Interested in learning more about security?

SANS Institute InfoSec Reading Room

The Growing Threats to Email Communications in 2004

Email has become a critical function for most businesses. As email has grown in popularity as a method of communication so have the variety and volume of threats. Viruses, worms and Spam (unsolicited commercial email) have developed over time along with email use. The number of threats to email has increased to epidemic levels in the 2004 despite the industries best efforts to keep them in check. This paper will attempt to show how the threats to email communications have been getting worse in 2004, some of the new met...

The Growing Threats to Email Communications in 2004
Scott Palmer
GSEC Practical (v.1.4b), Option 1
May 18th, 2004

Abstract

Email has become a critical function for most businesses. As email has grown in popularity as a method of communication so have the variety and volume of threats. Viruses, worms and Spam (unsolicited commercial email) have developed over time along with email use. The number of threats to email has increased to epidemic levels in the 2004 despite the industries best efforts to keep them in check.

This paper will attempt to show how the threats to email communications have been getting worse in 2004, some of the new methods and tactics utilized by these threats, what changes have occurred in how we react to these threats, and discuss some possibilities in defeating these threats.

Section 1: The threat is getting worse

Email viruses, worms and Spam can cause a great deal of damage to a business. These threats can use large quantities of disk space on email servers and in some cases run email servers out of space. They can saturate Internet connections by utilizing all available bandwidth. They can diminish employees' productivity by causing them to manage large amounts of irrelevant email. Finally, they can destroy data and cause costly cleanups.

The year 2004 to date has seen a tremendous volume of email worms. "[Trend Micro] said that the first quarter of 2004 saw the greatest number of virus alerts ever issued in a three-month period. Trend Micro during Q1 2004 issued 232 virus warnings, compared to a mere 35 issued by the company in Q1 2003." [1]

According to a WholeSecurity.com report, "Companies spent an average of $100,000 each cleaning up after widespread worms in 2003, according to ICSA Labs, a unit of security consulting firm TruSecure Corp. in Herndon, Virginia. That's up 23 percent from 2002." [2] Comparable estimated costs for cleanups for worm infections in 2004 are not available, but some figures on estimated total damages caused by the four major worms that have appeared in 2004 are:

MyDoom Worm -
The MyDoom worm appeared on January 26, 2004 and broke the infection volume records previously held by the SoBig.F worm that appeared in August

2003. “At its height, MyDoom.A accounted for 1 in 12 of all emails scanned.” [3] (MessageLabs) Mi2g Intelligence Unit, a digital risk analysis firm, estimated MyDoom's damages at $38 billion. [4]

Bagle Worm -
The Bagle worm (also known as Beagle) was discovered on January 18th, 2004. Figures on estimated damages for the Bagle worm were not available.

Netsky Worm -
The Netsky worm was discovered on February 16, 2004. Mi2g Intelligence Unit ranks the Netsky worm as the second worst malware since 1995 and estimates it damages between $35.8 billion and $43.8 billion. [5]

Sasser Worm -
The Sasser worm was discovered on April 30th, 2004. Mi2g Intelligence Unit ranks the Sasser worm as the fifth worst malware since 1995 and estimates its damages between $14.8 billion and $18.1 billion. [6]

These estimated costs of worm damages can be compared to a Trend Micro estimate that the overall cost of damages from malware in 2003 was $55 billion. [7] As you can see, the estimated cost of damages caused by worms for the first quarter of 2004 already are greater than the cost of damages from all malware for the entire year of 2003.

According to another mi2g Intelligence Unit report “Q1 results have shown DDoS (Digital Denial of Service Attacks) have caused $3.4bn - $4.1bn (US) damage - triple the damage for the whole of 2003 ($1.3bn - $1.6).” [8]

These estimated costs of damages from email worms in 2004 are astonishing. It should be mentioned that these figures are only estimates and are often disputed. One such website that disputes many of these damage calculations is http://www.vmyths.com.

If the volume of worm email threats to date in 2004 hasn’t been staggering enough, Spam volumes have also increased astronomically. “The volume of Spam sent out the first quarter of 2004 exceeded 1.6 trillion unsolicited messages, overtaking the 1.5 trillion sent throughout 2003.” [9]

Brightmail, an anti-Spam software vendor, lists the following percentages of email traffic that is Spam on their website:

May 2003	48%
June 2003	49%
July 2003	50%
August 2003	50%
September 2003	54%
October 2003	52%
November 2003	56%
December 2003	58%
January 2004	60%
February 2004	62%
March 2004	63%
April 2004 *	64%

* In April 2004, Brightmail filtered over 96 billion messages. [10]

As you can see from the statistics above, the percentage of email that is Spam has grown consistently and considerably from last year.

An interesting fact about the origin of Spam comes from an article by Robyn Greenspan: "...Brightmail's Probe Network found that 80 percent of Spam messages where in English, and Commtouch Inc. identified 60 percent of all Spam originating in the United States during the month of March [2004]...." [11]

Ferris Research estimates that Spam costs businesses more than $10 Billion in 2003. [12] Estimated damages from the Spam in 2004 were not available, but it's certain to be considerably more due to the fact that more Spam has been sent in the first quarter of 2004 than in the entire year of 2003.

As seen from statistics presented both the volume of and the damages caused by worms and Spam in just the first couple of months in 2004 have increased more than the totals for entire year of 2003. These statistics show that threats to email communication are growing at a massive and unchecked pace.

Section 2: New behaviors in threats

One of the main reasons for the increasing volume and success of viruses, worms and Spam in 2004 have been due to the tactics they've used. The following section will attempt to describe some of these methods. For most methods discussed, I will attempt to give examples from the four major worms that have appeared in 2004: MyDoom, Bagle, Netsky and Sasser. For further details on these worms please see the Resources section at the end of this paper.

Built-in SMTP engines

Although the first worms to include their own SMTP engines appeared before 2004, we've seen it become a standard for email propagating worms in 2004. By using its own SMTP engine, a worm can avoid the use of MAPI (Microsoft's Mail API). By avoiding MAPI, a worm can isolate itself from any email client configuration issues and integrated virus scanners that maybe present. The MyDoom, Bagle and Netsky worms all contain their own SMTP engines.

Social Engineering Tactics

The use of and reliance on social engineering in email worms is not a new development in 2004. However, we have seen the authors of worms in 2004 begin to improve on previously attempted tactics. The mission of an email propagated worm author is to get the recipient to open and execute the attachment. We've seen the following methods utilized heavily in 2004.

The first method of social engineering that worm authors use is the spoofing of an emails sender address. We've seen the MyDoom, Bagle and Netsky worms all spoof the sender address with a valid email address that's found on the infected computer. Another trick all worm authors have used is to make the email appear as if it is coming from someone within the recipient's own domain. Many times the sender address is made to appear as though the email was sent from someone in the administration, management or IT departments of the recipient's company or service provider. By utilizing common role names in the sender email address the recipient may be fooled. These tactics are often successful and can lead to many issues for helpdesks as users don't understand that the sender address is spoofed.

The next method of social engineering that worm authors are using is dealing with the subject and body of the message. The MyDoom, Bagle and Netsky worms have all made heavy use of making the subjects of emails appear as they are replies to a previous message the recipient sent. Subjects containing "Re: Hello>, "Re: your details", or "Re: Re: Re:" are very common sent from these worms. Another use of the subject and body of a message is to make the email appear as though it encountered an email system problem and include text containing technical terms that appears to be system generated. The MyDoom worm made heavy use of this tactic to much success. A technique used by the Netsky worm was to make its email appear to come from an anti-virus software vendor with a professional reading text that included an attachment claiming to be a definition update but actually contained the worm. Another notable tactic used by the Netsky worm was to make an email appear as though it came from the recipient's email account provider and that the recipient's email account was about to be deactivated or deleted unless they opened the attachment. The Bagle worm used a couple of interesting tactics. One was to make an email appear as an incoming fax from an automated facsimile to email gateway. This tactic was clearly targeting business users. Another interesting method the Bagle worm tried was to make an email appear to come from a dating service or

sex chat forum. The attachment in the email lead recipient to believe it was a picture of the women who sent the email. This approach is perhaps a little more embarrassing for the victim than the usual worm infection.

The final method of social engineering that worm authors use is the names and icons of attachments. In most cases, the attachment containing the worm needs to be executed by the recipient. Many users are aware that they should avoid opening files with names ending with the commonly known executable extensions so they must be tricked into it. In many cases worms will try to make the attachment filename fit with the subject and body of the email message. Attachment names such as "Your_document.doc", "readme.txt", "message.txt" and "file.xls" are often used with ".PIF", ".SCR", ".EXE", ".CMD" or ".BAT" as second extensions and some users are fooled. The Bagle worm would use icons of text files, folders and Excel files for executables in hopes a user would not examine the extension of the filename closely and open the attachment. The Netsky worm used two very interesting tactics. The first was that the worm would use the two extension filename trick but place 100 spaces between the extensions. Almost all programs don't display the whole filename so the user would see "file.txt…" instead of "file.txt<100 spaces>.exe". The second method the Netsky worm used was make a ".COM" (DOS command file) appear as though it was a link to a website with a domain name ending in ".com."

As you can see from the examples given, worm authors have started to hone their social engineer skills. Educating users to these tactics is often done reactively. In order to curb the success of worms using these techniques we must get users to behave proactively (perhaps to the point of paranoia?) and always question if an email is authentic.

DDOS against websites

Distributed denial of service attacks have become a stock feature in worms in 2004. The MyDoom worm first targeted www.sco.com for a DDOS attack. MyDoom in later variants added www.riaa.com, www.microsoft.com and www.symantec.com as targets. The Netsky worm targets www.kazaa.com and other peer to peer file sharing networks. These worm authors most likely think they are making some sort of a statement by targeting company websites, and we can expect this trend to continue as long as they are successful in temporarily shutting down some.

ZIP attachments with password protection

All three of the MyDoom, Bagle and Netsky worms use zip archives to help hide their attachments. The Bagle worm took this approach one step further by password protecting the zip archive that it sent its executable code in. The earlier variants of the Bagle worm included the password in plain text in the body of the message hoping the recipient would be unaccustomed to receiving protected zip archives and curious enough to open it and execute its contents. Later variants of Bagle included the password in a bitmap file which may appear

more legitimate to some users. Many virus scanners are not able to open password protected zip archives allowing the Bagle worm make it into some email servers.

Disabling antivirus and firewall software

A very interesting trend in 2004 is that worms actively try to disable antivirus and firewall software. The MyDoom, Bagle and Netsky worms all have long lists of common process names of the major security companies' products that they attempt to kill when the worm loads. A suggestion on how to address this issue will be made in the last section of this paper. An interesting side note is that the authors of the Bagle and Netsky worms have engaged in a competition were they are actively uninstalling other worms when they infect a computer. Within the code of their worms, the authors include taunts to each other.

Blocking access to antivirus and Microsoft websites (host file)

The MyDoom (B variant) uses an interesting tactic of overwriting the host file of an infected computer in order to prevent access to many antivirus vendor and Microsoft websites. This purpose of this is to obviously prevent users from gaining access to software to remove the worm. The modified host file is easily fixed, but it requires knowledge that most novice users do not have. One easy method to prevent tampering with the host file is to make the file read only.

Making worm executable filenames to look like part of Operating system or AV software.

A tactic that MyDoom, Bagle, Netsky and Sasser all try is to attempt to make their worm files and processes appear as though they are important parts of the operating system or security products. MyDoom started off with the name "taskmon.exe" for its worm. Later variants used the filenames "Explorer.exe", "Svhost.exe" and then random filenames. Bagle started off with "Au,exe" then moved toward the more "operating system" sounding names "Winsys.exe", "Winupd.exe", "Directs.exe", "Drvsys.exe" and "Drvdll.exe". Netsky started with a filename "Services.exe" and then moved onto "Winlogon.exe", "SysmonXP.exe", "Svchost.exe", "AVGaurd.exe", "FVProtect.exe", "EasyAV.exe", "SymAV.exe", "FirewallSvr.exe" and "Csrss.exe". An interesting side note is that the Netsky author(s) within their code refer to themselves as antivirus writers because in the competition with other worm authors they disable the worms and back doors of MyDoom, Bagle, and MiMail. It would seem logical that they use a filename to denote their worm is an antivirus program. All of these worms place their code in the %Windir% or %System% directories. Often worms will use filenames of actual operating system files whose real instances are located in different directories. These tactics in file naming make it very difficult for novice and intermediate users to spot these worms' files or process names.

Spreading through peer to peer file sharing networks.

Mydoom, Bagle and Netsky all try to propagate through peer to peer file share networks. The MyDoom worm actively looks for Kazaa. The Bagle worm tries to

replicate through the Kazaa and IMesh networks. The Netsky worm attempts to copy an executable containing its worm to any directory with "Shar" in the filename. This directory name target is one which is commonly used for the upload directory for various peer to peer file sharing clients. All of these worms attempt to name executables containing itself to appear as crack programs, pirated software or pornographic material. It should go without saying that unless you absolutely need to use file sharing services, they are best avoided from a security standpoint.

Masquerading as a patch

An interesting approach that some worms use is to attempt to fool the recipient into thinking that they are a patch for the operating system. The Sober.D worm tried to make the receiver believe it was a patch from Microsoft for the MyDoom worm. This tactic concerned Microsoft enough that they started a campaign to notify users they do not email patches. One of the last variants of the Netsky worm attempts to make the recipient believe that it was sent from an antivirus vendor and the attachment was a removal executable for a previous variant of itself, the Sasser, the Bagle, the MyDoom or the Blaster worm. The obvious way to avoid these types of schemes is to always go to the company website of a product to get an update.

Attacking known system vulnerabilities

The practice of worms attacking known system vulnerability is not new to 2004. The list of worms that have successfully exploited known vulnerabilities is extremely long. A few examples that reached extremely large infection rates are CodeRed, CodeRed II and Nimda. In 2004 this tactic is alive and well. Both a later variant of Netsky and the Sasser worms make use of Microsoft vulnerabilities for which patches have been available for some time. There is simply no substitute for staying current with operating system security updates and patches. These worms simply reinforce this concept.

Code sharing / Worm writing groups

A disturbing issue when considering the threats to email communication is that of people sharing code for email worms on the Internet.

"Symantec has reported finding found more than 38,000 Web sites containing source code for viruses and worms. In most instances, authorities are able to shut the sites down, but analysts also think that source code is transferred over the Internet in ways that are more difficult to trace. Virus and worm writers use small mailing lists, chat rooms and instant-messaging programs, as well as file-sharing networks such as Kazaa." [13]

There are USENET news groups dedicated to discussing virus code (ALT.COMP.VIRUS.SOURCE.CODE). A quick check of the newsgroup did not produce any code, but there were several individuals asking for either examples or the entire code for specific worms. This is a disturbing situation due to the ease of making small changes to the code of an existing worm so that current virus definitions will not detect it. Another issue is that of the worm writing group.

It appears that there were several individuals involved in writing and releasing the Netsky and Sasser worms. [14] This is a frightening fact. Multiple people working together in releasing a virus or a worm could cause much higher initial infections rates than we've seen to date. Hopefully law enforcement will continue to make headway against the individuals committing the crimes of writing these worms and viruses.

Backdoors

In 2004, we've seen all four major worms MyDoom, Bagle, Netsky and Sasser create backdoors into systems they've infected. These backdoors allow attackers to execute code on the infected computer and transfer data and executables to and from infected computers. Some of these worms use the backdoors to update their own code. These backdoors are very dangerous and not only expose the entire contents of the machine infected but the entire network that computer is connected to. One good way of combating this problem is by using Egress filtering so that traffic on the ports these backdoors are using is not allowed to reach back to the Internet. Another method of combating these backdoors is to make sure your computer is protected with good antivirus software and its definitions are up to date.

Spammer methods

To my knowledge, tactics used by Spammers have not changed much in 2004. The main reason for this is that they have not needed to change because their current methods are working just fine. There are several excellent papers in the SANS reading room on the techniques Spammers use. Please see the Resources section at the end of this paper for links. An interesting trend that a MX Logic news article mentions is that nearly 50% of all Spam email use Webbugs to validate recipient addresses when opened. [15] This practice allows Spammers not only to target addresses they have confirmed are "live" with more Spam but to also sell those addresses to other Spammers.

Section 3: Changes in responding to threats

Due to the shear volume of email worms and Spam that have laid siege to business systems in 2004, there have been several noticeable changes to how the industry is responding to these threats.

More frequent virus definition updates

Most antivirus software vendors make planned releases of updates to their virus definitions once a week. In 2004 due to the vast number of high threat level worms we've seen numerous occasions were antivirus vendors have been forced to make multiple releases of updated definitions in the same day. This puts a very heavy burden on IT staffs and the antivirus vendors. The threat of email worms has become so large that it has become mandatory that an IT Staff have someone on call to update antivirus definitions in the event of a major outbreak. Another issue is that the heuristics included in most antivirus software packages

do not seem to be working very well at catching new worm variants. Hopefully there will be some advances in these heuristics in the near future to make them more useful.

No longer try to clean infected files

A noticeable change due to the high volume of email worms in 2004 is that it is no longer considered best practice to attempt to clean a virus infected email with your antivirus software. The contents of a worm sent email are worthless. By trying to remove the worm attachment from an email and send it to the intended recipient you are simply clogging their email inbox with messages that are worth less than Spam.

No longer send virus found notification

The default behavior of most antivirus software is to send notification to the sender and receiver of the email that a virus was found in the message. Due to the overwhelming use of sender email address spoofing by worms this practice had to be discontinued. Sending notifications to email addresses that did not originate the offending email adds to the problem. Unfortunately not everyone has quite realized this fact yet and in some cases it has become necessary to treat antivirus notifications as Spam and set filters up to catch them. There is some hope that this problem will be solved by the antivirus software vendors. According to a Silicon.com article, Symantec has stopped the practice of sending virus notifications and other vendors will soon follow suit. [16]

Spam keyword and attachment filters used to block worms

An interesting technique I've used in blocking email worms is to use keyword filters in my Spam blocking software to catch some of the more popular subjects and attachment names worms use. Care must be taken not to introduce false positives depending on the nature of the email your business receives. Also, limiting attachment types in emails to allow only those document types your business uses is a good idea. Refusing to accept Zip archives as email attachments seems to be a rising trend due to the popularity of worms utilizing them, but this decision should be made carefully because of the wide spread use of Zip archives in business settings.

Bounties

In 2003 we saw Microsoft set up a reward program to pay individuals for information leading to the arrest of the authors of viruses and worms. Currently in 2004, Microsoft is offering bounties for information on the authors of the SoBig, Blaster and MyDoom worms. After MyDoom's DDOS attacks on www.sco.com, SCO also offered a $250,000.00 bounty for the author of the MyDoom worm. This quote explains Microsoft motivation in offering these bounties: "This bounty was meant to tear apart the virus writing communities and destroy mutual trust and the 'honour among thieves' culture which leads to collaboration and an impenetrable safe-house society that rallies around to protect its members' identities and whereabouts. " [17] In May of 2004 it appears

that this approach of bounties is paying off. The author of the Agobot (also know as Gaobot) worm has been apprehended as well as one of the authors of the Netsky and Sasser worms.

SURBLs

One interesting method of blocking Spam is the use of a SURBL or Spam URI Real-time Blocklist. This is a blacklist for domain names that appear in the message body of an email. This list can contain email domain names and websites of known Spammers. This helps alleviate the problem of Spammers spoofing their sender address. Please see the list of resources at the end of this paper for more details.

Section 4: Conclusions: Is it hopeless?

I've tried to show in the previous sections how severe the threats to email communication have become in 2004 and how the industry has started to react. In this section I will discuss and give my opinion on some approaches that are currently being developed to counteract these threats.

Can legislation stop Spam?

The CAN-SPAM act was signed into law in late 2003 and went into effect January 1st 2004. As seen in section 1, the volume of Spam has continued to grow throughout 2004. According to a Pew Internet & American Life Project report, "29% of email users say they have reduced their overall use of email because of spam." [18] However there maybe some hope, a MX Logic report states that "12 percent of senders of unsolicited commercial email are making efforts to comply with components of The Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act." [19]

The same MX Logic report continues to say that "Unsolicited commercial email that is wholly compliant with the law remains at 3 percent, representing no change in month-to-month compliance since the law went into effect on Jan. 1." [19] Perhaps when the FTC takes some Spammers to court the situation will improve. However, Spammers will have the option of moving their operations to foreign locations where the CAN-SPAM act does not apply and they can still target the same email addresses.

User education

There is a crisis in user education right now in dealing with the various email threats. Much more must be done by employers and by antivirus/antispam vendors to educate users on how worms and spam work. Appropriate training should be given to employees to spot social engineering tactics. Education is a life-long process and the IT Industry will have to do its best to keep users educated about security threats as they develop. I have included two interesting articles with different conclusions on worm victim responsibility in the Resources section of this paper.

SMTP Authentication

A technology that offers a lot of hope in combating the worm and Spam threats to email communication is SMTP Authentication. It is possible that a system based on some of the current proposed models could help put and end to sender address spoofing. Currently there are numerous competing standards and politics are deeply involved in the process. Unfortunately for a SMTP Authentication system to work, wide scale adoption will have to take place. Adoption will require updates to email server software. Most likely this is a longer term solution (will mostly likely take years to implement) to the email threat problem, but it does give hope.

Best practice for handling threats to email

Until some of the previously mentioned solutions are realized, the best way to combat the threat of viruses, worms and spam to email is through a multi-vendor antivirus and antispam software approach. It is a very good idea to perform edge or gateway scanning of email before it reaches your email server. It's preferable that you then use a different antivirus vendor's solution on your email server and on your clients. This should help limit the risk of one vendor being slow with definition updates. The use of gateway scanning can also help cut costs if your business must comply with email retention regulations. By refusing worms and Spam at the gateway before it reaches your email server you avoid the storage costs of retaining it.

Another excellent method to help reduce risks of viruses and worms to limit the security rights of users accounts that are used on a daily basis. Most viruses and worms attempt to modify the Windows registry and systems files that require high levels of access. The attempts by several worms to terminate processes of antivirus and firewall software can be thwarted by using proper security rights. By exercising a policy of least security rights given to perform a function, the damage most viruses and worms attempt to cause can be limited or even prevented. This practice is almost mandatory in a business environment and advisable in a home environment.

Hopefully this paper has shown the severity of the growing threats to email communication, some of the new methods these threats use and some of the new responds to these threats.

References

1. Chandrasena, Nirmal. “Virus alerts reach record levels” 5 April 2004. URL: http://www.itnews.com.au/ibmstorycontent.asp?ID=10&Art_ID=19041
2. “Economic Impact of Worms” URL: http://www.wholesecurity.com/threat/cost_of_worms.html
3. “January Monthly Report” URL: http://www.messagelabs.com/intelligence/reports/monthlies/january04/default.asp
4. Varghese, Sam. “MyDoom damage estimate termed absurd” 6 February 2004. URL: http://www.theage.com.au/articles/2004/02/06/1075854035648.html
5. “NetSky climbs to 2nd worst malware since 1995; Big Three malware cause record productivity losses in Q1 2004” News Alerts Section. 30 March 2004. URL: http://www.mi2g.net
6. “Sasser's colossal damage makes it 5th worst malware of all time” News Alert 10 May 2004. URL: http://www.mi2g.net
7. “Virus damage estimated at $55 billion in 2003: And it will just get worse this year, anti-virus firm says” 16 January 2004. URL: http://msnbc.msn.com/id/3979687/
8. Myers, Tracey. “2004 Q1 Malware total surpasses 2003” 3 April 2004. URL: http://www.net4nowt.com/isp_news/news_article.asp?News_ID=1950
9. Kapica, Jack. “Computer virus damage shatters records” 2 April 2004. URL: http://www.globetechnology.com/servlet/story/RTGAM.20040402.gtjackvirusapr2/BNStory/Technology/
10. “Spam Statistics” URL: http://www.brightmail.com/spamstats.html
11. Greenspan, Robyn. “Deadly Duo: Spam and Viruses, March 2004” 8 April 2004. URL: http://www.clickz.com/stats/big_picture/applications/article.php/3337751
12. “Research Focus: Spam” URL: http://www.ferris.com/offer/spam.html
13. Lemke, Tim. “Virus creators share code online to create copycats” 17 March 2004. URL: http://washingtontimes.com/business/20040316-093754-4080r.htm
14. “Police breaking open Skynet virus gang in North Germany, Sophos reports” 13 May 2004. URL: http://www.sophos.com/virusinfo/articles/skynetgang.html
15. “MX Logic finds nearly 50 percent of all Spam is bugged by Spammers, allowing them to validate addresses and send more Spam” 13 April 2004. URL: http://www.mxlogic.com/news_events/04_13_04.html
16. Sturgeon, Will. “Symatec stops frustrating virus-notification alerts” 11 May 2004. URL: http://software.silicon.com/security/0,39024655,39120602,00.htm
17. “Leader: Microsoft bounty pays dividends” 10 May 2004. URL: http://software.silicon.com/security/0,39024655,39120565,00.htm
18. Rainie, Lee and Fallows, Deborah. “PEW Internet Project Data Memo

RE: The impact of CAN-SPAM legislation" March 2004. URL: http://www.pewinternet.org/reports/pdfs/PIP_Data_Memo_on_Spam.pdf
19. "MX Logic sees unsolicited commercial email senders making some efforts to comply with CAN-SPAM act." 5 May 2004. URL: http://www.mxlogic.com/news_events/May.CAN-SPAM.html

Resources

Here are sources information on topics discussed in this paper. Although these sources are not referenced in this paper, they are included if the reader desires further information.

GIAC GSEC Practicals on Spam

1. El-Khoury, Nadim. "Controlling Spam in a Small Business" August 30, 2003
2. LeBlanc, Charlene. "Slipper Slope or Terra Firma? Current and Future Anti-Spam Measures" June 20, 2003

Websites to Research Virus and Worms

1. Symantec AV Center URL: http://www.symantec.com/avcenter/
2. Network Associates / McAfee Virus Information Library URL: http://vil.nai.com/vil/default.asp
3. Trend Micro Virus Information URL: http://www.trendmicro.com/vinfo/
4. Sophos URL: http://www.sophos.com

User Education

1. Mossberg, Walter S. "PC Users Deserve A Free, Simple Service To Handle All Threats" March 11, 2004 URL: http://ptech.wsj.com/archive/ptech-20040311.html
2. Mullen, Tim. "Stop Being a Victim" April 27,2004 URL: http://www.securityfocus.com/columnists/236

Spam URI Realtime Block List

1. http://www.surbl.org

General Security News

1. SecurityFocus URL: http://www.securityfocus.com
2. eWeek Security URL: http://www.eweek.com/category2/0,1738,1237860,00.asp

Last Updated: December 11th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Dubai 2018	Dubai, AE	Jan 27, 2018 - Feb 01, 2018	Live Event
SANS Las Vegas 2018	Las Vegas, NVUS	Jan 28, 2018 - Feb 02, 2018	Live Event
SANS Miami 2018	Miami, FLUS	Jan 29, 2018 - Feb 03, 2018	Live Event
Cyber Threat Intelligence Summit & Training 2018	Bethesda, MDUS	Jan 29, 2018 - Feb 05, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZUS	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS London February 2018	London, GB	Feb 05, 2018 - Feb 10, 2018	Live Event
SANS Southern California- Anaheim 2018	Anaheim, CAUS	Feb 12, 2018 - Feb 17, 2018	Live Event
SANS Secure India 2018	Bangalore, IN	Feb 12, 2018 - Feb 17, 2018	Live Event
Cloud Security Summit & Training 2018	San Diego, CAUS	Feb 19, 2018 - Feb 26, 2018	Live Event
SANS Dallas 2018	Dallas, TXUS	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Brussels February 2018	Brussels, BE	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, JP	Feb 19, 2018 - Mar 03, 2018	Live Event
SANS New York City Winter 2018	New York, NYUS	Feb 26, 2018 - Mar 03, 2018	Live Event
CyberThreat Summit 2018	London, GB	Feb 27, 2018 - Feb 28, 2018	Live Event
SANS London March 2018	London, GB	Mar 05, 2018 - Mar 10, 2018	Live Event
SANS Cyber Defense Initiative 2017	OnlineDCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced