Spam: How can we handle it?

Renata Cicilini Teixeira - renata@cais.rnp.br

CAIS/RNP: Brazilian Research Network CSIRT

FIRST Technical Colloquium

October, 2002
Spam: How can we handle it?

Contents

Introduction

Motivation

Statistics

How CSIRTs should handle Spam and other related issues?

An Overview of technical solutions

How does CAIS deal with SPAM?

Conclusions

References
Introduction

- **Spam** is any email message sent to several recipients without their permission or explicitly request.

- **UBE**: *Unsolicited Bulk Email*. It’s a formal word that means the same as “spam”.

- **UCE**: *Unsolicited Commercial Email*. It’s spam which contents are advertisement.

Why spam is so important nowadays?

- Spam messages are increasing so fast, polluting mailboxes worldwide;

- It’s taking valuable work time of users and administrators;

- It’s wasting bandwidth, email servers CPU time and so on.
Motivation

• 1999: CAIS shouldn’t handle Spam.

• Spam occurrences have been growing for the last two years;

• Nowadays, almost 30% of all security incidents handled monthly by CAIS are Spam related issues:

  • open relays;
  
  • anonymous proxies;
  
  • system and network administrators who don’t know how to deal with spam;
  
  • convinced spammers sending threats, advertisement or some other junk e-mail;
  
  • people who don’t know what spam is and think that Internet is a “powerful marketing media” ...
Spam: How can we handle it?

Statistics

- Security incidents handled by CAIS last months, and Spam incidents on the same period.
Spam: How can we handle it?

**Statistics**

- Amount of Spam reported by RNP staff during last months.
Spam: How can we handle it?

Statistics

- Results of a quick Spam poll, answered by RNP Staff on May, 2002:

  *How many Spam messages do you receive every day?*
How CSIRTs should handle Spam and related issues?

- Recommending best practices in order to correctly and securely configure mail servers, mail clients and proxies; email security policies and so on.

- Assisting and training network administrators on operational, technical and political procedures about spam:
  - Anti-relay configuration: mail servers and proxies
  - Header analysis basics
  - abuse@ and security@ implementation
  - How to report a spam and how to answer a spam incident report
  - How to train your users and administrators
  - Define and implement email policies
An Overview of technical solutions

- RBLs, Real-time Blackhole Lists: MAPS, ORDB,…

- Define *Private Blackhole lists* with local spammer domains, networks, IPs or emails.

- Questions: Filter or not filter? How to filter? Where?

- It’s recommended to use some filter solution:
  - RNP objective: public domain or freeware software.
  - Some options: Spamassassin, Bayespam, Bogofilter, Milter, Procmail, etc
Spam: How can we handle it?

An Overview of technical solutions

- Important issues to be considered to choose a filter solution:
  - CPU utilization;
  - How many mail users do you have;
  - How does filter software fit to your MTA software;
  - Filter customization;
  - Network and mail service performance impact;
  - Filter performance: amount of Spam filtered;
  - Amount of false positives generated.
How does CAIS deal with Spam?

- Operational procedure: forwarding all spam complaints to the related network administrators.
- Assist network administrators on handling spam complaints.
- Technical recommendations:
  - RBLs + Private RBL + Filter (Qmail + ...) or (Sendmail + ...)
- Email policy
- User education
- Network administrator awareness
How does CAIS deal with Spam?

- Best practices:
  - Correct and secure configuration of mail servers and proxies
  - Secure email usage (Internet downloads, attached files)
  - Users shouldn’t answer a spam message
  - Configure an automatic reply for filtered messages.
  - Define a spam handling procedure and inform all users about it.
Spam: How can we handle this?

Conclusions

• Filters usage is a controversy issue, however they are becoming necessary.

• It’s important to define and disseminate procedures in order to handle spam.

• Train users and network administrators about email security policies and other best practices.

• There isn’t a standard solution for all spam problems. There isn’t a miracle that eliminate all spam on your network. The only way is to find technical and comportamental procedures which could minimizes spam impacts.

• CSIRTs should be aware of spam problems, they should assist network administrators of its constituency, train them on best practices, secure configurations and security policies.
Spam: How can we handle it?

References

- Spamcop: http://spamcop.net
- SpamCon Foundation: http://www.spamcon.org
- Open Relay Database, ORDB: http://www.ordb.org
- Mail Abuse Prevention System, MAPS: http://www.mail-abuse.org
- Distributed Server Boycott List: http://dsbl.org/
- CAUBE: http://www.caube.org.au
- RedIris: www.rediris.es/mail/abuso
- SpamAssassin: www.spamassassin.org/
Spam: How can we handle it?

References

- Bayespam: http://www.garyarnold.com/projects.php#bayespam
- Bogofilter: http://www.tuxedo.org/~esr/bogofilter/