SPAM, the Annoying Culprit on the Net

BY | Sahrom Md Abu, Sharifah Roziah Mohd Kassim

Introduction

Spam has become a global issue faced by almost all Internet users. Though it is not as serious as malicious code, phishing, but is still considerably serious as spam has become a medium to transmit phishing sites, malwares, illicit contents and viruses.

Spam in general is defined as the use of electronic messaging systems to send unsolicited bulk messages to other Internet users. The most common type of spam is email spam. The other types of spam are instant messaging spam, spam in blogs and social networking spam. Spam is considered as an abuse of the Internet infrastructure to annoy, flood other users' mailboxes and consume unnecessary bandwidth.

Email spam has steadily grown since the early 1990s. Botnets, networks of virus-infected computers, are used to send about 80 percent of spam. Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, searching the web for addresses, from business cards, from conferences, seminars and exhibitions.

Techniques Used in Spamming

Generally, spammers use or jump to various techniques to bypass spam filters. The more sophisticated spam filters are the more sophisticated the spam techniques used. Direct sending spam emails to recipients is a very simple technique, in which spammers do not have to hide their identities. Spam filters can easily block these techniques by blocking the email address or the IP address. Open relay is another technique used in which spammers utilises vulnerable open-relay mail servers to send spam emails to recipients. This technique is also used to hide the spammers' information, particularly originating IPs.

Using compromised computers is also another method of sending spam. This is carried out by installing malwares such as Trojan droppers and downloaders into compromised computers that allows remote access or by exploiting MS Windows vulnerabilities and other applications such as Microsoft Outlook or Outlook Express. Another contemporary sophisticated technique used in spamming is the use of spambot.

A spambot is an automated programme designed to automate the sending of spams which works by creating fake accounts. While other spambots, in addition, can crack passwords and send spam using third party accounts. E-mail spambots harvest e-mail addresses from materials found on the Internet in order to build mailing lists for sending unsolicited e-mails. Such spambots are web crawlers that can gather e-mail addresses from websites, newsgroups, special-interest group (SIG) postings and chat-room conversations. Because e-mail addresses have a distinctive format, spambots are easy to write. Spambots are effective in sending mass emails.

Spam Analysis

During the first quarter of 2011, MyCERT received a total of 641 spam reported incidents. March recorded the highest number with 282 incidents reported. Meanwhile, Malaysia is the largest spam distribution centre; about 70 percent of spam come from Malaysia and 90 percent of that concerns fake lottery winnings and gambling related emails. In Q1, 2011 most of the gambling spam used were UK National Lottery, Exxon Mobil, Microsoft and Coca Cola as their fake

representation to cheat people.

Back in 2010, many of this kind of spam used sporting events like the FIFA World Cup 2010 and AFF Suzuki Cup 2010 to cheat people. In addition, all reported spam still used the old format with no advanced techniques, such as 'spam in PDF attachments' or 'using graphics as a background image'. Although there was an increase in the amount of spam reported from January to March 2011 in Malaysia, the number of reported damage or monetary loss was minimal.

The distribution of spam sources by region in Malaysia

As shown in Figure 1, Asia continues to be the world's foremost region for the distribution of spam in Malaysia for Q1, 2011. Overall, during the period of January to March 2011, Asian countries were responsible for distributing 80 percent of the total spam volume in Malaysia, with 70 percent of them originating from Malaysia itself.

Africa is among the many regions where the fight against cybercrime is virtually non-existent. In Q1, 2011 the volume of unsolicited messages coming from African countries accounted for 7 percent of the total spam in Malaysia, exceeding that of the USA or Europe. Poor anti-spam legislation and regulations as well as a lack of IT competence provided the ideal conditions for further increasing the volume of spam being distributed from this region.

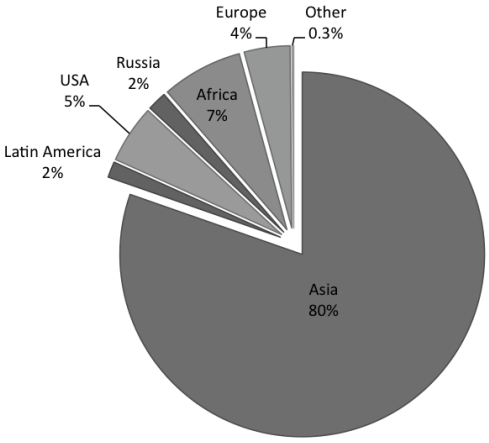

Figure 1: *The distribution of spam sources by region*

As shown in Figure 2, MyCERT noted that if a comparison were to be drawn between the spam output of Asia, Africa, USA and Europe, then the Asian region's output would be the highest. As a result, Asia continues to dominate as the leading source of spam, even when compared to the total spam output of Africa, USA and Europe as a whole (Asia 80 percent, Africa, USA and Europe 16 percent).

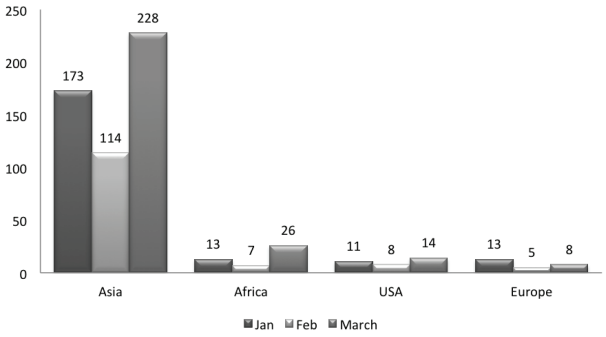

Figure 2 : *The fluctuations in spam going/directed to Malaysia*

The distribution of spam sources in Malaysia by country of origin

During Q1, 2011, there were a total of 641 spam cases being reported in Malaysia to MYCERT. Figure 3 shows Malaysia went firmly into the lead this quarter with a total of 492 of all spam detected, while USA remains a steady second place with 24. Nigeria became the top African country with a contribution of 22 spam messages.

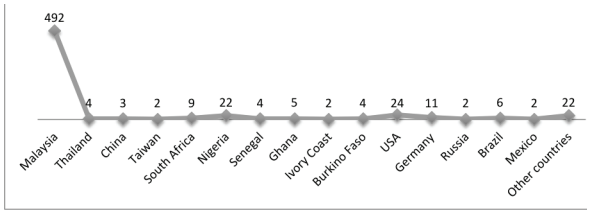

Figure 3: *Countries that are sources of spam*

Spam categories

Referring to Figure 4, the majority of spam emails are gambling advertisements and winning lottery notifications. The Personal Finance/Money recovery scam category was in second place followed by the Next-of kin category.

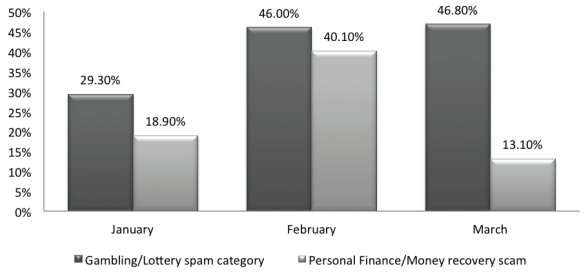

Figure 4: *The distribution of spam categories*

Gambling/Lottery was the most common spam category in the first quarter of 2011. Almost 90 percent of gambling/lottery emails came from Malaysia. As shown in Figure 5, the percentage for these scams consistently increased from January to March. Personal Finance/Money recovery emails came in second place. In February, the percentage of emails in this category reached the highest number within 3 months at 40.1 percent.

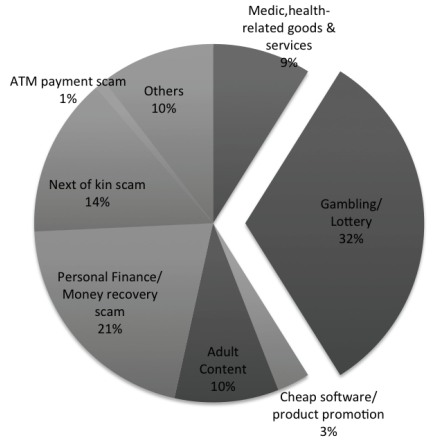

Figure 5: *The Gambling/Lottery spam and Personal Finance/ Money recovery scam categories in the first quarter of 2011*

According to Figures 3 and 4, the numbers of compromised hosts that are used to send Gambling/Lottery spam emails in Malaysia are increasing on a daily basis. From this data, we can also assume that there are many Malaysians who are still using Windows XP and the insecure Internet Explorer 6 web browser. This inevitably aids the distribution and infection rates for botnets that are used to send out spam such as Waledac, Kraken or TDL-4. It also shows that the majority of users in Malaysia lack awareness on how to securely protect their computers.

Spammers' tricks and techniques

During the first quarter of 2011, incidents involving gambling/lottery emails recorded a third of the total spam that was reported to MyCERT. The large numbers of spam recorded were on fake lottery winnings and compensation claim scams. Scammers will ask the victim to pay a certain amount to claim their winnings/compensation. Once the victim pays the fee, they will just invent a new fee that the victim has to continue paying. If the victim falls for that trick, they keep inventing a new fee, until the victim gives up or runs out of money.

If the victim becomes aware that the email that they received is a scam and stop sending money, the second stage of the fraud could occur. Scammers will introduce themselves as police officers or other employees who have been arrested or who seek to arrest the criminals in the first scam. They will promise to return the money stolen in the first scam as shown in Figure 6.

From: United Nations Compensation Fund <budirem1@neostrada.pl>
To: [redacted]
Cc:
Subject: Scammed Victims Compensation

Greetings to you,
SCAMMED VICTIM/ $900.000.00.USD BENEFICIARIES.
REF/PAYMENTS CODE: ECB/06654 $900.000.00.USD.

On behalf of the Malaysian National Sweeptakes Compensation Award,we wish to inform you of the results of the comprehensive web email search and wish to notify you as a beneficiary of $900.000.00.USD in compensation as a scam victim. This is to bring to your notice that we are delegated from the Malaysian National Sweeptakes Compensation Award in World Bank to pay 150 victims of scam $900.000.00.USD each.

Do contact CITI BANK INTERNATIONAL BANK,CITI BANK for verification and release of your $900.000.00.USD that we have deposited with the CITI BANK MALAYSIA.The account log on will be presented to you by the bank in order to access the funds before releasing into your nominated bank account.You will transfer the funds into your nominated account on-line as the CITI BANK MALAYSIA will provide the necessary information to you. If you are willing to accept the funds, do contact the Managing Director of the CITI BANK MALAYSIA, with the following details:

You are to fill the appropriate form and submit to the bank.
[1] Full Names:_____
[2] Contact address_____
[3] Direct Telephone No: _____
|4| Occupation :_____
Managing Director of the CITI BANK MALAYSIA
Name: Mr Abu Bakar Bin Saud
Email:citi_bankonline@sify.com

Yours Faithfully,
Dr. David Adams
Coordinator.
Malaysian National Sweeptakes Compensation Award© 2011

Figure 6: *Second stage of fraud for the fake lottery scam*

Why Spam is prevalent

Even though spam is a nuisance, it is still prevalent on the net with increasing statistics every year. One of the reasons why spam is prevalent is because many recipients of spam emails reply due to lack of awareness about spam emails. Many users also purchase goods through spam emails. By responding and purchasing goods through spam emails, it actually propagates further spam activities on the net.

Another reason why spam is prevalent is because spamming is a cheap way in promoting services and products. This is in addition to the many tools available on the net for free that can be used for spamming. There are also many cheap software that can be used to spam on a large scale and also the availability of various database of emails that can be purchased on the net for a very cheap price.

Another reason is due to the lack of laws in many countries that can be used to punish and prosecute spammers. Only very few countries have spam legislations such as Australia with its Spam Act 2003, Singapore and its Spam Control Act 2007 and New Zealand with its Unsolicited Electronic Messages Act 2007. Unprotected and vulnerable computers also enable spam to be prevalent on the net. Computers without anti-virus protection can lead to malicious programme infections and enable the infected computers to become spam zombies.

Spam Mitigations

Though there is no special prescription to eradicate spam entirely, certain mitigation steps can be implemented to minimise spam to some extent. Some of the steps users can implement to protect themselves are to safeguard your email address from spammers. This includes being careful when signing up online using your email address and making sure the website you sign up with is reputable and not involved in unethical activities on the net. You must not reply to a spam email or unsubscribe to a spam email as this will further propagate the spam. If your email is exposed on the net, make sure it is in the form that a spambot cannot easily detect and grab. When choosing a new email address use one that is hard to crack - make it more than a few characters long with a few unusual characters like underscores if they are allowed. You can also consider using a secondary email address to avoid publicising your primary email address or use a disposable email address. Read email in plain text, switch off the preview pane, or disable the automatic downloading of graphics in HTML emails. Do not click links on spam emails as the links may contain an encoded version of your email address and indirectly informing spammers that your email address is valid.

Using spam filtering is also an effective way of preventing spam. Spam filtering can be done at your computers, your organisation's email gateway and at your ISP level. Spam filtering at your computer can be done either by using spam filtering software or spam filtering features available in your email client, which can be configured based on keyword and routing or source of email information. The emails can be filtered to be sent to a spam-trash folder. System Administrators can install spam filtering software at their email gateways to prevent spam emails from reaching their users within the organisation. Users can also subscribe to their ISPs' spam filtering services which help to prevent spam emails from reaching the end-users' mailbox. Besides the filtering, make sure your computer is secured and running an updated version of an anti-virus software and is patched regularly. This can help to prevent your email address from being harvested from your PC or your PC being used as a spam zombie.

Conclusion

In conclusion, we can say that spam continues to grow and are still prevalent on the net. This is due to various factors such as lack of user awareness, availability of spamming tools on the net. There is no magic wand to eradicate spam. However, with safe email practices by users and proper spam filtering, spam can be minimised to a certain extent. This will eventually make spam less annoying and the Internet a comfortable place for all of us. ■

References

1. *Cyber999 Help Centre*
2. *http://www.securelist.com/en/analysis/spam*
3. *http://www.419scam.org/*
4. *http://www.scamomatic.com/*
5. *http://www.securelist.com/en/threats/spam?chapter=95*
6. *http://en.wikipedia.org/wiki/Spambot*
7. *http://en.wikipedia.org/wiki/Email_spam_legislation_by_country*
8. *http://spamlinks.net/prevent-users.htm*