CMSGu2012-07

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Spam Control

CERT-MU

National Computer Board
Mauritius

Version 1.0

September 2012

Issue No. 7

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

The purpose of this guideline is to help users manage their email accounts and systems with a view to counteracting spam e-mails.

1.2 Audience

The target audience for this document includes IT managers/officers, security managers/officers and home users.

1.3 Document Structure

This document is organised into the following sections:

Section 1 contains the document's content, the targeted audience and the document's structure.

Section 2 gives a background on spamming and types of spam.

Section 3 talks about the spam controls

Sec*tion 4* concludes the document.

Section 5 contains a list of references that have been used in this document.

2.0 Background

Spamming is the abuse of electronic messaging systems to send unsolicited, bulk messages. While the most widely known form of spam is e-mail spam, the term is applied to similar abuses in other media, for example, instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs and mobile phone messaging spam.

The nonstop attack of junk messages strains networks, erodes user productivity, propagates dangerous malware and costs business millions of dollars. The following section gives us a glimpse of the different types of spam in existence today.

2.1 Types of Spam

Though all junk email might look the same, spam continues to arrive in a seemingly endless number of configurations, ranging from the innocuous to the lethal. The major spam types include:

- **Advertising**: Spam is used to promote an entire spectrum of products and services, from software to real estate to questionable medical and nutritional offerings.
- **Malware Delivery**: Spam is one of the main distribution channels for delivering viruses and other types of malware. Targeted individuals, believing they have received an important document or media file, are often tricked into opening a malware attachment.
- **Scams**: Posing as Nigerian princes, Swiss bankers, tragically ill children and other stock types, scammers prey on recipients' sympathy and greed.
- **Phishing**: Hiding behind the names of respected retailers, financial institutions, businesses, charities and government bodies, phishers attempt to lure unsuspecting recipients to bogus Web sites where they steal personal financial or identity information.
- **Nonsense**: A significant chunk of junk-mail text is pure gibberish. Some of this material is generated in an effort to trick spam-filtering technologies into passing an attached message onto recipients. Many nonsensical messages seem to exist for no purpose at all.

2.2 Spam Media

Spam is overwhelmingly an email problem. Yet as Internet technology advances, junk content is rapidly spilling over to many other types of IP media, including:

- **IM (instant messaging)**: Spam is a growing problem on IM networks, where the threats closely parallel those of email spam.
- **VoIP**: **SPIT** (Spam over Internet Telephony) is a rare but potentially dangerous form of spam that threatens to annoy users and jam voice-mail inboxes.
- **Search Engines**: Using techniques such as hidden text, doorway pages and mirror sites, a search-engine spammer attempts to boost a Web site's ranking by redirecting traffic to the site. This practice is also known as "spamdexing."
- **Web Message Boards**: Spammers like to use Web message boards and Usenet.com groups to promote products and services that are usually unrelated to the site's content focus.
- **Blogs**: Junk advertising is inserted into a blog's reader-comment area.
- **Online Video**: YouTube LLC and other video-sharing sites are plagued by video spam, which consists of thinly disguised commercials for products and services of dubious value.

3.0 Spam Control

This section seeks to identify the most common tools that can help eradicate spam.

3.1 Gateway Filters

Gateway filters are significantly gaining in popularity. These solutions will run on a system separate from the mail server itself in order to offload performance and even bandwidth consumption issues with running them on the mail server directly. They often come as solutions for in-house consumption and management or as an outsourced service that can be purchased from a third party.

3.1.1 In-house solution

As an in-house solution, these systems tend to have many options, but will often require trade-offs to be made about specific features (such as direct filter control by end users) in order to purchase a single solution that will be used for the entire environment. These solutions will typically be coupled with antivirus to provide a complete mail filtering application.

3.1.2 Outsourced service

As an outsourced service, these solutions offer the medium to large enterprise the opportunity to buy just as much filtering as they need and to even offload a significant amount of bandwidth consumption from being consumed by the companies that own Internet connections. Since mail will first go to a third party provider, their bandwidth is consumed for sending the unfiltered mail and only the filtered mail will theoretically consume bandwidth. Unfortunately, this also means trusting a third party to have resiliency within their network infrastructure.

3.2 Mail Server Engines

Mail server engines represent some of the initial methods that centralized anti-spam solutions that were deployed. These products run on a mail server directly and process spam locally. These applications are typically coupled with antivirus solutions. However, their usage has been declining in favour of gateway filters that process mail before reaching a mail server. While they have the benefit of being centrally managed to process mail for an entire domain at once, they tend to contain fewer features than the gateway filter counterparts and often

have a noticeable impact on the overall performance and response capability of the mail infrastructure especially in larger environments.

3.3 Client Side Applications

Client side applications will install on a user's workstation directly and these applications usually involve a cost per installation. However, careful consideration should be taken before deploying such applications. In a corporate environment, these applications rarely make sense to be deployed as a corporate initiative because they are decentralised by nature and thus would require much more administration than their mail server or gateway solution counterparts. In addition, since filtering occurs as email is received, end users will directly experience the common issue of a slight performance drain as the system processes mail for spam. While this delay occurs in the mail server engines and gateway filters, the end user is shielded from the concern since they will rarely have any observance of this delay occurring. Another downside of such applications is that they often require a little bit of end user knowledge and awareness to be able to use them fully.

On the other side, client side applications have the capability to be much more in tune with what a specific end user needs. While an anti-spam application might filter any and all user groups, another may be more effective at permitting authorized distribution groups and filtering appropriately based upon the content rather than the pattern upon which the message was received. These types of applications tend to be much better at heuristics and Bayesian filtering capabilities since it only needs to focus on the pattern and established heuristics and Bayesian patterns of a single user rather than many. Further, their low cost for a single license make them very affordable and ideal for a home user or for an office with just a small number of users for which a much more costly mail server engine or gateway filter may not make sense.

3.4 Hashing/Checksums

During e-mail filtering, the hashing/checksums checks normally go through a mathematical computation against an e-mail or portion of e-mail to look for and filter based upon the amount of matching emails sent. This method of anti-spam identifies bulk mail messages which may be sent or match known spam content. Rather than store the entire content in question, hashing/checksums engines will simply perform a mathematical computation against that content to show it in a smaller form for matching purposes. An e-mail which

corresponds with the resulting hash will, by definition, be a bulk e-mail which is a fairly good sign that a message is a SPAM and should probably be blocked.

3.5 Open Relay Checks

The open relay checks will verify if the source mail server allows relays. Some mail servers may either do this directly, or they may also rely upon generally available online databases, such as ORDB – Open Relay Database: **http://www.ordb.org/** . Mail servers that relay are normally considered to be misconfigured and are a very big target for spammers who will use them as a way to reduce problems from being blacklisted and thus unable to continue sending spam. By blocking servers that allow relaying, this issue can be circumvented.

3.4 Real-time Blackhole List (RBL) Checks

Real-time blackhole lists, such as SPEWS or SpamCop are a list of DNS names or IP addresses from which spam has been found. These lists are usually made available for free or it may also be available for a small fee and subscribers may block any or all e-mails which are coming from a mail server listed in an RBL list. However, these lists are often vulnerable to false positives and it should be used very carefully within a corporate environment.

3.5 Bayesian Filtering

Bayesian Filtering carries out a statistical calculation of probability that a given message is a spam based upon user input. This method works depending upon feedback from users to train the filter about false positives and false negatives so that it can dynamically adjust its filtering capabilities. This type of technique normally works best when deployed in a client side application filter, but does have some use in more centralized filters as well.

3.6 Heuristics

Heuristics is another form of statistical calculation that will put together a number of detection techniques to identify patterns that when taken together may show the probability of spam. This is normally carried out by assigning certain point values to specific matches such as signature matching or an existing in an RBL and then setting a point threshold that, if crossed, will show that the message is a SPAM and should be treated as such.

3.7 Signature Matching

One of the first methods that was used to filter spam is signature matching. This technique normally deploys a simple filter that looks for specific keywords within a message. However, this is often vulnerable to false positives and receives a lot of criticism. For example a filter will block a message as spam if it contains the word “Nudity”. Now, if this filter is deployed in a law enforcement agency, which regularly receives and sends e-mail regarding nudity issues in the society, this can be a bit of a problem.

3.8 Blacklisting

Blacklisting is a type of localized RBL. A blacklist is the practice of identifying a specific source address, domain or IP from which all e-mails should be blocked. The main difference between blacklisting and an RBL is that the blacklist is maintained by the organisation whose e-mail is filtered by the system that uses it.

3.9 Whitelisting

Contrary to blacklisting, whitelisting is the practice of identifying a specific source address, domain or IP from which all mail should be allowed. Similar to blacklist, whitelists are typically maintained by the organisation is filtered by the system that uses it. They are often deployed when continuous false positives occur and other configuration changes will not easily ensure that the legitimate e-mail can bypass the filter.

3.10 Antivirus solutions

Spam that carries some type of malware are some of the most dangerous types of spam that exist nowadays. In various cases, antispam techniques will work to identify and block e-mails that contain malware well before antivirus vendors have identified and deployed filters for the new and emerging threats. However, after the initial “hit”, that is, when the spam e-mails are seen, they will tend to fall out of the standard filters used to detect sudden bulk e-mails, at which point in time antivirus application plays an important role in preventing further spread of viruses and other malware.

Besides, user education and awareness is very important in defending against viruses and other malware that arrive through e-mail. Some of the basics that users need to know are:

- Do not open e-mail that appear to be suspicious
- Do not click on links in unsolicited e-mails

- Do not respond to unsolicited e-mails

3.11 Antispyware solutions

Spyware are also linked with spam in one way or the other. For example, user education and training that would normally help prevent someone from deploying spyware, works hand in hand with the same training that can help prevent a person from doing things that could lead to receiving an increased amount of spam. Also, spyware have been known to be linked directly to providing e-mail addresses that can subsequently be used by spammers.

As such, good antispyware implementation can help reduce exposure to spam and other security issues. The good news is that there are many commercial and free tools available, such as Ad-Aware, Spybot Search & Destroy and Spyware Doctor that can help detect and destroy spyware.

4.12 Avoiding the "unsubscribe" trap

Very often, unknowingly, we are tempted to click the "unsubscribe" link on a spam e-mail. Spammers work to idenfity "validated" e-mail accounts and use these to sell or trade with each other. By clicking on an "unsubscribe" link, you may be actually falling into a trap set by the spam to validate that a real human is reading the message. This act makes your e-mail address more valuable and this can result in an increased amount of spam in your mailbox, rather than removing you from the spammers list.

3.13 Spamsinks

Spamsinks are email accounts setup, typically on free email services such as yahoo, hotmail and gmail, with the specific purpose of being able to provide a throw away e-mail address when forced to submit an e-mail address in some way. In some cases, these accounts may be an alias for the real account or you may set them up independently and check them on a periodic basis as need be. The more paranoid users may choose to create a new account each time they are required to provide an e-mail address to a questionable source so that they can know who may have shared their e-mail account to spammers and hence take appropriate action.

3.14 Avoiding typing e-mails in public places

A very common technique that spammers use is to set up scripts that automatically parse company websites and public e-mail group archives to harvest e-mail addresses. If we are more vigilant when displaying e-mail address in these public ways, a lot of spam can be avoided. A few techniques that can be used to do this could be to post an e-mail address in such a way that a human would be able to understand what the e-mail address is, but a computer program doing basic parsing will likely miss it. An example could be: "sample @ domain . com" or "sample [at] domain [dot] com".

A different method in html is to encode the "@" and the "." symbols in ASCII such as "Sample@domain.com"

An even more effective way, especially on company website, is to never publicly display e-mail addresses, but instead provide forms that can be filled out and will result in the backend web code to send e-mail to the designated mailbox.

One more method that can be used is to display e-mail addresses as an image rather than as actual text. A last technique that you could use is to have a separate account from your primary account for use in public discussion forums or for public display. When such accounts are bombarded with spam, a new account can be created and the original one thrown way, much like a spamsink account.

3.15 Cookie Management

Cookies are files that are stored by a web browser to contain specific user information for later retrieval by a website that is being accessed. The information in these cookies may often provide specific information, such as credit card numbers or e-mail addresses that can potentially be harvested by specially crafted websites. By disabling cookies or at least carefully managing the storage and retrieval of these cookies by specific websites, these harvesting techniques can potentially be defeated.

3.16 Protection of one's own network

The implementation of proper security controls in your own company networks and home networks, you can reduce the number of systems and networks that spammers can use to carry out their activities. A very important part of defending one's own network and systems

against becoming a launching point for spam, is to look carefully into blocking all outbound SMTP (25/TCP) traffic from all systems with specific exceptions allowed for known and authorized mail servers only. This act can also reduce the probability that an internal infection by a virus that spreads through its own STMP engine will be further propagated by you or your organization.

3.17 Proper configuration of mail servers

Careful attention should equally be given to the mail server. More specifically, due care should be taken to ensure that relaying is not permitted from the Internet. There may be legitimate reasons to permit relaying from specific internal hosts, but these should be done with due diligence and care. In addition, when sending e-mail on behalf of a user, some form of authentication should be required to prevent your mail server from sending potential spam messages that could be from an unauthorized external user who spoofs the source e-mail address to look like internal e-mail account. By requiring authentication for sending all outbound e-mails, this threat can greatly be reduced.

3.18 Sender Policy Framework (SPF)

The SPF record is defined by RFC 4408. This is a way to use DNS such that someone having control over a site's DNS records can set a specific record that will identify which servers or IP addresses are authorized to send e-mail on behalf of that domain. Once fully implemented, servers can then choose not to accept e-mail claiming to come from an e-mail address where the source address of the e-mail connection is not coming from an IP address listed in the SPF record. This method can help to significantly minimize the amount of spoofing relating to spam messages.

3.19 Avoiding chain mail and hoax mail propagation

Chain e-mails and hoaxes represent a noticeable share of spam. By educating employees so that they do not fall victim to the message that such e-mails contain, the problem can be alleviated. Any suspicious e-mail should be treated with caution. By focusing on developing some skepticism when responding to or forwarding on e-mails that have a lack of plausibility and reality, users can learn to become more aware and avoid traps of even more serious social engineering threats that contain malicious viruses that present a more serious concern.

3.20 Turning off HTML rendering in email clients

Turning off html in e-mail clients can help significantly in reducing the amount of information leakage and in reducing the amount of benefits that spammers receive from sending their message. By not viewing e-mails in html, phishing scams are much easier to spot when link targets do not match the apparent text for the link intended to be clicked. Furthermore, the technique of sending single pixel images within embedded html associated with specific e-mail addressed can be defeated as these images will never be accessed and account validation will not happen. Also, if spammers depend upon certain banner ads to be viewed in order to generate revenue, they will not be able to collect anything if your e-mail client does not display the banner as a result of rendering the html within a received e-mail. In addition to these benefits, exploits that depend upon html rendering, especially by Internet Explorer, can be avoided entirely from coming in as a result of receiving a specially crafted e-mail.

However, it is improbable that many organizations will choose to enforce this method due to the abundance of legitimate e-mail that use html. The ease and convenience of this feature will oven win over the technical and security that it provides.

3.21 Reading and responding to e-mail headers

You can learn to read e-mail headers, you can better protect yourself to correctly interpret and respond to spam messages. This information contained within the headers provide solid evidence about the true source of spam e-mails and are essential when responding to or reporting spam messages within an abuse reporting environment.

4.0 Conclusion

The spam battlefield is in a constant state of flux. As better weapons are built on the defense side, spammers are constantly finding newer techniques to overcome these measures on the offensive side. By becoming and staying informed, about the offensive and defensive weapons of both spammers and anti-spammers, we can prepare ourselves and our organizations to take direct measures to reduce the proliferation of spam.

5.0 References

- Focus, **http://www.focus.com**
- Spamlinks, **http://spamlinks.net**
- Spam and Anti-spam, SANS