Global Information Assurance Certification Paper

Controlling Spam in a Small Business

GSEC Practical Assignment Version: 1.4b

Option 1

Nadim El-Khoury
August 30, 2003

Table of Contents

Abstract

Junk e-mail is on the rise and it seems that spammers are using every tool and technical advantage that is at their disposal to bombard everyone with their unwanted mail. Small companies are at a particular disadvantage because often they do not have a system administrator that is maintaining the IT infrastructure. This paper will explain methods spammers are using to exploit e-mail, and what measures are being taken by ISPs to curb the effect of spam. But most importantly what the choices that are available for small companies to control the effect of spam on their business and the productivity of their employees. Also, knowing full well that there is not a fully-effective method to disallow spam from coming through; preparedness is the only option to help reduce the effect of spam on employees as well as company resources.

Introduction

As we have seen in recent weeks, the "SoBig.F" virus has caused large amounts of damage and has wasted valuable resources both in combating the virus as well in lost productivity. E-mail systems were overwhelmed and employees that depended on e-mail to get their jobs done found themselves scrambling to work around this obstacle. My motivation in writing this paper is to give a system administrator, especially in a small company, an idea of what spam is and what is being done to fight it as well as to provide him/her with resources to educate their users. With an educated public the effect of such viruses and spam can be substantially reduced.

Why worry about spam?

Spam is an issue because it places the cost of these mailings on the consumer. With direct mail and most other forms of unsolicited advertising, the advertiser pays to send the ad, and the consumer is merely burdened with the inconvenience or annoyance of receiving and reading or deleting it. This is not the case with spam.

The cost to the spammer is the same whether he or she sends one e-mail message or a million. The majority of the cost is being passed along to the recipient. This cost could come in the form of storing the unwanted e-mails on disks, to having to buy more powerful spam blocking software, or even the loss of productivity by the employee. "Each year spam costs each U.S. end user between $30 and $50 and companies $730 in lost productivity for every employee with e-mail, according to the Anti Spam Research Group."[15]

The effects of spam are to paralyze computer systems, gobble up disk storage space, and essentially drain time and resources from the internet companies that are forced to store and process these messages. In its simplest form, spam is a waste of resources. Additionally, spam is irritating and often the content (advertisements for pornographic sites, penis and breast enlargement) is offensive.

The problem is worldwide and growing in scope and magnitude. It affects almost all e-mail users worldwide, wherever Internet connectivity and SMTP-based mail services are available. For example, the SoBig.F virus has "affected nearly 6 percent of e-mail messages worldwide since August 18th 2003" [14]. In terms of scope, we are now seeing spam expand to include other aspects of electronic communication such as IM (Instant Messaging), and cell phones as well as the old famous fax spam.

Why is spam an information security concern?

Spam is not just a nuisance anymore. It is a threat to every company regardless of its size. Hostile spam contains viruses, Trojan horses, and worms. These are very dangerous because they can be used to destroy the contents of your computer, can spread like wildfire inside your company and overwhelm your e-mail systems. This was first demonstrated by "Melissa" virus back in 1999 and now by "SoBig.F" which has been declared "the fastest spreading e-mail plague of all time" [9]. The "SoBig.F" is a classic example of a hostile spam that contains a Trojan horse that uses the victims PCs to relay spam e-mail.

It is evident that we have not learned our lessons from the Melissa outbreak. Companies rushed to purchase and install anti-virus software. The problem with this approach is that in many cases, the anti-virus software cannot block the virus until after it has already become a problem. The anti-virus software cannot block the virus until a virus definition file has been produced by the anti-virus software company. This often happens well after the virus has begun to spread. Anti-virus software is of definite assistance in attempting to block these viruses, but is useless if the virus definition files are not updated frequently. The burden is on the user/admin to monitor for virus definition updates and keep their software current.

How can you prevent such a virus if you do not have the antidote?

Viruses are also a security threat because while a large portion of the company resources are being dedicated to fight that one nuisance (the virus), a real attack could be occurring somewhere on your network or from your network toward the network of another company. For many viruses and worms to spread they use the well known SMTP protocol and take advantage of known security

weaknesses that have emerged over the years in popular programs like Sendmail or Exchange. This is the basis of many of these exploitations.

What is SMTP?

Simple Mail Transfer Protocol (SMTP) is the network protocol used to send e-mail across the Internet. It is a "store and forward" system which was an acceptable concept when the networks were open and trusted. One of the major problems with SMTP in the past was the "open relay system". Mail relay is the process of sending mail from one mail server that is being forwarded along to another mail server on a different domain. Historically, SMTP servers did not check to verify that the sender was who he claimed to be and would simply pass the mail on with whatever return address was specified. Unsolicited bulk mailers have taken advantage of this to send huge volumes of mail with invalid return addresses. Understanding how a message is put together will definitely help the system administrator in stopping spam.

Anatomy of a message

To be able to stop spam, one need to understand the components of an e-mail message. An e-mail message consists of header fields and a body. The headers hold message routing information and are name-value pairs that are delimited by a colon. Some of the headers are required and others are optional. Headers must appear before the message body and be separated by a blank line. Usually headers will appear in the following order: [1]

- Return-Path
- Received
- Date
- From
- Subject
- Sender
- To
- CC
- Others

The first three (return-path, received, and date) are created by an MTA (Mail Transfer Agent) such as Sendmail, Exchange, Lotus Notes, etc.... Date, From, and either To or BCC are mandatory while CC, and Subject are optional.

This is what sample headers would look like after a message has been received.

```
From Nadim_Elkhoury@domain.edu  Mon Jul 14 21:54:28
2003
Return-Path: <Nadim_Elkhoury@domain.edu>
Received: from login9.domain.edu (login9.domain.edu
[10.10.0.1])
        by veloce.domain.edu (8.12.9/8.12.9) with SMTP
id h6F1rRxJ001988
        for elkhoury@veloce.domain.edu; Mon, 14 Jul
2003 21:54:03 -0400 (EDT)
Date: Mon, 14 Jul 2003 21:53:27 -0400 (EDT)
From: Nadim Elkhoury@domain.edu
To: elkhoury@veloce.domain.edu
Message-Id:
<200307150154.h6F1rRxJ001988@veloce.domain.edu>

Testing to see what the headers should look like.
```

Please note that in the example above, all of the important headers (**From**, **To** and **Date**) are present and also that the **Message-Id**, **Return-Path** and **Received** headers were actually created by the MTA.

Having a better idea of the components of an e-mail header and where they are generated lets us look at how some spam techniques are being manipulating headers to deceive users and bypass filters.

Spam Techniques

Spammers seem to always be a step ahead of everyone. On a daily basis they find new methods to bypass filters. There are different types of filters that administrators and users can use to fight spam. There are the client based rule sets and filters as well as server-based ones. The Mozilla Bayesian junk mail filter is an example of a client-based tool used to filter out spam. Microsoft Outlook has a “rules wizard” that can help you set your own rules.

The techniques range from misspelled words, sending e-mails from what appears to be yourself and make you think that the message is from a friend by changing the messages in the subject line.

Here is an example of the headers from a spam that I received. The **From** address of nelkhour@domain.com has been made to look like my **To** address of nelkhour@example.com. Other spammers have actually made the From address and To address look exactly the same. But if you look even closer in the headers you should notice that the **Received** header has a different domain name from the domain name that was inserted into the **Message-Id** header by the SMTP server that sent this mail message out.

```
X-Message-Info: JGTYoYF78jEHjJx36Oi8+Q1OJDRSDidP
Received: from qtrirj.domain.com ([10.0.1.2]) by mc6-
f16.law1.example.com with Microsoft
SMTPSVC(5.0.2195.5600);
  Mon, 9 Jun 2003 21:53:00 -0700
Received: from m182.domain.com by qtrirj.domain.com with
SMTP for nelkhour@example.com; Tue, 10 Jun 2003 00:54:27 -
0500
From: nelkhour@domain.com
Date: Tue, 10 Jun 2003 00:54:27 -0500
Message-Id: <20030610005427.0182xx5bykaq974@bogus.com>
To: nelkhour@example.com
Content-Type: text/html;
 charset="us-ascii"
Subject: Bigger breasts in 30 days. All natural and safe
Importance: Normal
MIME-Version: 1.0
X-Mailer: Microsoft Outlook Express 5.00.2615.200
Content-Transfer-Encoding: 7bit
Return-Path: nelkhour@domain.com
X-OriginalArrivalTime: 10 Jun 2003 04:53:02.0005 (UTC)
FILETIME=[2BF44E50:01C32F0C]
```

Here is another set of headers in which the **From** address does not match the **Received** header field.

```
X-Message-Info: JGTYoYF78jEHjJx36Oi8+Q1OJDRSDidP
Received: from domain1.com ([10.0.1.2]) by mc1-
f2.law16.example.com with Microsoft
SMTPSVC(5.0.2195.5600);
  Tue, 15 Jul 2003 14:05:52 -0700
Message-ID: <3F146CFC.D6700455@domain1.com>
From: "Cathrine Thomas" <cathrinethomasuh@domain.com>
To: nelkhour@example.com
Subject: Did you find the file?
Date: Tue, 15 Jul 2003 21:07:08 +0000
MIME-Version: 1.0
User-Agent: Mozilla/5.001 (windows; U; NT4.0; en-us)
Gecko/25250101
Content-Type: text/html
Content-Transfer-Encoding: 8bit
Return-Path: cathrinethomasuh@domain.com
X-OriginalArrivalTime: 15 Jul 2003 21:05:53.0382 (UTC)
FILETIME=[E076D860:01C34B14]
```

The popular free e-mail system Hotmail.com inserts the following header fields:

X-Originating-IP which would contain the user's actual IP number
X-Originating-Email header which would contain the user's actual Hotmail e-mail account

This is done to ensure that the mail came from one of their users.

Why are the discrepancies in the headers fields so important in assisting administrators who are trying to block spam? The answer is very simple. Understanding how spammers exploit our e-mail systems by forging headers is a key to stopping spam in its tracks. The more you familiarize yourself with falsified headers the more effective you will be at stopping them and making sure that your system remains efficient and uncompromised.

Spammers maintain an asymmetric relationship to their "spammees". They have our identity (email address) but we don't have theirs. Spammers use several techniques to get our email addresses. One method is using robots that harvest them off of publicly available web sites. Usually, if a user or administrator removes that email address from the web the spam typically tapers off.

Another method spammers use to obtain valid email addresses is to purchase a list of email addresses. There are companies in the marketplace that collect e-mail addresses and turn around and sell them. Users must be careful when you fill out forms on the web or enter sweepstakes. There is a good chance that they are agreeing to have their e-mail address be sold to a third party.

A third method of obtaining legitimate email addresses is to use brute force dictionary attacks. Spammers send the same message to all of the most common permutations of individuals' names and initials in email systems, and then weed out invalid addresses from the auto-response "undeliverable" messages sent by the recipient's mail system. Some naive email users utilize the opt-out link in their email to eliminate spam. This only serves to verify that it is a valid email address and could actually generate additional email.

Another technique that spammers are using is called "drive by spamming". Basically, they drive around looking for unsecured wireless connection that would give them access to a secured mail relay as well access to your internal network. By gaining access to the internal network spammers can use your SMTP server to spam the world since the mail would be coming from a legitimate e-mail client on the network.

Another technique used by spammers is to randomize e-mail content to increase "uniqueness", thus making it more difficult to establish effective filters. By slightly changing the subject line or the name of the executable file containing a virus, then that particular message will pass through your filter undetected.

What is it being done about spam?

It is obvious that everyone is tired of being spammed. Thirty-three states already have anti-spam legislation in effect [2]. Many countries have nationwide anti-spam laws. The United States of America currently has no federal anti-spam laws but several anti-spam bills have been introduced.

What is government doing about spam?

- **CAN-SPAM Act of 2003 (S. 877)**
  The "Controlling the Assault of Non-Solicited Pornography and Marketing" (CAN-SPAM) Act was reintroduced by Senators Sen. Conrad R. Burns (R-MT) and Ron Wyden (D-OR) in April 2003, with only minor changes from the previous year's version, S.630 (2002). The CAN-SPAM Act of 2003 would require unsolicited commercial e-mail messages to be labeled (though not necessarily by a standard method) and to include opt-out instructions and the sender's physical address. The law would prohibit the use of deceptive subject lines and false headers in such messages. It would pre-empt any state laws that prohibit unsolicited commercial e-mail, but would not affect the majority of state spam laws.
- **Computer Owner's Bill of Rights (S. 563)**
  S. 563, introduced in March 2003, would require the Federal Trade Commission to establish a "do-not-email" registry of addresses of persons and entities who do not wish to receive unsolicited commercial e-mail messages. The FTC would be empowered to impose civil penalties upon those who send unsolicited commercial e-mail to addresses listed on the registry.
- **Wireless Telephone Spam Protection Act (H.R. 122)**
  H.R. 122 addresses cellular phone spam. Introduced in January 2003, the bill would prohibit the use of wireless messaging systems to send unsolicited advertisements.
- Federal Trade Commission has created an e-mail address to be used by citizen's reporting spam. uce@ftc.org

ISP strategies and techniques

Some of the major ISPs are deploying smart filters that range from checking black lists servers to giving you the choice to receive mail only from people that you have in your address book. Hotmail already gives you this option, while AOL will have this feature available in their 9.0 version. Another major ISP, Earthlink uses a challenge response technique. Basically, if you are not in the recipient's

address book, you will automatically receive an e-mail message telling you that your message has been delivered to a “suspect email” folder and that to be delivered to the user he/she need to add you to their senders list. Here is an example of what the automated message you will get back. The actual address of the earthlink user has been changed.

> “This is an automatic reply to your email message to someuser@earthlink.net
>
> This email address is protected by EarthLink spamBlocker. Your email message has been redirected to a "suspect email" folder for someuser@earthlink.net. In order for your message to be moved to this recipient's Inbox, he or she must add your email address to a list of allowed senders.
>
> Click the link below to request that someuser@earthlink.net add you to this list.
>
> https://webmail.pas.earthlink.net/wam/addme?a=someuser@earthlink.net&id=19DjKp1c03NZFjX0 “

We of course can’t list all of the techniques that each ISP in the country is using to stop spam and spammers. But, as a system administrator in charge of the IT infrastructure at a small company, your duty is to educate your users and ask them not to respond to unsolicited e-mail [3].

What can system administrators do?

The primary role of an administrator in battling spam is to make sure that their systems are secure and that they are not improperly configured. Even though the issue of open relay systems has been addressed in the Sendmail program, Exchange servers and other popular mail servers, there are still lots of SMTP servers that are misconfigured or have not been upgraded to the latest version and are being used as relays. This is one of the errors that spammers exploit. They scan the network for such systems and use them to send out their unsolicited e-mail.

One way to address this SMTP security breach is to restrict access to the outgoing mail server. This can be done in several ways. One method is to verify that the computer is on your local network by making sure that the IP address used by the computer in question falls in the IP address range that was assigned to you.

The second method is to insist on a local domain return address. When you connect to your company's mail server for "example.com" it should only allow you to send mail that is from "userid@example.com". If you try to send from another account and have the return address of "username@anotherexample.com" your message will be rejected with the error of "relaying denied".

A third method is to restrict access to your outgoing SMTP server by asking your users to authenticate themselves. This will give you another layer of security to your server, by allowing your users to send e-mail from anywhere in the world and at the same time preventing spammers and unauthenticated people from using your resources.

The second most important role of an administrator is to educate their users about the effect of spam on their company. We have briefly talked about client-based and server-based filters. It is clear that the administrator would be involved in setting up the server-based filters that would either delete or reject unsolicited e-mail. Here is a table that explains the choices that are available to administrators as well as the benefits and disadvantages of each. [16]

Methods	Pros	Cons
Keyword Searches	Searches for specific text that identifies unwanted mail. Easily customizable	Labor-intensive to develop and maintain word lists. Easily circumvented by tricks such as alternate spellings or interspersing invisible code between letters.
Black Lists	Blocks mail from known spam sources Readily available pools of lists	May block harmless messages Needs constant updating and maintenance Some lists have aggressive definitions of spammers
White Lists	Guarantees delivery of known good addresses	List maintenance can be cumbersome
Hashes/Signatures	Blocks known spam Low rate of false positives	Time-sensitive Can be circumvented by randomization
Heuristics	Applies multiple detection tests Provides greater confidence in identifying spam messages	Tests must be regularly updated to adapt to new spam techniques

Reverse DNS Lookups	Phenomenally accurate	May block mail from innocent but misconfigured hosts
Header Analysis	Identifies headers that don't conform to RFC's, a strong indication of spam	Misconfigured hosts may be incorrectly tagged as spam
Bayesian Filtering	Phenomenally accurate Learns new spammer tactics automatically	Functions best with individual user settings Accuracy dramatically decreases when deployed as a generic gateway solution Requires more processing power than other solutions
Image Scanning	Filters out offensive images before a user sees them	Many legitimate e-mails include images

A small company might not have their own SMTP server, but they can use the above table as a guideline in choosing an ISP. This will give the chance to ask questions about what is the ISP doing about spam and which of the above techniques they are using to fight spam.

What can users do?

The best technique to combat spam is for the system administrator to educate his or her users. The administrator can do this by putting together an FAQ or even a quick checklist of what his or her users need to know about spam. A sample checklist and FAQ are available in Appendices A, B.

Users can make sure that their anti-virus definition file is current. Anti-virus software companies have made it so easy to have the file updated. They can make sure that their PCs are patched.

Conclusion

This paper has examined the problem of spam and surveyed techniques and vulnerabilities exploited by spammers. Spam is a problem because it is a drain on the financial as well as on systems resources of companies. Spammers use many different approaches from forging headers to using open mail relays to send out their unsolicited e-mails. Education and awareness of the users and administrators is the key to fighting spam. Legislation is being introduced in congress to help curb the effect of spam by making sure that spammers pay for

their crime. ISPs are also making sure that their systems are secure and are not widely open. Small companies would know what they are up against if they have to run their own SMTP server as well as know what to ask of the ISP that would be running an SMTP server on their behalf.

An FAQ is included in a form of an appendix to inform users about what they can do to fight unsolicited e-mail. The spam fighting techniques discussed are not one hundred percent effective, but at least they will minimize the effect of spam, and the effect of spam will be reduced in the long run with an educated user population.

References

1. "Standard for the format ARPA Internet Text Messages". RFC822 URL: http://www.ietf.org/rfc/rfc0822.txt?number=822
2. "How to end spam in the future." By Jane Weaver URL: http://www.msnbc.com/news/936568.asp
3. "Anti-Spam Configuration Control". By Eric Allman URL: http://www.sendmail.org/m4/anti_spam.html
4. cf/README file: URL: http://www.sendmail.org/8.12.9.html
5. "Asian govts slow to fight spam". By Teresa Leung http://www.asiacomputerweekly.com/acw_ViewArt.cfm?Magid=1&Artid=20380&Catid=3&subcat=29
6. "Look-alike e-mail scam on the rise" By Bob Sullivan URL: http://www.msnbc.com/news/941872.asp
7. "Why Spam could destroy the Internet". By David Berlind. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2897473,00.html
8. "Anti-Spam Quotes". URL: http://www.isode.com/solutions/anti-spam-quotes.html
9. "SoBig.F Fastest Spreading Computer Virus Ever". Associated Press. URL: http://www.foxnews.com/story/0,2933,95325,00.html
10. "CAN-SPAM Act of 2003 (S.877)". URL: http://www.spamlaws.com/federal/108s877.html
11. "Computer Owners' Bill of Rights" URL: http://www.spamlaws.com/federal/108s563.html
12. "Wireless Telephone Spam Protection Act (H.R 122)" URL: http://www.spamlaws.com/federal/108hr122.html
13. "Summary of Laws Introduced" URL: http://www.spamlaws.com/federal/summ108.html#hr122
14. "Much-feared Internet attack fizzles" URL: http://www.msnbc.com/news/955498.asp
15. "The secret tricks that spammers use" URL: http://www.msnbc.com/news/940853.asp?vts=081120031510
16. "The Pros and Cons of Common Spam-fighting Methods" Fighting the Spam Monster and Winning, Andrew Conry-Murray, Network Magazine, April 2003.

Appendix A: Spam Checklist

What Your Users Need to Know About Spam

1. Never reply to spam, because usually these are invalid.
2. Don't trust the opt-out or unsubscribe features included in spam messages, which will only confirm to the spammer that the responder's e-mail address is valid.
3. Don't post your e-mail address on websites, newsgroups, discussion groups, etc…
4. Don't provide your e-mail address without knowing how it will be used (e.g. online registration to access online resource, consider using a free email address available from Hotmail or Yahoo, which you can use specifically for that purpose)
5. Don't participate in Internet chain e-mails, since these are often used to harvest e-mail addresses.
6. Don't use your mail client's preview pane.
7. If you receive spam in your inbox, forward it to uce@ftc.gov (with all the mail headers intact).

Appendix B: Spam FAQ

1. **What is spam?**

   Spam is the term for unsolicited bulk e-mail. Spam is often sent to advertise dubious products, get-rich-quick schemes, pornographic web sites or quasi-legal services.

2. **Who are spammers?**

   Spammers are typically multilevel marketers promoting services like those mentioned above.

3. **How are they able to send spam?**

   Spammers search the internet to find e-mail servers that are inappropriately left open to relay e-mail messages. When they find these servers, they then send their e-mail through them.

4. **How do spammers get e-mail addresses?**

   Spammers harvest e-mail addresses from a number of sources, including Usenet postings, e-mail mailing lists and web sites.

5. **Who is vulnerable to receiving spam?**

   Just having an Internet e-mail address makes you susceptible to receiving spam.

6. **Why doesn't my e-mail address appear in the spam message's "To:" field?**

   Often spammers will address e-mail addresses using the Blind Carbon Copy (BCC) field. The contents of the BCC field are hidden from the recipient. It is quite probable that the spammer entered in that field either your e-mail address or that of an e-mail list to which you belong.

7. **How do I know if my e-mail server has an open relay that spammers might exploit?**

   You can use the following web site to test your e-mail server:

   http://www.abuse.net/relay.html

8. **What are blacklists and how do I get in one?**

Blacklists are lists of e-mail servers known to have been used by spammers. They are used by ISPs to deny connectivity to listed servers. E-mail servers on such lists are refused connectivity, preventing them from relaying more spam. This also blocks them from sending and receiving legitimate e-mail.

9. **How do I fix an open relay on my server?**

The Abuse.net web site has links on how to fix an open relay;
http://www.mail-abuse.org/tsi/ar-fix.html

10. **What can I do to avoid receiving spam?**

- **Use Filters**
  If your e-mail program allows it, use automatic filtering options to block "bulk senders" or move them to a separate mailbox. Hotmail, Yahoo and others do just that. Be careful, however, to check the list of senders you are blocking. It is easy for the automated filters to confuse a message from your spouse for one from a spammer.
- **Read Privacy Policies**
  When filling in an online form with your e-mail address, be sure to read the privacy policy of that site. You should be able to opt out of receiving "special offers" from their affiliated companies.
- **Just Hit Delete**
  If all else fails, just take a deep breath and hit that delete button. Sometimes it's faster and less aggravating to do so.

11. **Should I reply to spam, to be removed from the spammers' list?**

It's not clear at this point that remove requests are effective. Common opinion is that using these remove reply addresses will only make the problem worse for you by confirming for the spammer that your e-mail address is still valid. This too is hard to prove. It's likely you won't have much effect one way or the other by using them. Another option is to visit one of the many global opt out lists on the web. This too is controversial. Some assert that these opt out lists are merely schemes to harvest e-mail addresses. Your best choice would be for an opt-in rule instead.