Vi@9ra, M0r+gages, and RoL3x w@tch3s

Spam on Rensselaer’s Central Email Servers

Michael Sofka & Gary Schwartz
Communications & Collaborative Technologies
Rensselaer Polytechnic Institute
sofkam@rpi.edu
Gary Schwartz, Director C&CT
Michael Sofka, C&CT, Sr. Systems Programmer
Brenden Conte, C&CT, Systems Programmer
Frank Hill, C&CT, Sr. System Administrator
Gail Kaiser, C&CT, Academic Computing Analyst
What is Spam?

Spam is email that is:

- Unsolicited,
- Sent to thousands/millions of recipients,
- Selling or promoting a shady enterprise
  - Viagra, Body Enhancement, Pornography, Mortgages
  - Pyramid Marketing, Ponzi, Nigerian 419
  - Commercial, Unwanted Email
  - Phishing for information

Pre-history of Spam:
- Jon Postel, RFC 706 “On the Junk Mail Problem,” 1975
- Chain letters
- Good Times virus hoax
- Cantor & Siegal, Usenet “Green Card” Lottery, April, 1994
- Usenet Spam:
- Jeff Slaton, Spam King; Sanford Wallace, Cyber Promotions.
Spam is a widespread problem

More than 80% of email is spam

Approximately 50% of RPI email is spam

**Up to 90% of external email sent to RPI**
- Up from 50% in 2003, 30% in 2002

Spam is profitable (Leung, 2003)
- Spam has a 0.005% response rate (50/1,000,000)
- Cost to spammer low because spammers steal services

Easy for spammers to hide:
- Forge sender address
- Use “Open” mail relays
- **Compromised home machines**

Harder for average user to hide (stay out of spammer databases)
- Web-page harvesters (illegal under CAN-SPAM)
- Open database harvesting
- Web bugs
Financial Cost

- $9 billion, US; $2.5 billion, EU (Ferris Research, 2003)
- Productivity: email management and distraction
- Connectivity: slower servers and networks
- Storage: It costs money to store email
- Support: Anti-spam products, training
- Complaints: To help desk, ISP blacklists

Nortel estimates average $1.00 per spam message

AOL $5.00 per user per month
Social Cost (Fallows, 2003)
Email has become an unfriendly place
Personal spam load varies from zero to 100s/day
People less trusting of email, e-business
Women bothered more than men, older more than younger
Spam is increasingly used to further a crime

Nigerian 419 scams

Pyramid marketing (often for spam services)

Ponzi schemes

Stock Market pump-n-dump

Phishing for financial information

Identity theft
Spammers often engage in crime to distribute spam
Viruses installing back door (Sobig-F)
Hackers going “pro” and selling services
Conditions of Use/License violation
Violations of CAN-SPAM act since January 1, 2004
- Address “harvesting” (Spam Honey Pot Project)
- Misleading subjects
- False/Forged reply information
Theft of service by using open relays
Compromised Home “Spam-Bot” Machines
Technical Responses

Delete key (best for low base-rate spam)

Rensselaer Enterprise SPam Interdiction TEchnology (RESPITE, http://respite.rpi.edu/)

Based on CanIt, by Roaring Penguin Inc.

IP exchange with vendor (documentation, interface, algorithm improvements)

Suited to the University environment
- Opt-in service
- User control and configuration
- Server-based: Works with any email client
- Keeps email out of end users mailbox
- Central management, optimization
- 2,200 users (1/4 of active email users)
- Traps, Blocks or Tags over 250,000 messages per week.

CanIt in use at many Universities

Universities starting to take opt-out approach (Cornell)
Technical Limitations

All spam traps are heuristic:
- Patterns, keywords (difficult: $6 \times 10^{20}$ Ways to spell Viagra)
- Statistical (Bayesian) filters
- Real-Time blacklists

Can never eliminate false-positives (<1%)

Can never trap all Spam:
- Active adversary
- Motivated by profit
- Willing to commit crime
- Often very smart
- Smart spammers sell technology

Tests not specific enough for low base-rate spam
- for a few spam a day the delete key is the best technology

That said, anti-spam has become very effective over the past two years
Legal Responses

Federal Trade Commission (most spam already illegal)
State Anti-spam Laws
CAN-SPAM: Controlling Abusive Non-Solicited Pornography and Marketing act
ECPA: Electronic Communications Privacy Act
CFAA: Computer Fraud and Abuse Act
Lawsuits against spammers are usually successful—but recover no money after legal costs
6 \times 10^{20} \textbf{Ways to spell Viagra:}


\textbf{Spamhaus:} http://www.spamhaus.org/

\textbf{SpamCop:} http://www.spamcop.com/

\textbf{MIT Spam Conferences:}

http://www.spamconference.org/


\textbf{Spam: How it is hurting email and degrading life on the internet, Fallows, 2003:}


\textbf{ARC Helpdesk:} http://j2ee.rpi.edu/helpdesk