Implementation of Anti-Spam Techniques in ASNET-AM Network

Arthur Petrosyan

Institute for Informatics and Automation Problems, NAS RA
Yerevan, Armenia
e-mail: arthur@sci.am

ABSTRACT

Article describes the experience of Academic Scientific Research Network of Armenia (ASNET-AM) in blocking unsolicited E-mail messages (called "Spam"). Spam blocking solutions implemented last years in ASNET-AM are being described.

Keywords

Spam, E-mail, Anti-spam, RBL, Mailserver, Greylisting, SPF, ASNET-AM.

1. INTRODUCTION

E-mail Spam is the electronic version of junk mail. It involves sending unwanted messages, often unsolicited advertising, to a large number of recipients. Spam is currently a serious security concern as it can be used to deliver Trojan horses, viruses, worms, spyware, and targeted phishing attacks. As Spam is a problem that is continuing to grow from day to day, there is a need to find out effective spam blocking solutions to protect our networks from it, while at the same not blocking legitimate E-mail messages.

2. SPAM HISTORY

Spam is a form of abuse of the Simple Mail Transfer Protocol (SMTP), which is implemented in email systems on the basis of RFC 524. First proposed in 1973, RFC 524 was developed during a time when computer security was not a significant concern. As such, RFC 524 is not a very secure command set, making it and SMTP susceptible to abuse.

Most spam-making tools exploit the security holes in SMTP. They do this by forging email headers, disguising sender addresses, and hiding the sending system, such that it becomes difficult or even impossible to identify the true sender. That is why you may receive a message where you will not find your address in 'To:' header.

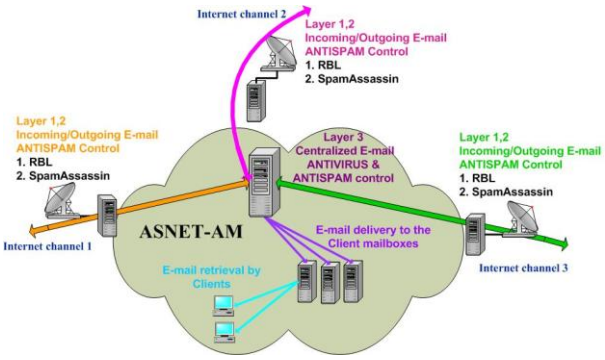
Today there are a large number of solutions designed to help eliminate the spam problem. These solutions use different techniques for analyzing email and determining if it is indeed spam. Because spam is constantly changing, the most effective spam blocking solutions contain more than one of these techniques to help ensure that all spam, and only spam, is blocked.

The following article presents an overview of techniques we effectively use in the Academic Scientific Research Network of Armenia (ASNET-AM) for spam blocking.

3. SPAM BLOCKING SOLUTIONS

First of all it should be noted that several defense layers are to be used to protect your email server from spam attacks. There are a large number of techniques for filtering/blocking spam on different defense layers.

Current ASNET-AM Mail Service is implemented as a complex distributed system. ASNET-AM uses a number of Internet channels (currently 3) for redundancy and reliability. The Mail Service at ASNET-AM and DNS records of appropriate domains are configured to ensure that incoming E-mails have several ways to come into the ASNET-AM network.



Each next mailserver at ASNET-AM have one or more of below spam defense layers implemented:

- Rejecting incoming mails at the border mailserver
  - RBLs
  - Greylisting
- Filtering incoming mails at the border mailserver
  - SpamAssassin
- Filtering incoming mails at the intermediate antivirus/antispam mailserver
- Filtering incoming mails at the local mailserver
  - Procmail
- Filtering incoming mails at the MUAs (Outlook, Thunderbird, Webmail, etc.)

Previously, we have used a Reverse PTR (Pointer Record) DNS record check technique to drop all incoming connections to our mailservers from the sources that have no reverse PTR or have a reverse PTR, not looking like the server name. It was assumed that any valid maliserver should have a properly configured reverse PTR record. In fact this method seems to be fail de-facto, because we have found a lot of domain administrators, who don't care about PTRs at all, and as a result our clients have no opportunity to receive E-mail messages from such domains. We have tried to make exceptions for such domains, but they were too many. Thus, it was decided not to use Reverse PTR record check technique at all although our measurements showed it was quite effective. Unfortunately, we are trying to reach the same result in anti-spam protections with other methods decribed below.

We use Realtime Blackhole Lists (RBLs) also known as DNSRBLs. An RBL is a list of hosts that are known as spammers or open relays (misconfigured mail servers). Using RBLs means to check the source IP address of every incoming E-mail message at the initial stage of SMTP connection against a list of IP addresses in the RBL. If the IP address is listed in the RBL, then the email is identified as spam and blocked. It should be noted that we use only a free RBLs at ASNET-AM.

It should be noted that some RBL's are very aggressive, others are ineffective, so we have made thorough monitoring and currently have left only the following 4 RBLs, that proved to be effective at ASNET-AM:

- spamcop.net
- spamhaus.org (sbl, xbl)
- abuseat.org (cbl)
- sorbs.net (dul)

When ASNET-AM border mailserver gets connection from IP address listed in one of the above RBL, it rejects to talk with such peer and bounces the message back with detailed explanation about why the connection was refused, in which particular RBL the IP address was found and a link with directions on how to get unlisted from it is added.

Recently Greylisting and Sender Policy Framework (SPF) methods were implemented at ASNET-AM.

CONCLUSION

Spam is a continuing problem. Fortunately though, there are different anti-spam techniques to help counter the various types of spam. Current ASNET-AM experience is that by using the above mentioned techniques 95% of Spam can be blocked. Of course all that solutions require continuous enrichment and improving to get better results.

Because spammers are always trying to bypass anti-spam techniques by changing the methods they use to send spam, it's best for organizations to protect themselves with a spam blocking solution that uses more than one spam blocking technique. Each one of these techniques has advantages, disadvantages, as well as limitations.

To minimize the amount of spam that enters an organization, a spam blocking solution that includes a combination of the most effective techniques should be implemented as it is done at ASNET-AM network.

REFERENCES

1. Anti-spam techniques, Wikipedia®
http://en.wikipedia.org/wiki/Anti-spam_techniques

2. A. Petrosyan , R. Tadevosyan, H. Khudoyan,
"Blocking Spam - ASNET-AM Experience", Proceedings of the Conference CSIT'2007, Yerevan 2007

3. Jaeyeon Jung, Emil Sit, An empirical study of spam traffic and the use of DNS black lists , Proceedings of the 4th ACM SIGCOMM conference on Internet measurement.
http://www.scotnpatti.com/UNL/Csce810/p370-jung.pdf

4. Common DNS Operational and Configuration Errors
http://tools.ietf.org/html/rfc1912

5. Composite blocking list
http://cbl.abuseat.org/

6. Spam and Open Relay Blocking System (SORBS)
http://www.sorbs.net/

7. Spamcop Project
http://www.spamcop.net/

8. Spamhaus Project
http://www.spamhaus.org/

9. Greylisting, Wikipedia®
http://en.wikipedia.org/wiki/Greylisting

10. Sender_Policy_Framework, Wikipedia®
http://en.wikipedia.org/wiki/Sender_Policy_Framework

11. Academic Scientific Research Network of Armenia (ASNET-AM)
http://www.asnet.am