Global Information Assurance Certification Paper

GSLC Version 1.0

- SPAM in the Enterprise -

Kevin Agnew
August 25th, 2003

Table of Contents

Abstract

Spam is defined as unsolicited or unwanted e-mail. There are many challenges in defending an enterprise against Spam as Spammers attempt mass e-mail distributions utilizing any vulnerable host such as SMTP gateways, proxy servers or even user workstations. Spammers obscure their identity, use phony unsubscribe mechanisms to verify a user, brand spoof, use false subject lines to get the user to open the message and make pornographic or fraudulent offers.

Relevance of SPAM

The Aberdeen Group estimates that by mid-2003 as much as 50% of total corporate e-mail traffic will be SPAM[1].

Spam touches many different facets of a business to lost productivity of employees, potential distribution of e-mail viruses and malware[2], increased bandwidth consumption, excessive storage consumption, brand spoofing and the potential legal implications of employees not being protected by the corporation, particularly in the case of pornographic spam.

In addition to the available antispam technologies, reducing spam in the enterprise requires corporations to practice due diligence in applying patches to SMTP gateways and proxies. Workstations must also be included in the patch management and antivirus updates as spammers are known to hijack workstations to distribute spam.

Business Implications of SPAM

A majority of the cost of SPAM is the lost productivity for users having to process these messages. SPAM messages are written to entice the user to open it, almost always contain “intriguing” URLs to again get the user to investigate further. With the expectation that the proliferation of spam will continually increase year after year this hidden cost to the business is quite substantial. All of this is wasted time from a business perspective for the user to process the e-mail forcing Corporations to invest in anti-spam technologies as a method to combat spam and increase productivity.

One concern with antispam technologies is separating spam from legitimate e-mail. Even within an organization there are conceivably different definitions of spam from various user groups. Some keywords or phrases for one group may be spam but for another, legitimate e-mail. This raises the issue of false positives and potentially the corporation losing valid business e-mail as it is being flagged

inappropriately. In order to ensure no e-mails are lost corporate resources would have to be tasked to review and classify the false positives.

The Internet bandwidth, paid for by the corporation, which SPAM utilizes for delivery, is unavailable to other legitimate business functions. The spammers are using the resources of the corporation and ISPs at no cost to them. The bandwidth loss has potential customer impact for businesses with an online presence or to a business using Internet connectivity for any necessary function.

E-Mail systems require excess storage availability to hold the SPAM. Indirect impacts of SPAM entering an organization are the longer backup window of the e-mail system, more space required on the backup media and more disk for the e-mail database itself. In addition, supporting software such as antivirus, are required to process more messages, requiring more processing cycles leading to a degradation of system performance.

Brand spoofing damages a company's reputation. SPAM is sent appearing to be from a legitimate company to again try and lure the user to divulge personal information. The company loses business directly impacting the bottom line due to the lost confidence in the marketplace. This is an intangible cost so is very difficult to put a dollar value on. It is also hard for the company, once targeted, to prevent this from happening.

"The latest trend in spam and identity theft is called brand spoofing. The spam has no traceable return address and appears to be sent from a large company seeking information from its customers"3

Due to the attention SPAM is getting from Businesses and the public, laws to deal with this issue are being passed[4]. The laws do not prohibit spam, but make it easier for detection by spam solutions thus preventing it from getting to the users mailbox. These laws are the step in the right detection but still need to evolve further to completely protect the enterprise or, at the very least, provide a recourse action for the company to recoup potential losses. There must also be some consistency in the laws across countries as the world wide presence of the web presents spammers many opportunities to exploit servers in any part of the Globe. Until there is an outright ban with penalties of heavy fines or imprisonment there is little, legally speaking, discouraging spammers from continuing their trade.

Security Implications of SPAM

Improperly configured SMTP servers, known as open mail relays, do not require any authentication, accept e-mail from any IP address from any origin and will deliver to any e-mail address. This is obviously an ideal environment in aiding spammers. Corporations must implement policies and procedures for ensuring all public facing servers do not get deployed without being locked down. In addition

another set of policies and procedures must be in place to ensure proper system updates and patches occur at regular intervals.

Internal e-mail servers must also remain protected. Spamming an e-mail virus or worm is a serious threat to any corporation. As another level of defense corporations have to remain diligent in patching gateways and keeping antivirus software updated.

The purpose of a SPAM message can be used to spread a Trojan horse[4]. The e-mail itself may be seemingly harmless but its real purpose may be to open a backdoor for access at any future point in time. In addition to the perimeter patching, e-mail server patching, workstations must also be part of the defense in depth strategy.

Yet another level to protect the Enterprise would be to deploy a URL filtering package to prevent users from accessing the websites contained in the spam. Sites can be blocked by URL, IP address or by the broader filter of site categories.

Spammers can obtain company e-mail addresses from websites by a technique called harvesting. A security policy limiting the exposure of company e-mail addresses on web sites would help keep internal e-mail addresses internal. There are, however, legitimate reasons for businesses to utilize web support or discussion groups so employees should be instructed to be cautious about divulging their e-mail addresses in places where it may be harvested. These measures do not solve the problem but combined with the other defense strategies will make it easier for an enterprise to prevent the spam epidemic.

Along with the standard defense techniques mentioned above there are other technologies available that are targeted specifically at controlling spam. Techniques used by these devices protect the Enterprise against,

- Address Harvesting – Spammers connect to a company mail server and attempt to deliver messages to recipients using a dictionary of user names.
- Anti-spoofing – Typically mail servers will allow any e-mail to pass from its own domain. Spammers spoof the from address so the e-mail passes unchecked.
- DNS checks – Spammers using forged domain names. A DNS lookup to verify the domain name would stop this type of spam.
- Blacklists – Known spammer IP addresses can easily be blocked.
- Text Analysis Tools – Able to search for keywords in the message.

There are obvious costs for any antispam solution including the training of support staff, installation and ongoing maintenance. Also policies and procedures governing the use of the antispam system such as assigning ownership and dealing with false positives must be developed and implemented.

Defending against SPAM is not unlike defending against any other threat. The Defense in Depth strategy will go a long way to ensuring business risk is mitigated. Perimeter devices need to have the latest patches, up to date antivirus definitions, workstations also with the latest patches and virus definitions. Clear policies on using company e-mail addresses on websites and, most importantly, a well trained user community will go a long way to defending the Enterprise.

References

1. "2003 Predictions for Security and Privacy", The Aberdeen Group
   http://www.aberdeen.com/ab_company/researchareas/Security2003.htm

2. "Spammers and virus writers unite"
   http://news.bbc.co.uk/1/hi/technology/2988209.stm

3. "Warning goes out on New SPAM Attacks", Sharon Gaudin, July 10, 2003
   http://itmanagement.earthweb.com/secu/article.php/2233661

4. "Texas anti-spam law takes effect Sept. 1"
   http://www.chron.com/cs/CDA/ssistory.mpl/headline/tech/2061448

5. "Trojan turns victims into DDoS, SPAM zombies"
   http://www.securityfocus.com/news/6419