Spam: Why It's Not Just Junk Mail

Inveniamviamautfaciam

“Where did it all start?”

- Monty Python + MUD = SPAM
- Not a new problem. 1975, RFC 706: “Junk Mail problem” written
- Early spam (1980’s) was generally chain letters
- First virus/spammer was in December 1987 on BITNET and VNET
- 1994 – Canter and Siegel with “Green Card Lottery”. Later wrote *“How to make a fortune on the Information Superhighway”*
- 1995 – Jeff Slaton. Self-proclaimed Spam King
- 1996 – Sanford Wallace and Cyber Promotions Inc.
- By 1997/98 spam was no longer for individuals

Invenia mvia mauta facia m

“What is the fuss about?”

- Time, not only time users waste but also for administrators fixing it
- Confidence, it erodes the confidence users have in the Internet
- Reputation, when spam spoofs as you .. people get mad at you
- Payload, spam is more recently becoming used to spread malware
- Finance, cost in resources and actual monetary loss
- Performance, the strain on network resources and internet as a whole
- Just plain nasty!

Inveniamviamautfaciam

“Why does Spam work?”

- The cost per send is almost nothing as opposed to other communications
- Speed at which spam can be sent
- Many businesses see proper system administration as a burden not a need
- The email protocols were made in more trusting times
- Spammers make lots of money
  - Click-Thru
  - Clients
  - Sales of goods
  - Sales of databases
  - Plain old theft
- People are greedy

Inveniamviamautfaciam

“The old way to stop spam”

- Hit the delete button, and send it to the recycle bin
- Whitelists for approved senders, for the trusted people
- Blacklist for the spammers, for the provably untrustworthy people
- Blacklisting keywords, stopping all those bad words
- Complain to the ISP and try to shutdown the spammer
- Mass actions against spamers and spammer-friendly networks

Inveniamviamautfaciam

“The new way to stop spam”

- Community IP blacklists, community listings of spammer IP’s
- Community Domain blacklists, community listings of spammer domains
- Greylisting, checking protocol compliance
- Bayesian filters, natural language learning filter
- Hash Signatures, to compare spam
- RFC compliance, to check for proper email protocol usage
- “Good neighbour” checking, to stop open relays
- Keyword weightings, to better implement keyword blacklists
- Null zone domains, dead-ending known bad domains
- Legislation against spam makes getting caught more of a hassle

Inveniamviamautfaciam

“The future of defense?”

- Challenge/Response systems to ensure a human sender
- PKI setups to ensure trusted networks and users and non-repudiation
- Overhaul the protocols used for better security – ie; IPv6
- Implement encrypted email protocols for better controlled usage and security
- Impose financial penalties, like each email costing one cent
- Using the proposed trusted sender-ID system
- Impose computational penalties for email senders
- Unfortunately many of these ideas are unfeasible for use

Inveniamviamautfaciam

“The future of spam”

- Covert channels for use in secret communications and data exchange
- Spyware and Malware payloads
- Phishing and Pharming to increase a spammers payday
- Drive-By spamming for wireless networks
- SPIT, or spam in VOIP networks
- Actual message manipulation to defeat filters
- Usage of zombie-nets to defeat community efforts
- Spamming methods constantly evolving in a type of arms race
- More and more spam is becoming driven by monetary/criminal gain

Inveniamviamautfaciam

Thank you for your attention

Inveniamviamautfaciam