Global Information Assurance Certification Paper

Open Mail Relays – SPAM Gateways

GSEC Practical Assignment (v.1.4b)

Bobby Hunter
December 17, 2002

ABSTRACT

SPAM is defined as "unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups" [1]. And, while there are several different mediums available for one to distribute such material, one of the easiest and most popular methods remains via open mail relays.

This paper will provide an overview of open relay servers, including what they are, how they are identified and utilized, the potential consequences to the organizations that own them, and how those organizations can protect themselves.

INTRODUCTION

It is possible that SPAM has surpassed viruses as the single largest concern to e-mail systems administrators and users alike. "We are in the midst of a SPAM epidemic", says Daniel Tyman of PC World, and that, "according to e-mail filter vendor Brightmail, the number of SPAM attacks has risen by more than 500 percent since March 2001" [2].

While it is possible, and in these times necessary, to take defensive measures against the thousands of porn site advertisements and financial scams that plague Inboxes, it must also be realized that open mail relays are a distribution medium for SPAM and are contributing to the "SPAM epidemic". In many cases, making a contribution toward reducing the impact of SPAM on the industry can be as simple as a single mouse click.

IDENTIFICATION

An e-mail server is designed to store and exchange local users' messages both to and from internal and external recipients. The server recognizes that either the sender or receiver of a particular message is a local user and processes the message in the manner in which it has been instructed. When a mail server will process messages when neither the originator nor recipient can be identified as a local user, it is acting as a third party, or open mail relay. It is via this medium that spammers are able to utilize the resources of a third party mail server to distribute unsolicited bulk e-mail messages.

Open mail relays are attractive to spammers for several reasons:

- The IP address of the open relay conceals the actual SPAM source, and prevents its address from being added to blacklists, or assists in evading any blacklists that it may already have been placed on.
- Through their use, spammers can increase the volume of SPAM distribution. If they are able to utilize the services of more than one open relay server concurrently, they can potentially increase message distribution volume exponentially.
- Distributing SPAM via open relay servers allows spammers to utilize the computing resources, such as network bandwidth and storage capacity, of a third party.
- Distributing SPAM via open relay servers allows spammers to avoid the limits and terms that their own Internet Service Providers (ISPs) have set forth in their Acceptable Use Policies.

There are several factors related to open relay servers playing a role in the problems that SPAM has introduced, including: Spamware, bulk e-mail services, Korean and Chinese relays, and even ISPs themselves.

SPAMWARE

Locating open relay servers has become increasingly easy via the use of Spamware. Spamware is bulk email software whose principal design and purpose is to send unsolicited bulk email [3]. Through the use of simple graphical interfaces, Spamware makes it particularly easy for spammers to "hide the sender, falsify the origin information, use multiple relays, disguise URLs to obstruct identification of web sites advertised in the SPAM, or attempt to circumvent ISP SPAM filters"[3]. Spamware can also include databases of hosts known to be vulnerable to relay highjacking, which makes finding an open relay relatively simple [4]. And, although they are very easy to find and use, it should be noted that 8 U.S. States, including Connecticut, Delaware, Illinois, Oklahoma, Rhode Island, Virginia, and West Virginia, have passed legislation that has made the sale or distribution of stealth Spamware applications illegal [3].

BULK E-MAIL SERVICES

In addition to Spamware applications, there are bulk e-mail services organizations contributing to the SPAM scourge – offering their computing resources as "for hire" for the distribution of SPAM. Havoc Systems, for example, offers server space and bandwidth to mass e-mailers for a charge, in addition to marketing and selling their own Spamware, as well as software tools that harvest addresses and manage lists.

KOREAN AND CHINESE RELAYS

It has been documented that a large number of Korean and Chinese schools have been identified and blacklisted as sources of SPAM via open relay servers. The problem is reported to be a threat to e-commerce in these nations, because many systems have been configured to reject communications from them. Due to the volume of SPAM being relayed through the IP address ranges of these nations, the simplicity of blocking all e-mail communications from them is very appealing [5].

INTERNET SERVICE PROVIDERS

Many ISPs have developed Acceptable Use Policies that contribute to the fight against SPAM, however, as spamhaus.org reports, there are a number of ISPs that "support and profit from the SPAM industry, provide hosting for SPAM service purposes, and knowingly fuel the Internet's SPAM problem" [6]. With SPAM services creating high volumes of data traffic, and ISPs making money based on the amount of data traffic created by their clients, some ISPs have refused to prohibit the transmission of SPAM on their networks.

With all of these factors considered, it is easy to predict that the SPAM problem is only going to grow worse. A study conducted by Jupiter Media Metrix states that "by 2006 a typical consumer can expect to receive nearly 1500 servings of SPAM annually – double the number that the average user gets today" [1].

CONSEQUENCES

Many organizations have been able to make a profit via SPAM, whether they are the organizations advertising products or services in unsolicited bulk mailings, or the organizations providing the services themselves to distribute the material. "SPAM wouldn't exist if it weren't so successful", states Jared Blank of Jupiter Media Metrix [1]. However, while SPAM has contributed to economic success for some, there are others dealing with the consequences that SPAM, and owning an open relay server, knowingly or not, have incurred upon them. All of the potential consequences seem to impact the financial well being of an organization in one way or another. These include:

- Unscheduled system downtime
- Inclusion on anti-SPAM blacklists
- High jacked computing resources
- Legal repercussions

SYSTEM DOWNTIME

With spammers utilizing the services of a mail server to send thousands of unsolicited bulk messages, in addition to, depending on the size of the

organization, the thousands of valid messages being exchanged by local users of the system, a mail server could easily become overwhelmed and fail. The mail server experiences a Denial Of Service and becomes unavailable for use, which can be costly to the organization in several ways. An organization that is unable to communicate with its customers or clients in a convenient and efficient manner, which in these times is very often via e-mail, is an organization that stands to experience a significant economic impact. The cost of replacing hardware, potentially made necessary by a system failure of this type, could also be significant and should be considered. In addition, the costs of compensating qualified personnel to bring systems back online and restore functionality must also be factored into the equation.

BLACKLISTS

There are several anti-SPAM organizations that house blacklists aimed at restricting the ability of mail servers that have been identified as open relays distributing SPAM from being able to deliver those messages to other domains. While this is an effective way to prevent the transmission of SPAM, it can also limit an organization's ability to transmit valid business communications via e-mail. As long as an organization's mail server is on one or more blacklists, it is potentially unable to communicate with both current and prospective customers and clients, which again could have a significant economic impact. Additionally, being included on any one blacklist has the potential to tarnish an organization's technical reputation, and possibly affect the ability for it to attract new customers or clients.

COMPUTING RESOURCES

If an organization's mail server is being utilized as a relay server by a third party, computing resources such as storage capacity and network bandwidth are effectively being stolen. Many ISPs bill their customers based on their bandwidth utilization, which can increase significantly if a mail server is being used as a relay. "SPAM costs businesses worldwide some $8 billion to $10 billion per year in bandwidth charges alone, according to estimates by the European Union" [1]. It is also possible that a server being used as a relay could cause an organization to violate the Acceptable Use Policy of its ISP and be forced offline. This scenario could be cause for additional downtime and potential lost revenue, especially if an organization were forced to locate service through another ISP. Add to all of this the additional local disk capacity required to store and forward the thousands of unsolicited bulk messages that arrive daily, and the potential cost of these resources to an organization can multiply very quickly.

LEGAL REPERCUSSIONS

Legal repercussions, although arguably a threat that is still in its infancy, are now being introduced as another weapon in the fight against SPAM in an effort to hold

organizations accountable for contributing to the problem. There are now several governments that have either passed, or have pending, legislation aimed at assisting in reducing the amount of unsolicited bulk mail that clogs their networks. One example of pending legislation against SPAM in the United States is the Unsolicited Commercial Electronic Mail Act of 2001, which has endured several stages of review. An Amendment to the bill outlines proposed criminal penalties against a party in the event that it:

> "intentionally initiates the transmission of any unsolicited commercial electronic mail message to a protected computer in the United States with knowledge that any domain name, header information, date or time stamp, originating electronic mail address, or other information identifying the initiator or the routing of such message, that is contained in or accompanies such message, is false or inaccurate." [7]

Legislation in Europe also exists that requires "senders of advertisements by "electronic mail" to have the recipient's prior consent [8]. This "opt-in" statute is similar to sections of the proposed Unsolicited Commercial Electronic Mail Act of 2001 that state "the provider shall provide an option to its subscribers not to receive any unsolicited commercial electronic mail messages" [7].

In a recent legal development involving unsolicited bulk mail, PC World reported on December 16, 2002, that the U.S. District Court of the Eastern District in Virginia ruled against SPAM outfit CN Productions and ordered them to pay America Online $7 million, as well as to cease the distribution of unsolicited bulk mail to AOL subscribers. "AOL alleged that CN Productions and its conspirators had transmitted more than 1 billion junk e-mail messages to its members" [9]. Underlining the fact that legislation is still being molded to become a factor in the fight against SPAM, is the claim that the damages awarded under this ruling were the first under a new amendment to the "Virginia anti-SPAM statute that provides fines of $25, 000 for each day SPAM is sent" [9].

While the development and enforcement of SPAM related legislation has been slow, this, along with the additional open relay-related repercussions discussed, should be taken seriously as a potential consequence of SPAM distribution due to the financial and corporate image-related implications that come with it.

PREVENTION

With all of the consequences of owning an open relay server and being identified as a source of SPAM considered, organizations must look for ways to be proactive and prevent any of the implications from affecting their business operations. There are several options available, all of which exist at various levels of financial commitment, for an organization to contribute defensively to the fight against SPAM and to ensure that they are not part of the problem. These include:

- Application firewalls

- Review local configurations
- Perform relay testing
- Deploy anti-SPAM software
- Become an anti-SPAM advocate
- Review ISP Acceptable Use Policies

APPLICATION FIREWALLS

Application specific firewalls can provide an organization with an option to deploy a defense-in-depth strategy. An e-mail application firewall, specifically, might work in conjunction with, and complement, a traditional firewall and intrusion detection system by focusing on specific SMTP ports and services. "Application firewalls overlap onto the domain of traditional firewalls and IDS systems, but offer a different type of protection that neither of them or both can offer" [10]. Several e-mail firewall vendors advertise that their devices are capable of multiple functions, such as SPAM prevention via proprietary content filtering technologies, anti-virus protection via third-party detection engines, web mail and hacker protection, e-mail policy enforcement, and so on. One very appealing function of an e-mail firewall as it applies to this discussion is that some available devices can be configured to block unauthorized relay attempts while allowing local users, such as remote employees, the ability to relay as required. And, in addition to all of this, an application firewall "can also be used to reduce the amount of possible information that an attacker can glean from the system it protects" [10], as well as provide valuable reporting information to an administrator. Unfortunately, this type of solution may fall outside the reaches of several organizations due to the potentially high costs associated with it.

PERFORM RELAY TESTING

There are ways for an organization to take the defensive to ensure that their servers will not be utilized as open relays, with the only potential financial setback being the cost of an administrator or consultant's time. An organization can take the time to perform relay testing on their own servers to ensure that they are secure in this manner. There are several websites that offer experimental relay testing services that are free of charge and as simple to use as typing in the name or IP address of the server in question. These tests may be simple, but can help to point an unsure administrator in the right direction. Another simple test that can be performed against a mail server to determine whether or not it will allow relaying is via TELNET, if its configuration will allow for it. By opening a TELNET session and establishing communication with a mail server, an administrator can determine the relaying status of a mail server through a few typed commands. The command sequence via a command prompt should appear as follows, if the server being tested will not allow relaying:

TELNET [*mail server name or IP address*] 25

At the TELNET ready prompt:

MAIL FROM: [external internet e-mail address]

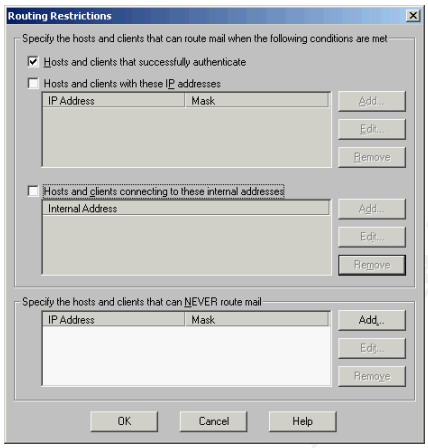
250 OK – mail from <external internet e-mail address>

RCPT TO: [external internet e-mail address]

550 Relaying is prohibited

REVIEW LOCAL CONFIGURATIONS

In many cases where an organization is found to be operating an open relay server, they can be doing so unknowingly or mistakenly due to an oversight or lack of knowledge on the part of an administrator. Another defensive option available to an organization for only the cost of an administrator or consultant's time, is to review the configuration of their server to ensure that its settings will not allow unauthorized relaying. For some platforms, the difference between becoming a bad citizen of the Internet by hosting an open relay server and being a responsible e-mail system administrator are a few simple mouse clicks. The Routing Restrictions page in the properties of the Internet Mail Service on an Exchange 5.5 server, for example, is one location where a configuration setting can make the difference for an organization.



ANTI-SPAM SOFTWARE

Although anti-SPAM software will not assist with open relay server issues, it is mentioned here as an effective way to reduce the amount of unsolicited bulk mail that is received and as a weapon in defending against SPAM. Anti-SPAM software does exactly what its name suggests, and there are numerous products on the market from which to choose. It can be argued that anti-SPAM and anti-virus software can be mentioned in the same breath in these times, underlined by the fact that many anti-virus suites now offer some sort of anti-SPAM solution as well. As discussed previously, there are also many e-mail application-level firewall appliances that include anti-SPAM components as a part of their functionality. As the SPAM problem continues to grow, anti-SPAM software packages will be a necessary component of any e-mail system.

BECOME AN ANTI-SPAM ADVOCATE

Like anti-SPAM software, promoting the anti-SPAM movement will not assist directly with open relay server issues, but it can provide an individual with another method in contributing to the defense against SPAM. There are many websites dedicated to the efforts being made against SPAM that can provide an individual with a medium to learn about everything from new defense mechanisms, technologies, and prevention methods, to current SPAM-related legislative developments taking place around the world. Many of these same sites offer a system of reporting newly discovered sources of SPAM, which contribute to blocklists, as well as a way of searching and locating existing IP addresses and domains that have been identified as distributors of unsolicited bulk mail.

REVIEW ISP ACCEPTABLE USE POLICIES

With ISPs being identified as a potential contributor to the problems that SPAM has introduced, an organization may want to review the Acceptable Use Policy of their own ISP as another means of defense. With some ISPs still refusing to prohibit the transmission of unsolicited bulk mail on their networks, the choice of service providers could have financial implications for an organization. With a certain number of ISPs still supporting and profiting from the SPAM industry, an organization could find itself unable to conduct legitimate business communications in the event that its ISP ends up on a SPAM blocklist. However, many major service providers now have clauses and stipulations in their policies banning SPAM service sites and the act of spamming itself.

CONCLUSION

As technology continues to advance and grow, so too will the means by which unsolicited bulk mail is transmitted, paralleled by the problems that it presents to e-mail systems administrators and users worldwide. SPAM is a rapidly growing problem, and its distributors have and will continue to find alternate mediums by which to deliver their product by. It is up to the information technology and information security sector to find the defense mechanisms required to protect our networks from both current and future exploits. Addressing the problem of open relay servers and the role that they play in this "SPAM epidemic" may not be the only solution, but is an important step toward reducing the overall impact that is felt in our industry.

BIBLIOGRAPHY

1. URL: http://dictionary.reference.com/search?q=spam

2. Tyman, Daniel. "Spam Inc.". PC World Magazine, August 2002.
URL: http://www.pcworld.com/resource/printable/article/0,aid,101769,00.asp

3. URL: http://www.spamhaus.org/rationale.html

4. Nicholas, Nick. "Spamware Defined". Feb. 2, 2000.
URL: http://mail-abuse.org/rbl/spamware.htm

5. Hunter, Jean. "Korean School Relay Spam: A Blot On Korea's IT Reputation".
Mar. 19, 2002. URL: http://www.emailclub.net/bbs_read.html?db=asia1&no=34

6. URL: http://www.spamhaus.org

7. "United States of America - Federal Laws - Unsolicited Electronic Mail Act of 2001". URL: http://www.emailpilot.com/publicroot/main/spam/107-2.html

8. "Europe Outlaws Spam". May 30, 2002.
URL: http://www.spamhaus.org/newsdog.lasso?article=112

9. Weiss, Todd. "AOL Wins $7 Million From Spammers". Dec. 16, 2002
URL: http://www.pcworld.com/news/article/0,aid,108007,00.asp

10. Permeh, Ryan. "The Use of Application Specific Security Measures In A Modern Computing Environment". Mar. 22, 2001
URL: http://www.eeye.com/html/Research/Papers/DS20010322.html