Enables wide spread DDoS attacks on innocent third parties.
    - Doesn’t actually stop any spam.

Spam Folders

- What’s the point?
  - Users will not check the spam folders.
  - Spam has already used the resources.
  - As with dropping, the sender doesn’t know the message has gone unread.
    - » Return receipts will be sent on delivery.

SORBS

- SORBS is a blocklist.
  - Many different data sets.
  - A crude, but effective tool.
  - Very efficient.
  - The wider the use, the more effective.
  - Owned by GFI, but run by volunteers, and me.

The Current Security Problem.

- Firewalls.
- Hacked Machines.
- Trojans and Viruses
- End Users and Scams
- So how can this affect you?

Firewalls

- So does a firewall make you secure?
- No, of course not.
- Will a firewall stop a hacker?
- No, but it will stop automated scripts.
- Firewalls are only needed to prevent stupidity
    - Without stupid people we wouldn’t need them.
    - Without nasty people we wouldn’t need them either….

An example (home user).

- Senior Unix Admin working for a *.gov.au
  - Can’t make Zone Alarm work with program.
  - Installs VNC for help.
  - Opens VNC port in firewall.
  - Doesn’t set password.
- 18 hours later, “hacker attack”
  - RootkitRevealer reveals nothing.
  - Machine under full remote control.

An Example (Professional)

- Professor, external project.
  - Has 2 servers, RedHat, and Windows 2003
  - Machines are “Servers” for custom app.
- ITSec alerted to scanning at 03:30 5th Feb ‘07
  - 10:00 “Networks” blocked external access.
  - 15:30 6th Feb ‘07 machine and owner located.
  - Operator and Professor wondering why Windows 2003 was ‘having problems’
  - 15:35 6th Feb, machine removed from internal network.
  - 13:00 8th Feb ITSec asked to examine machine.
  - RootkitRevealer indicated unidentified RootKit.
  - 9th Feb machine re-installed.

So what’s the Problem?

- Unix Admin, opens a port in firewall, doesn’t secure service.
- Professor hasn’t patched Win 2003 server, common IIS exploit used to ‘Root’ server.
- Both ask ITSec why firewall didn’t stop the “hacker”…?

How does this affect you?

- So what are the risks here…?
  - A server hacked on the corporate network?
  - A home user, with their computer hacked?
  - A mobile user with a laptop?
- Another example, the Chinese Laptop..
  - Staff member takes laptop to China
  - Laptop gets infected with ‘Drive/Share’ virus.
  - Staff member hands USB drive around.
  - 5+ machines get infected…

Security and Spam

- So what has this got to do with spam?
    - In 2007 99% of infections are AGOBOT or SDBOT variants.
        - » SDBOT enables both spamming and DDoS
        - » AGOBOT enables both spamming and DDoS
    - In 2009 more than 80% of infections are Rustock spambots
        - » Rustock enables spamming a DDoS
- Why are DDoS's a problem?
    - They attack anti-spam systems.
    - They attack corporate systems.
    - They attack anything they feel like at the time…

Security Conclusions

- Attacks are everyone’s problem.
  - They attack the foundation of the Internet.
  - No-one is safe.
  - Liability issues.
- 99% of all trojans enable delivery of spam.
  - Whilst the trojans are capable of DDoS their primary purpose is delivery of spam, including self replication.
  - Most of the trojans will attack your network from the inside out.
- Desktops are not the only target, watch out for those pesky PDAs.

SORBS, and SORBS v2.0

- SORBS
  - The admin Interface
    - » Antiquated, and limited.
  - Feeds to the ACMA.
  - Feeds to the Australian Federal Police.
- SORBS v2.0
  - Highly configurable.
  - Designed to offload administration to the end users.
  - More fine grained reporting. (Inc ‘Instant Reports’/FBLs)
  - Ability to see the ‘Top 10’.
  - Ability to track botnets.
  - URI Tracking and publication.

SORBS v2.0

- On to the demonstration….

Thank You

Michelle Sullivan