MEASURES TO COMBAT SPAM

By Maslina Daud and Zahri Yunos
National ICT Security and Emergency Response Centre (NISER)
(This article was published in STAR InTech on 17 May 2005)

IN mid-December 2004, a US judge awarded an ISP (Internet service provider) the huge amount of US$1bil (RM3.8bil) in a court case involving three spammers in Iowa. The three companies were found guilty of sending the ISP's 5,000 customers millions of spam messages between August and December 2003 (see *The Star*, Dec 20, 2004) [1]

In a similar case recently, Debitel, a German-based telecoms operator, was fined a record 2mil kroner (RM1.3mil) by a Danish commercial court for sending 12,000 SMS (short message service) messages and 36,000 spam e-mail to customers of rival operator Telmore in April 2003.[2]

A common element of these two verdicts is spam.

The term “spam” should not be limited to e-mail only. It should also include other electronic media such as SMS, MMS (multimedia messaging service) and fax. Spam has become a significant and growing problem that requires a global solution. Besides being a nuisance, it costs organisations losses in terms of bandwidth, human resources and technology.

Spam is often used as a vehicle to spread viruses and worms, fraud and other deceptive content such as spoofing and phishing. This phenomenon is hampering the development of the information society by undermining user confidence and trust in online activities. Appropriate actions to solve the problem of spam are necessary at national and international levels.

There are several definitions of spam; however it is usually defined as unsolicited bulk and commercial e-mail. It becomes the subject of debate whether it is transmitted in bulk or if it is commercial in nature. Another point being hotly debated is whether an unsolicited e-mail sent to existing customers without prior consent is considered spam.

Impact and severity

Spam has become and remains one of the more rampant security problems. Exactly 14,371 spamming cases were reported to the Malaysian Computer

Emergency Response Team (MyCERT, www.mycert.org.my) last year, compared with a total of 3,383 cases in the previous year. [3]

Niser (www.niser.org.my) has been conducting the ICT Security Survey for Malaysia over the past three years when it was reported that e-mail spamming was one of the top security breaches experienced by Malaysian users.

The summary of the online survey on spam conducted in 2003 shows that:

·66% of organisations saw spam as a serious issue.

·Only 12% had taken steps to prevent it.

·82% felt the need for legislation against spam.

·74% wanted the Government to take action against the culprits.

·61% wanted the culprits punished.

·52% received about 10–50 spam e-mail messages a day.

The impact of spam on the Internet community is great, causing significant financial costs and losses in productivity. A paper prepared by the ITU World Summit on the Information Society indicated that more than half of all e-mail communication was considered spam. [4]

According to Message Labs, spam has grown to represent almost 80% of the total e-mail traffic. The estimated cost to the global economy is approximately US$25bil (RM95bil). [5]

This is due to the material cost of the time spent identifying and deleting unsolicited messages. It is therefore costly in terms of productivity and the need for technical support and software solutions.

Four-layered approach

In addressing the spam issue, there is a four-layer approach that can be considered: Strong legislation, technical measures, adoption of best practices and international cooperation.

Strong legislation

It is obvious that legislation is very much needed in order to lessen or stop spam. There are countries that have already had legislation in place in combating spam. The United States has enacted its first federal antispam law, Can-Spam Act of 2003, to regulate interstate commerce by imposing limitations and penalties on the transmission of unsolicited commercial electronic mail via the Internet. [6]

Australia has its Spam Act 2003 in place with similar objectives. [7]

Despite the legislation in place, there is always the question of its effectiveness in stopping spam. For instance, some antispam activists and observers have concluded that there is no evidence of a reduction in the number of spam e-mail one year after the Can-Spam Act 2003 went into effect. [8]

In Malaysia, there is no specific antispam law yet. However, Section 233(1)(a) and (b) in the Communications and Multimedia Act 1998 may be applied against spammers. The Malaysian Communications and Multimedia Commission (MCMC, www.cmc.gov.my) has conducted a discussion on whether the current legislation is sufficient to act against spammers.

The current steps taken by the MCMC are self-regulation by users through education and awareness programmes, management by service providers and international collaboration.

Technical measures

Although spam laws could be in place, organisations and enterprises should not expect legislation to solve their spam problems. Instead, a combination of smart e-mail management and judicious use of spam-filtering technology would be good protective measures to be deployed as the next layer in addressing the spam issue.

In implementing technical measures to curb spam, three different stages in the e-mail system need to be accounted for: The source where the e-mail is sent out; the destination where the e-mail is received; and at the enduser's e-mail client.

For every stage, various technical measures such as filters could be applied. [9]

Adoption of best practices

Organisations and individuals should strive for the highest antispam best practices.

Realising this, Niser established the Anti-Spam Working Committee in July 2004 with the objective of providing a framework that can be made as a reference for the Malaysian Internet community against e-mail spamming.

Members of the Working Committee include government agencies, Internet service providers, Internet datacentres, antivirus solution providers, antispam solution providers and e-mail marketing organisations. After three thorough brainstorming sessions, the working committee then produced the "Anti-Spam Framework of Best Practices and Technical Guidelines." This document focuses on spam that originates from e-mail.

In developing this document, a set of guiding principles was emphasised in addressing the qualities that should characterise best practices for antispam to be adopted and complied with by organisations and individuals.

Those principles include: The need to respect the privacy of those individuals and organisations; for them to strive for the highest antispam standards; utilise the latest antispam technology and to comply with existing legislation. Another guiding principle that was taken into account is providing lawful outlets for marketers.

Best practices in the document are structured in accordance with areas which have significant roles on Internet. The six areas are organisations, home users, marketers, providers of Internet service, providers of webhosting and mailing list management service. For each area, those best practices were further segregated into four categories: Awareness, technology, procedures, and compliance and enforcement.

International cooperation

Spam mostly originates from other countries. Thus, international cooperation in addressing spam is regarded as the best approach if most governments combine it with domestic legislation. On Oct 20, 2003, NOIE (currently known as the Australian Government Information Management Office) and the Australian Communications Authority (ACA, internet.aca.gov.au) signed a Memorandum of Understanding with the Korea Information Security Agency (KISA, www.kisa.or.kr) which sets out the cooperative arrangements between those bodies for sharing information and intelligence about spam-related activities. The MoU with South Korea is anticipated to be the first of many international agreements. [10]

Other initiatives include arrangements between Australia, Britain and the United States in providing a framework in fighting cross-border spam affecting those three countries.

In a similar development, in Japan recently, some 30 Japanese companies including leaders in the computer and mobile phone industries said they would form a body to fight spam, saying the country was lagging in stopping e-mail abuse.

The Japan E-mail Anti-abuse Group will be formed to attack spam at the technical level in addition to having groups address the problem from a legal angle. [11]

Conclusion

Every year mountains of spam messages are sent to users, and every year the perpetrators devise more devious and vicious methods to send even more spam using various platforms. It is not a major problem yet, but as VoIP (Voice-over-Internet Protocol) grows over the next few years, it is anticipated that “spitters” will be ready to send thousands of spam to VoIP voice-mail boxes with only a simple click.

There are always points to ponder on – whether the current practices and regulations in place globally are sufficient to combat spam as more and newer technologies and sophisticated attacks are to be produced. Only time will tell.

References

[1] "Internet Service Provider Awarded $1 Billion in Spam Damages", by Grant Gross, IDG News Service, December 20, 2004, http://www.pcworld.com/news/article/

[2] "Denmark fines mobile operator for SMS Spam", by John Leyden, The Register, March 16 2005, http://www.theregister.co.uk/2005/03/16/debitel_sms_spam_fine/

[3] www.mycert.org.my

[4] International Telecommunications Union, World Summit on Information Society Thematic Meeting on Countering Spam, Spam in the Information Society: Building Frameworks for International Cooperation <http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Building%20frameworks%20for%20Intl%20Cooperation.pdf

[5] MessageLabs, *Spam is still growing*, ZdNet, June 14 2004, online at <http://zdnet.com/2102-1105_2-5233017.html?tag=printthisH>

[6] http://www.spamlaws.com/federal/108s877.shtml

[7] http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm

[8] http://www.pcworld.com/news/article/0,aid,119058,00.asp

[9]http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_Curbing%20Spam%20Via%20Technical%20Measures.pdf

[10] http://www.agimo.gov.au/media/2003/12/2940.html

[11] "Japanese companies join forces to fight spam", Technology AFP, March 15,2005,http://story.news.yahoo.com/news?tmpl=story&u=/afp/20050315/tc_afp/japaninternetspam