Interested in learning more about security?

SANS Institute InfoSec Reading Room

SPAM and Anti-Spam

The SPAM battlefield is in a constant state of flux. As better weapons are built on the defense side, spammers are constantly building better weapons to overcome these measures on the offensive side. By becoming and staying informed, about the offensive and defensive weapons of both spammers and anti-spammers, we can prepare ourselves and our organizations to take direct measures to reduce the proliferation of SPAM. Finally, by understanding the elements that define what a spam message is and the tactics that are use...

SPAM and Anti-Spam

GSEC Gold Certification

Author: T. Brian Granier, briang at zebec dot net

Adviser: Jim Purcell

Accepted: October 27th 2006

Outline

1. Abstract

This paper discusses many issues related to SPAM and Anti-spam. A basic definition is provided that leads in to the motivations for sending SPAM messages. Legal issues related to SPAM in the United States are covered as well as a few example court cases. This is followed by discussing the "battlefield" on which the SPAM vs. Anti-Spam war is fought and the respective weapons in the arsenal for either side of the battle are discussed in detail. Finally, tips for organizations wishing to send mass emails who want to retain legitimacy and avoid being classified as a Spammer are provided.

2. Defining "SPAM"

Providing a succinct definition for the term "spam" that all IT professionals can agree with is not an easy task. To a large extent this is due to an ever changing environment where a definition good today will not be complete tomorrow. Nonetheless, an attempt will be made to discuss an early definition for the term and then to discuss a more thorough definition that is used as the starting point for this paper.

Why do we call it SPAM?

Before we go much further, here's a quick nod to the origination of the term SPAM that is now a common part of our technical vocabulary. As many of us know, SPAM is the name of a product created by Hormel Foods Corporation. This canned meat product was used in a Monty Python sketch that featured a room full of Vikings in a restaurant whose principle ingredient was, you guessed it, SPAM. As the skit goes, every time the word "SPAM" is mentioned a certain number of times, the entire room full of Vikings would break out into chorus spewing the word spam over and over again. This constant repetition of the word in the skit was compared to the quantity and repetition of what we now call SPAM and a new term was born.

Dictionary Definition

It is difficult to identify one specific dictionary definition with universal acceptance. However, the following definition was taken from http://www.dictionary.com as an example of the type of definition that is common for the word spam:

spam Pronunciation Key (spăm)

n.

Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail.

tr.v. **spammed, spam·ming, spams**

1. To send unsolicited e-mail to.
2. To send (a message) indiscriminately to multiple mailing lists, individuals, or newsgroups.

Unfortunately, the "dictionary definition" is often less than adequate at encompassing all aspects of what spam is. A slightly more thorough definition found at http://www.wikipedia.org reads as follows:

Spamming is the abuse of electronic messaging systems to send unsolicited, bulk messages. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, and mobile phone messaging spam.

This is a more usable definition, but it still misses the mark on discussing a few of the aspects that we will cover in this paper. For clarification sake, the following section offers an operational definition that will define the scope of the term "SPAM" used from here forward.

Practical Definition

As correctly pointed out by the Wikipedia definition, spam can refer to messages sent in any electronic format. However, for purpose of this paper, we will focus on narrowing down the term SPAM to discuss issues related to messages sent via email. Further, this paper uses a highly ambiguous definition that is subject to interpretation and could be the source of heavy debate. However, this paper is not about clarifying the ambiguities of the term, so the following definition is presented for consideration with respect to this paper:

> **Spam is any marketing, deceptive or abusive use of email that the recipient does not wish to receive.**

DISCLAIMER: As mentioned above, this definition is not meant as an accurate and complete definition for the term SPAM. It is just the one used for purposes of this paper.

3. Motivations for SPAM

Ultimately there are many motivations for SPAM. In many cases, papers or reports on this topic suggest that all SPAM has money as its root motivation. However, this stance implies that spam is only unsolicited marketing based emails that will lead to direct or indirect financial profit. As the definition we're using here includes abusive or deceptive emails as well, which often have nothing to do with money; we must consider more motivations than just financial. Once we understand the motivations of the spammer, we are in a better position to choose our weapons to defeat them.

Makes lots of money

Regardless of the disclaimer posted in the opening paragraph for this section, money really is the largest motivator for SPAM.

Direct Marketing and Sales

A common misconception about spammers is that they are marketing products that they directly sale and this blitz marketing technique is how they make their money by trying to reach a larger market share and sell their own product. While this does happen, this is actually very rare. A large number of articles exist making this point clear, but just to provide a few:

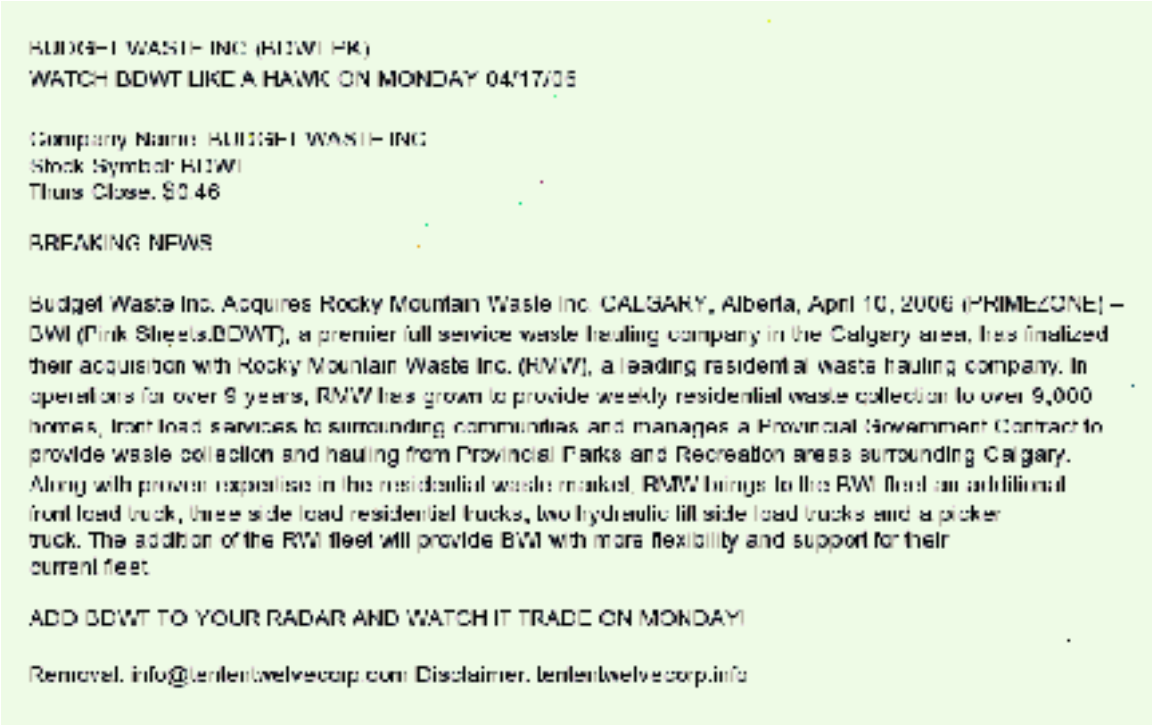
- http://www.techdirt.com/articles/20030804/0239218.shtml
- http://ask.yahoo.com/20050103.html
- http://cc.uoregon.edu/cnews/summer2003/spameconomics.html

Odds are high that if a SPAM message is on the surface advertising the product, the spammer was either paid by the maker of the product to send the solicitation or that there is some indirect ulterior motive, such as causing a banner ad to appear for which the spammer gets paid as a "hit".

Stock Market Game

There seems to be some clues that suggest there is a possibility that spammers are trying to play the stock market. This technique is often called "pump and dump". Specifically, a recent observance was seen by a group known as TenTenTwelveCorp that sent a large number of emails advertising valid stock on the US Stock Exchange. Interestingly, these messages do not provide any details about how these stocks can be purchased through the spammer in such a way that they would directly profit. The apparent goal seems to be actually to affect the stock price for certain stocks with the theoretical goal of the spammer profiting from the sale. These does seem a little far-fetched as the face-value of these spam messages could very well have a different purpose (described in one of the other motivations), but this type of spam has been in the increase. Review the following sites for more information:

- http://www.psychpage.com/spammer.html
- http://www.aubreyturner.org/index.php?/orglog/comments/1377/
- http://home.versanet.de/~pdietrich/spam-block.html
- http://www.npr.org/templates/story/story.php?storyId=5711560&ft=1&f=2



BUDGET WASTE INC (BDWT-PK)
WATCH BDWT LIKE A HAWK ON MONDAY 04/17/06

Company Name: BUDGET WASTE INC
Stock Symbol: BDWT
Thurs Close: $0.46

BREAKING NEWS

Budget Waste Inc. Acquires Rocky Mountain Waste Inc. CALGARY, Alberta, April 10, 2006 (PRIMEZONE) – BWI (Pink Sheets:BDWT), a premier full service waste hauling company in the Calgary area, has finalized their acquisition with Rocky Mountain Waste Inc. (RMW), a leading residential waste hauling company. In operations for over 9 years, RMW has grown to provide weekly residential waste collection to over 9,000 homes, front load services to surrounding communities and manages a Provincial Government Contract to provide waste collection and hauling from Provincial Parks and Recreation areas surrounding Calgary. Along with proven expertise in the residential waste market, RMW brings to the BWI fleet an additional front load truck, three side load residential trucks, two hydraulic lift side load trucks and a picker truck. The addition of the RW fleet will provide BWI with more flexibility and support for their current fleet.

ADD BDWT TO YOUR RADAR AND WATCH IT TRADE ON MONDAY!

Removal: info@tententwelvecorp.com Disclaimer: tententwelvecorp.info

Figure 1 - TenTenTwelve Stock based SPAM

Multi-level marketing (MLM) or Make Money Fast (MMF)

MLM is an acronym that is known to mean, "Multi-level marketing" or sometimes "Make lots of money". The biggest characteristic of an illegitimate MLM program is that they will usually promise to make you rich quick. They report themselves to be setup in a pyramid infrastructure such that individuals who have been in the program the longest will tend to make more money because they will have more people in the program below them from whom they get a cut. In order for the program to work, there is usually some sort of a product that has to be sold to end consumers and you have to try and sign up additional people to be salesmen under

you. Historically, this type of model became well known and successful by Amway who won a lawsuit posed by the Federal Trade Commission (FTC) that paved the way for other companies to use this model.

Unfortunately, with the coming of the Internet, MLM schemes have become widely spread and have gained quite a reputation for being associated with illegitimate business practices. A good portion of SPAM is advertising an MLM program that really is not a legitimate business. These programs are really only designed to make the creator of the program rich and no one else. The red flags about these scams are as follows:

- Offer to make lots of money at an unbelievable rate. If it sounds too good to be true it probably is.
- If there is a significant capital investment just to get signed up, then the real money maker is probably just the sign up fee.
- If you can't really get any information about what the actual "product" being sold is, then there probably is not one.
- The "product" being sold is overpriced. An overpriced product won't sell and the real goal is probably to get you to pay the signup fee.
- The offer to join the program was unsolicited, such as through email. Most legitimate MLM programs will involve a face to face meeting with the person trying to sign you up for the program

Make money fast (MMF) scams are similar in nature, but will emphasize the speed at which money is made and will typically lack the pyramid scheme setup.

As a general rule, any MLM/MMF advertisement coming through email has an extremely high probability of being illegitimate and probably even illegal. A good resource that discusses these and other red flags can be found at: http://www.mlmstartup.com/articles/b24ho.htm.

As sample make money fast example can be seen on the next page.

Date: Wed, 26 Jul 2006 12:52:07 +0700
From: Rose Household Textiles LTD
<rosehouseholdtextilesltd@rosehouseholdtextilesltd.co.uk>
Reply-To: parttimejoboffer@hotmail.com
To:
Subject: PART TIME JOB OFFER

Dear Sir/Madam,
Rose Household Textiles LTD is a UK textile company A subsidiary of (A Division of Actexotextile INC) in HongKong We produce and distribute clothing materials such as batiks,assorted fabrics and traditional costume worldwide. We have reached big sales volume of textile materials in the Europe and now are trying to penetrate the US market. Quite soon we will open representative offices or authorized sales centers in the US and CANADA and therefore we are currently looking for people who will assist us in establishing a new distribution network there. The fact is that despite the US market is new to us we already have regular clients also speaks for itself.
WHAT YOU NEED TO DO FOR US?
The international money transfer tax for legal entities (companies) in UK is 25%, whereas for the individual it is only 7%.There is no sense for us to work this way, while tax for international money transfer made by a private individual is 7% .That's why we need you! We need agents to receive payment for our textiles(in certified money orders, certified cashier's check and to resend the money to us via Money Gram or Western Union Money Transfer. This way we will save money because of tax decreasing. JOB DESCRIPTION?
1. Recieve payment from Clients
2. Cash Payments at your Bank
3. Deduct 10% which will be your percentage/pay on Payment processed.
4. Forward balance after deduction of percentage/pay to any of the offices you will be contacted to send payment to(Payment is to forwarded either by Money Gram or Western Union Money Transfer).

HOW MUCH WILL YOU EARN?
10% from each operation! For instance: you receive 7000 USD via checks or money orders on our behalf. You will cash the money and keep $700 (10% from $7000) for yourself! At the beginning your commission will equal 10%, though later it will increase up to 12%!

ADVANTAGES
You do not have to go out as you will work as an independent contractor right from your home office. Your job is absolutely legal. You can earn up to $3000-4000 monthly depending on time you will spend for this job. You do not need any capital to start. You can do the Work easily without leaving or affecting your present Job.The employees who make efforts and work hard have a strong possibility to become managers.
Anyway our employees never leave us due to our excellent work condition.

MAIN REQUIREMENTS
18 years or older legally capable responsible ready to work 3-4 hours per week. With PC knowledge e-mail and internet experience (minimal) And please know that Everything is absolutely legal, that's why You have to fill a contract! If you are interested in our offer, please respond with the following details in order for us to reach you:
NAME:
CONTACT ADDRESS:
PHONE NUMBERS:
AGE:
SEX:
OCCUPATION :
MARITAL STATUS:
Thanks for your anticipated action.And we hope to hear back from you. So if interested kindly reply to my personal email and i will get back to you immediately. I believe If we love the Lord we will obey His Word.And God bless us as you get back to me as soon as you are interetsed in working with my company. Stay blessed, for further inquires.
Micholas Ones
CEO Rose Household Textiles LTD.
Rose Household Textiles LTD. 37 PECKHAM HIGH STREET, LONDON, SE1 5SW, UNITED KINGDOM

Figure 2 - MLM/MMF Scam

Nigeria Scam

The "Nigeria scam" gets its own category because it's was really the first of its kind to become well known. This scam is also known as a "419 fraud" after the criminal code in Nigeria that it violates, which is where this type of fraud famously began. To make a long story short, this scan will usually come in the form of an email from someone presenting themselves as being from a foreign country. They will have some story about how they have access to a large sum of money that they need to transfer out of the country to a bank account. This individual will provide some method of contact to get back in touch with them via a fax number or an email address or some other means of communication along with a compelling reason not to involve law enforcement. After initial contact is made, the scammer will attempt lead the victim down a path that will ultimately result in the victim providing a "startup" amount of capital reportedly used to start the process of releasing the large sum of money or to bribe appropriate officials or to open up a bank account in which the money is to be transferred. If the victim is particularly gullible, it is possible that they will need more and more money due to needing to cut more red tape or bribe more officials over time until they have depleted the gullibility of the victim. Once it is clear there is no more money to be made, the scammer will go away richer than he came and the victim will have a very difficult time in retrieving the money.

A much more detailed explanation of the Nigeria Scam and its history can be found at: http://www.hoax-slayer.com/nigerian-scams.html. An example of the

Nigerian Scam taken from this web site is as follows:

Dear Friend,

REQUEST FOR URGENT BUSINESS ASSISTANCE

After due deliberation with my children, I decided to contact you for your assistance in standing as a beneficiary to the sum of US30.5M Thirty Million, Five Hundred Thousand United States Dollars Only)

First, let me start by introducing myself as Mrs. Stella Sigcau, a mother of three children and the Minister of Public Works in South African Government (17 June 1999) to date under the auspices of the President of South Africa MR THABO MBEKI. You can view my profile at my website: http://www.gov.za/gol/gcis_profile.jsp?id=1068 THE PROPOSAL

After the swearing in ceremony making me the Minister of Public Works in South African Government (17 June 1999) , my husband Mr Edelebe Sigcau died while he was on an official trip to Trinidad and Tobago in 1996.After his death, I discovered that he had some funds in a dollar account which amounted to the sum of US$30.5M with the BANK OF ENGLAND which had her offshore House in HOLLAND IN MASTERDAM

This fund emanated as a result of an over-invoiced contract which he executed with the Government of South Africa. Though I assisted him in getting this contract but I never knew that it was over-invoiced by him. I am afraid that the government of South Africa might start to investigate on contracts awarded from 1990 to date.If they discover this money in his bank account, they will confiscate it and seize his assets here in South Africa and this will definetely affect my political career in Govern I want your assistance in opening an account with GLOBAL CREDIT COMISSION. THE BANK IN AMSTERDAM WHERE THE MONEY IS KEPT through my Attorney so that this fund could be wired into your account directly without any hitch. As soon as the fund gets to your account, you are expected to move it immediately into another personal bank account in your country. I will see to it that the account is not traced from South Africa. As soon as you have confirmed the fund into your account, I will send my elde SHARING PERCENTAGE

For your assistance, I am offering you 20% of the principal sum which amounts to US$6,100.000.00 (Six million One Hundred Thousand United States Dollars Only) However, you have to assure me and also be ready to go into agreement with me that you will not elope with my fund.

If you agree to my terms, kindly as a matter of urgency send me an email. Due to my sensitive position in the South African Government, I would not WANT you to call me on phone or send a fax to me. All correspondence must be by mail.

If you want to speak with my Attorney, that is fine and okay by me. His chambers will be representing my interest at the GLOBAL CREDIT COMMISION. All correspondence must be made either to my Attorney Barrister Richard Lithuli, of Lithuli Chambers,or send me an email. I will also like you to give me your contact address,telephone and fax to enable my Attorney call or reach you from time to time.

Please I do not need to remind you of the need for absolute Confidentiality if this transaction must succeed. YOU MUST NOT CALL ME!

If you do not feel comfortable with this transaction, do not hesitate to discontinue.

Figure 3 - Nigerian/419 Scam

Phishing

Phishing attacks have gained a lot of press in recent times. These attacks ultimately seek to cause identity theft and/or to steal credit card numbers or other financial account information in order to directly obtain money that does not belong to them. Most of the time, a phishing email will appear to come from some type of financial institution. Popular examples are eBay and national banks. In most cases, a phishing email will provide some reason that you need to immediately login and verify your account information or check into the status of some issue. These emails will usually have some type of link in them that look legitimate. By going to the link, they user will be presented with an official looking site where they are expected to enter the information the phisher is after. Usually this will be personal information, credit card numbers or username and passwords that can ultimately lead to the phisher obtaining direct access to financial accounts owned by the victim. In most cases, by viewing the source code behind the email and understanding a little bit about html, it is possible to quickly identify these types of SPAM scams. Take the following example:

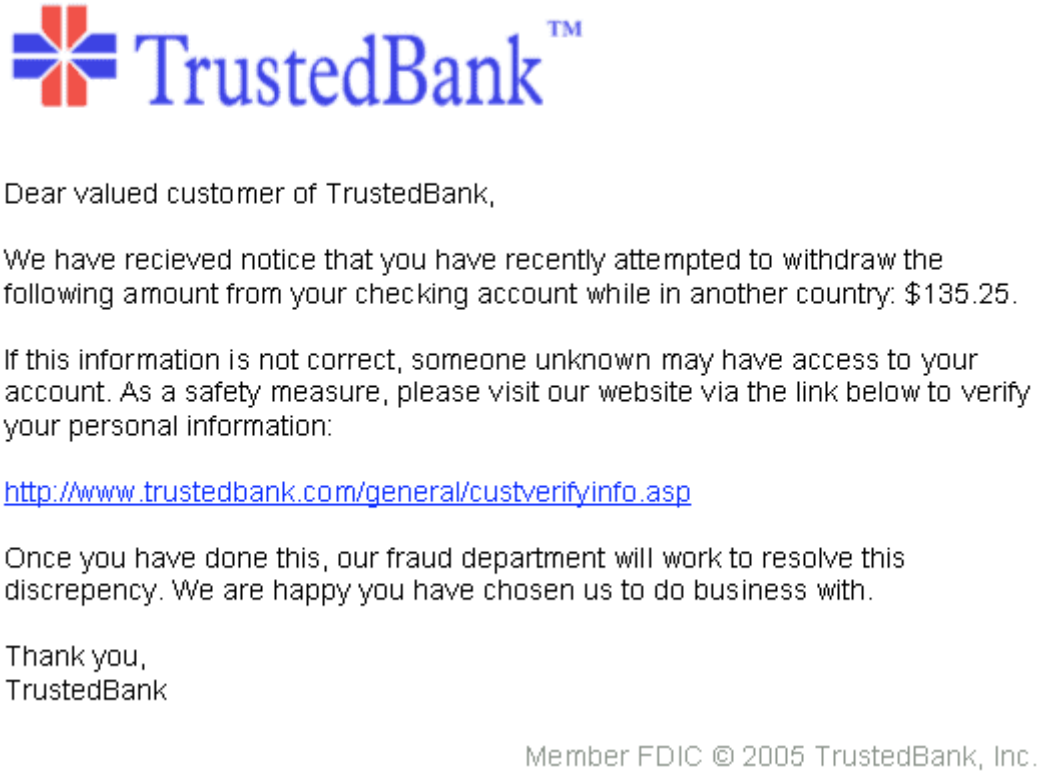


Figure 4 - Phishing example - Taken from Wikipedia.org

Suppose you took this email and viewed the html source and saw the following:

http://www.trustedbank.com/general/custverifyinfo.asp

In this example, the unsuspecting user clicks a link that looks like it's going to "Trusted Bank" when in fact it is going to some place different entirely. More nefarious examples have even gone so far as to use vulnerabilities in browsers to even hide the real location these links took the user by manipulating the way the link shows in the address bar or to register domains that may look legitimate at first glance, such as bank0famerica.com.

Advertising - banner ads

Arguably one of the most widespread motivation for SPAMmers has nothing to do with trying to get you to respond at all. Instead, the generate financial profit by establishing advertising relationships with unsuspecting web sites or companies who pay the SPAMmers for advertised based upon the number of times a specific ad banner is viewed or a particular web site is visited. By crafting enticing emails and by taking advantage of email clients that will decode html, spammers are often able to make just a tiny profit just by virtue of a target receiving and viewing the target email.

A concise article about this issue is available at: http://www.washtimes.com/business/20030803-110550-8329r.htm

Validating and reselling email lists

In a bizarre twist of fate, SPAMmers even make money off of each other. There are many places that a SPAMmer can go to purchase a list of "validated" email addresses. These email lists are nothing more than a list of addresses that the seller claims to have a real human behind them. How are these lists generated? Usually by the fact that emails sent to those addresses don't bounce, or worse by virtue of the fact that the person who owns the address took some type of action based upon a previous SPAM to them, such as asking to be removed from the list. People who purchase these lists will often turn around and sell them to other people, who in turn will sell the list again. This is one of the major reasons why once you've begun to receive SPAM, the likelihood it will ever stop is very low.

Deploying Malware

Another way to look at email born malware is to consider them SPAM. In fact, many of the techniques used to identify and automatically block SPAM will have a side effect of blocking viruses and other malware that come through email systems. In most cases, malware that is deployed in this way is not done directly by the "spammer". Instead the malware will make use of local address books or generate random destination emails using the processing power and privileges of an infected machine to do so. In other cases, there have been some cases of malware delivered by SPAM that ultimately captured information from infected systems and "dialed home" to deliver information that may ultimately lead to identity theft.

Steganography

So far we have talked about motivations for sending spam. Let us briefly shift gears and discuss a motivation for making something look like spam that really is not. Since spam is so prevalent, it is fairly routine to quickly glance at and ignore messages that look like spam. What if you wanted to convey a message to somebody, knowing that there was a high probability that people for whom the message is not intended will be looking in. Further, you wanted to try and make sure that the bystanders who happen to see the message won't recognize the true meaning and don't recognize it as being an obfuscated message. Here is where the art of steganography comes in. In short, steganography is the practice of achieving the goals listed above. Due to its very nature, SPAM makes an excellent carrier for

messages within the world of steganography. For an example of this technique in action, visit: https://www.spammimic.com/.

Reconnaissance

Similar to techniques used for generating lists of validated emails, some attackers send spam just as a means to try and enumerate valid email accounts against a domain. In this scenario, the end goal has nothing to do with the spam, but rather in identifying the valid email accounts from which a list of potentially valid user names can be generated. This information can then be used to launch a brute force attack against usernames and password against a companies computer systems. Since the attacker knows that the emails they are sending are going to be received by valid users, they will often send messages that look like spam with the expectation that the message will be treated as spam and blindly deleted. This gives the attack and advantage of being stealthy even though they are taking an action that might otherwise send off alarm bells.

Competitor Sabotage

Although rare, there have been cases where SPAM was sent with the direct intent of trying to spoil the name of a company or individual. The motivation to do this can be for revenge or in order to try and get a leg up on the competition. The following excerpt was taken from the incidents.org list archive:

> Last summer I received a pornographic spam that had web links (supposedly to the porn site). Since I nearly always complain about spam I receive, I was looking at the message and headers with Sam Spade and noticed that the referenced web site was to a company that was not to far from where

I live.

I then loaded the raw webpage and saw that it was not porn at all, but a legitimate company that provides lifeguards for apartments, hotels etc.

I emailed the listed contact person for the site, appending a copy of the spam. He replied that he believed this was an attempt by a competitor to drive him out of business, as he depended on email for contacts and being associated with porn would really damage his ability to recruit employees (mostly part time university students).

Since it was hard to trace the originator of the spam (dial up using spam relay), it would be almost impossible to prosecute this malicious act.

This kind of social engineering type of attack is one that we as intrusion analysts will also need to understand, not just the bad packet header attacks.

Available at http://archive.cert.uni-stuttgart.de/archive/intrusions/2002/12/msg00114.html

Humor, Chain Letters and Hoaxes

Some would argue that spam messages include those from people who know who have good intentions, but choose to send you things you just don't want cluttering your in box. Often, these messages are for humorous value for a chain letter or simply to pass on email that is in reality a hoax. By the definition used in this white paper, if the recipient has no desire to receive these emails, they are fair to classify it as spam. The motivation to send them is to pass on good humor, to satisfy some degree of superstition about the disaster that might occur if they don't pass on the email or due to being fooled into believing that they will receive a large sum of money from Microsoft if they pass on the message.

Unfortunately, “spam” falling into this category is likely one of the most difficult to block. This is because they usually come from people you know and are usually not sent out as a bulk and blind mailing. One way to try and reduce this type of email is to gently educate your friends and family who continually fall victim to these methods of propagation. A good resource to help them self-check the validity of emails that look like a hoax is http://www.snopes.com/. Training these people if you don’t want to receive humorous or chain letter emails, however, is a more difficult task.

4. Legal Issues of SPAM

DISCLAIMER: I AM NOT A LAWYER NOR DO I PLAY ONE ON TV!

The information contained in this section should not be considered legal counsel. For any information about the law or the interpretation thereof, please consult with your own legal counsel. Furthermore, in order to minimize any factual errors in this section, the vast majority of this section was taken from other sources with little original authorship done by the author of this paper. Appropriate credit is given for each source used.

CAN-SPAM

The CAN-SPAM act of 2003 is under the jurisdiction of the Federal Trade Commission. This law establishes requirements for email that is sent as an advertisement. It defines punishments for both the people sending the spam and the companies whose product is being advertised. This act sets forth specific guidelines that must be following for such email. In summary, they are:

- No false or misleading SMTP header information
- No deceptive or misleading subject lines
- Provide a working method for email recipients to opt-out
- Correctly identify the email as an advertisement and include the senders valid physical mailing address.

Penalties for violating the CAN-SPAM act can be up to $11,000 per incident. Additional fines can be applied for spammers who use other spamming techniques such as email harvesting, generating a large number of emails for purposes of sending spam or relay mail through other systems/networks in an authorized manner.

The information above in this section was borrowed heavily from: http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm.

In addition to these details, the CAN-SPAM act gives the FTC the optional right, to establish a do-not-e-mail registry and also allows for imposing specific requirements in subject labeling for sexually explicit material as prescribed by the FTC. The FTC chose to decline the granted authority to create the do-not-e-mail registry citing issues with difficulty to maintain and the fact that spammers are likely to use the registry as a list of validated email addresses to spam; thus negating the purpose of the registry. Consumers should be wary of any site that claims to be the national do-not-e-mail registry. For more information, see http://www.snopes.com/computer/internet/unsub.asp.

With respect to the label for sexually explicit material, the FTC established guidelines that require the term "SEXUALLY-EXPLICIT" to be contained in the subject line for any email whose opening will result in the viewing of sexually explicit material. Additional details can be found at: http://www.ftc.gov/opa/2004/04/adultlabel.htm.

The first actual conviction

Nicholas Tombros has the not so glamorous distinction of being the first to be convicted under the CAN-SPAM act. Nicholas was "wardriving" in order to locate and utilize open WiFi connections from which he could use other peoples networks to blast spam messages. This conviction had a side benefit of attracting a lot of attention to the need to secure wireless networks.

More detail about this incident and the source from which this section was written can be found at the following sites:

- http://news.zdnet.com/2100-1035_22-5390722.html.
- http://www.fbi.gov/page2/nov04/warspammer111004.htm.

CAN-SPAM Timeline

The following timeline was taken verbatim from http://www.lyris.com/resources/articles/200412canspam.html.

By Shannon Coulter

It's been a whole year since the CAN-SPAM Act was signed, so we thought we'd take a quick look back at some of the major highlights (and lowlights) of its first year as law.

December 16, 2003
President Bush signs the CAN-SPAM Act. It establishes the first national standards for commercial e-mail and requires the Federal Trade Commission to enforce its provisions.

April 2004
The first criminal charges are filed under the CAN-SPAM act when the FTC arrests four Detroit area men for selling fraudulent weight-loss products via email.

June 2004
The Coalition Against Unsolicited Commercial E-Mail (CAUCE) notes that in the six months since the CAN-SPAM act has been in effect, the volume of unsolicited commercial messages has increased dramatically.

September 2004
The first-ever conviction under CAN-SPAM takes place when a Southern California man pleads guilty to spamming people through unprotected hot spots. The case raises concerns about the risks of open-access Wi-Fi service.

October 2004
Email security firm MX Logic reports that only 4 percent of all unsolicited commercial email complies with the CAN-SPAM law. The FCC expands its regulation of spam to the realm of text messaging, making CAN-SPAM applicable to wireless devices such as cellular phones and personal digital assistants

November 2004
The FTC declines to implement a national "do-not-spam" list, citing difficulties associated with authentication. Two siblings-a brother and a sister-receive the first felony spam convictions under Virginia's anti-spam law. The Virginia law includes tougher sentences than the national CAN-SPAM act; the jury recommends a nine-year sentence. Industry observers note rapid growth in unsolicited email messages that contain religious themes. Because most messages are not overtly commercial, they are deemed CAN-SPAM compliant. The state of Ohio sends a new anti-spam bill to the governor who is expected to sign it.

December 2004
Microsoft files seven lawsuits against defendants who allegedly sent spam that violated the anti-spam law by not including the label "SEXUALLY EXPLICIT" in the subject line and initially viewable area of the messages.

5. Anti-Spam battle field

The battle against spam is fought on many fronts, both offensively and defensively. This section seeks to identify the most common battlefields where the fight is carried out.

Gateway Filters

Gateway filters are gaining significantly in popularity. These solutions will run on a system separate from the mail server itself in order to offload performance and even bandwidth consumption issues with running them on the mail server directly. They offer the benefit of coming in solutions that involve purchasing the solution for in-house consumption and management or as a service that can be purchased from a third party company. As an in-house solution, these systems tend to be very feature rich, but will often require trade-offs to be made about specific features (such as direct filter control by end users) in order to purchase a single solution that will be used for the entire environment. These solutions will typically be coupled with anti-virus to provide a complete mail filtering application. As an outsourced service, these solutions offer the medium to large enterprise the opportunity to buy just as much filtering as they need and to even offload a significant amount of bandwidth consumption from ever being consumed by the companies own Internet connections. Since mail will first go to a third party provider, their bandwidth is consumed for sending the unfiltered mail and the only the filtered mail will theoretically ever consume any bandwidth. Unfortunately, this also means trusting a third party to have resiliency within their network infrastructure and in order to ensure continuous availability for

your mail environment.

Mail Server Engines

Mail server engines represent some of the first methods that centralized anti-spam solutions were delivered. These products will run on a mail server directly and process for spam locally. These applications are typically coupled with anti-virus solutions. However, their usage has been on decline in favor of gateway filters that process mail before ever making it to a mail server. While they have the benefit of being centrally managed to process mail for an entire domain at once, they tend to contain less features than the gateway filter counterparts and often have a noticeable impact on the overall performance and response capability of the mail infrastructure, especially in larger environments.

Client Side Applications

Client side applications will install on a users workstation directly. These applications will typically cost between $20 and $40 per installation. However, careful consideration should be taken before deploying such an application. In a corporate environment, these applications rarely make sense to be deployed as a corporate initiative because they are decentralized by nature and thus would require much more administration than their mail server or gateway solution counterparts. In addition, since the filtering occurs as email is received, end users will directly experience any the common issue of a slight performance drain as the system processes the mail for spam. While this delay occurs in mail server engines and gateway filters as well, the end user is shielded from the concern

since they will rarely have any observance of this delay occurring. The last big down side of such applications is that they often require a little bit of end user knowledge and awareness to be able to be used to its full extent. While technical and especially security personnel rarely have an issue with this, it is a skill that will often elude the less technical amongst us.

On the other side, client side applications have the capability to be much more in tune with what a specific end user needs. While one anti-spam application might filter any and all user groups, another may be more effective at permitting authorized distribution groups and filtering appropriately based upon the content rather than the pattern upon which the message was received. These types of applications tend to be much better at heuristic and Bayesian filtering capabilities since it only needs to focus upon the pattern and established heuristic and Bayesian patterns of a single user rather than many. Further, their low cost for a single license make them very affordable and ideal for a home user or for an office with just a small number of users for which a much more costly mail server engine or gateway filter may not make sense.

A few client side applications to consider are as follows:

- SpamBully: http://www.spambully.com/
- InBoxer: http://www.inboxer.com/products.shtml
- Qurb: http://www.qurb.com/

This list should not be considered a definitive list of all client side anti-spam software nor as an endorsement for any of the software above. Client side anti-spam applications are plentiful and should be reviewed for specific features

appropriate to the system/user for which they will be used.

6. Weapons of Anti-Spam

Hashing/Checksums

When filtering mail, hashing/checksum checks is performing a mathematical computation against an email or portion of the email to identify and filter based upon quantity of matching emails sent. This technique helps to identify mail messages that may be sent in bulk or match known spam content. Rather than store the entire content in question, hashing/checksum engines will simply perform a mathematical computation against that content to present it in a much smaller form for purposes of matching. Mail that matches the resulting hash will by definition be a bulk mail which is a fairly good sign that a message is SPAM and should probably be blocked.

Open relay checks

Open relay checks will check to see if the source mail server permits relays. Some mail servers may do this directly, or they may rely upon generally available online databases, such as ORDB - Open Relay Database: http://www.ordb.org/. Mail servers that relay are generally considered to be misconfigured and are a very big target for spammers who will use them as a means to limit problems with being blacklisted and thus unable to continue sending spam. By blocking servers that permit relaying, this issue can be avoided.

RBL checks

Real-time blackhole lists, such as SPEWS or SpamCop are a list of DNS names

or IP addresses from which SPAM has been detected. These lists are generally made freely available or available for a small fee and subscribers may block any and all mail that is coming from a mail server listed in an RBL list. Unfortunately, these lists are often prone to false positives and should be used with extreme caution within a corporate environment.

Bayesian Filtering

Bayesian filtering is performing a statistical calculation of probability that a given message is spam based upon user input. This techniques works based upon feedback from users to train the filter about false positives and false negatives so that it can dynamically adjust its filtering capabilities. This type of technique usually works best when deployed in a client side application filter, but does have some use in more centralized filters as well.

Heuristics

Heuristics is another form of statistical calculation the will combine a variety of detection techniques to recognize patterns that when taken together may indicate the probability of SPAM. This usually comes in the form of assigning certain point values to specific matches such as signature matching or existing in an RBL and then setting a point threshold that, if crossed, will indicate that the message is SPAM and should be treated as such.

Signature matching

Signature matching was one of the first methods used to filter for SPAM. This

technique will deploy a simply filter that will look for specific keywords within a message. Unfortunately, this is often prone to false positives and receives a large amount of criticism. Consider for example a filter that will block a message as spam if it contains the word "breast". Now consider if this filter is deployed in a healthcare organization who regularly receives and sends mail about breast cancer.

Black listing

Black listing is effectively a kind of localized RBL. In effect, a black list is the practice of identifying a specific source address, domain or IP from which all mail should be blocked. This type of list categorically differs from an RBL in that it is typically maintained by the organization whose mail is filtered by the system that uses the black list.

White listing

On the opposite side of black listing, we have white listing which is the practice of identifying a specific source address, domain or IP from which all mail should be permitted. Like black lists, white lists are typically maintained by the organization whose email is filtered by the system that uses the white list. White lists are often deployed when continuous false positives occur and other configuration changes will not easily ensure that the desired email can bypass the filter.

Anti-virus

Some of the most dangerous types of SPAM that exist in the world today are the kind that carries some type of malware. In many cases, anti-spam techniques will work to identify and block emails containing malware long before anti-virus vendors have identified and deployed filters for the new and emerging threats. This occurs often because the initial deployment of an email born virus happens with such speed that methods used to detect large amounts of emails with the same content will hinder the spread of new and emerging threats. However, after the initial "hit" when these mails are seen, they will tend to fall out of the standard filters used to detect sudden bulk mails, at which point in time anti-virus application serve a crucial role of providing a fail safe to prevent the further spread of viruses and other malware through these spam email messages.

Further, the same user education that is often taught for defending against viruses and other malware that arrive through email will help to prevent proliferation of spam. Namely, do not open emails that appear suspicious in nature. Do not click on links in unsolicited email and do not respond to such emails.

Anti-Spyware

Spyware applications are also associated with spam for several reasons. First, the user education and training that would help prevent someone from deploying spyware works hand in hand with the same training that can help prevent a person from doing things that could lead to receiving an increased amount of spam. Furthermore, spyware applications have been known to be linked directly to providing email addresses that can subsequently be used by spammers to send their

bulk messages. In short, a good anti-spyware implementation can help minimize or reduce exposure to spam and many other security concerns related to these applications. The good news is that there are many commercial and free tools available, such as Ad-Aware, Spybot Search & Destroy and Microsoft AntiSpyware (beta) that can help detect and destroy spyware.

Avoiding the unsubscription trap

As tempting as it may be to hit the "unsubscribe" link on a piece of spam mail, this is often a bad move. Since spammers will often work to identify "validated" email accounts and use these to sell or trade with each other, by clicking on an "unsubscribe" link, you may be actually falling into a trap set by the spam to validate that a real human is reading the message. This act makes your email address more valuable and can have the end result of increasing the amount of spam you are about to receive rather than removing you from the spammers list.

Spamsinks

Spamsink accounts are email accounts setup, typically on free email services such as hotmail or gmail, with the specific purpose of being able to provide a throw away email address when forced to submit an email address in some way. In some cases, these accounts may be an alias for your real account or you may set them up independently and check them on a periodic basis as a specific need requires. The more adventurous may choose to create a new account each time they are required to provide an email address to a questionable source so that they can know who may have shared their email account to spammers and take appropriate

action.

Avoiding putting emails in public places

One of the most common techniques that spammers use to obtain address is to setup scripts that automatically parse company web sites and public email group archives to harvest email addresses. By using a little diligence when displaying email addresses in these public ways, a lot of spam can be avoided. A few methods to do this could be to post an email address in such a way that a human would be able to understand what the email address is, but that a computer program doing basic parsing will likely miss. For example, you might post:

sample @ domain . com or sample (at) domain (dot) com

Another method in html is to encode the @ and the . symbols in ASCII such as:

Sample@domain.com

Especially on company websites, an even more effective way is to never publicly display public email addresses, but instead to provide forms that can be filled out and will result in the back end web code to send email to the designated box.

Another technique to achieve this goal is to display email addresses as an image rather than as actual text.

A final point for consideration is the technique of using a separate account from your primary account for use in public discussion forums or for public display

in use. When such an account becomes overburdened with spam, a new account can be created and the original one thrown away much like a spamsink account.

Cookie Management

Cookies are files that are stored by a web browser to contain specific information for later retrieval by a web site that is being visited. Unfortunately, the information in these cookies may often provide specific information, such as credit card numbers or personal names and email addresses that can potentially be harvested by specially crafted web sites in order to harvest email addresses. By disabling cookies altogether or at least by carefully managing the storage and retrieval of these cookies by specific web sites, these techniques used by spammers to harvest email addresses can potentially be defeated.

In Internet explorer, cookies can be disabled by going to Tools -> Internet Options -> Privacy -> Adjust the slider appropriately.

In Firefox, go to Tools -> Options -> Privacy -> Cookies.

Nearly every web browser will provide controls for you to manage your cookies. If you're not using Internet Explorer or Firefox, research how to do this in your browser and consider whether or not you can live without storing cookies. It's only fair to point out that by disabling cookies, some inconvenience and minor annoyances will be experienced.

If instead of disabling cookies, it is more desirable to actively manage them, there are many third party applications that can do this, such as Cookiewall,

Cookie Monster and Cookie Jar, just to name a few. These applications each work with different browsers or sets of browsers and offer different features. Consider identifying a solution that can help you determine which cookies to store and can help you know when a site is requesting a cookie and give you the power to fine tune which sites can pull which cookies to help reduce the likelihood of cookie harvesting.

Protection of ones own network

Due to the response that spammers have received from blacklisting and other anti-spam techniques, they have been forced to become more mobile and work to invent or identify new sources from which to send their SPAM. This means that spammers have begun wardriving or using other means to obtain control of systems on the internet from which to launch their spam attacks. By implementing proper security controls in our own company networks **and home networks** we can all play a part in reducing the number of systems and networks that spammers can use to carry out their activities.

As mentioned previously, the first actual conviction using the CAN-SPAM act involved an incident with Nicholas Tombros who was wardriving to locate unsecured wireless networks from which he sent spam messages. This is a clear and specific indication that this kind of threat is real in our world today and by doing out part to work to secure our own networks against such attacks, we can at least try to prevent becoming part of the problem.

A very important part of defending ones own networks and systems against

becoming a launching point for spam, look carefully into blocking all outbound smtp (25/tcp) traffic from all systems with specific exceptions allowed for known and authorized mail servers only. This act can not only help mitigate against becoming a launching point for spam, but can also help reduce the probability that an internal infection by a virus that spreads through its own smtp engine will be further propagated by you or your organization.

Proper configuration of mail servers

In a similar vein to protecting ones own network, careful attention should be paid to the mail server. Specifically, due care should be taken to ensure that relaying is not permitted from the general Internet. There may be legitimate reasons to permit relaying from specific internal hosts, but these should be done with due diligence and care. Furthermore, when sending mail on behalf of a user, some form of authentication should be required to try and prevent your mail server from sending potential spam messages on that could be from an unauthorized external user who spoofs the source address to be an internal email account. By requiring authentication for sending all outbound mail, this threat can greatly be reduced.

SPF – Sender Policy Framework

SPF (Sender Policy Framework) records are a fairly recent invention and are not yet a standard. However, several companies have already begun to use or require SPF records in order for a mail server to be permitted to send mail. The SPF record is defined by RFC 4408. In short, this is a way to use DNS such that someone with control of a sites DNS records can set a specific record that will identify

specifically which servers or IP addresses are authorized to send mail on behalf of that domain. Once implemented fully, servers can then choose to not accept mail claiming to come from an email address where the source address of the mail connection is not coming from an IP address listed in the SPF record. This technique can help to significantly reduce the amount of spoofing that is occurring in spam messages. The primary website to read about and learn more about SPF is http://www.openspf.org.

Only permit outbound SMTP from authorized mail servers

As spammers like to use zombies in order to send their mail, a responsible company will implement defense in depth strategies that include only permitting the access that is required. While it is easy to open up all access outbound and implement a more restrictive rule-set for inbound traffic, this strategy is irresponsible and leaves the company exposed to a variety of risks. If and when an attacker manages to gain control of a system that may be on a company network, the usefulness of that system will be dictated by the access that this system has and the resources that it can provide. By blocking outbound SMTP access except from known and authorized mail servers, the threat that spammers will obtain control of and then use your companies' resources in order to spam is greatly diminished. Furthermore, this has a side benefit of protecting against viruses that propagate by way of their own SMTP engines and some spyware applications that will do that same.

Avoiding chain mail and hoax mail propagation

Although chain mail and hoax emails are more in the category of humor than the product of spammers seeking to profit from any of the methods previously mentioned, it still represents a noticeable portion of spam. By teaching employees to resist the urge to fall victim to the message such emails contain, a more important lesson of avoiding gullibility can be taught. Any suspicious email should be approached with caution and by focusing on developing a healthy skepticism and not blindly believing, responding to or forwarding on emails that have a lack of plausibility and reality, users can learn to become more aware and avoid the traps of even more serious social engineering threats that contain malicious viruses that present a more serious concern. A very good resource for identifying if an email that has been received is a known hoax, check out http://www.snopes.com.

Turning off HTML rendering in email clients

Turning off html in email clients can help significantly in reducing the amount of information leakage and in reducing the amount of benefits that spammers receive from sending their message. By not viewing emails in html, phishing scams are much easier to spot when link targets do not match the apparent text for the link intended to be clicked. Additionally, the technique of sending single pixel images within embedded html associated with specific email addresses can be defeated as these images will never be accessed and account validation will not occur. Also, consider that spammers that depend upon certain banner ads to be viewed in order to generate revenue will not be able to collect if your email client does not display the banner as a result of rendering the html within a

received email. In addition to these benefits, exploits that depend upon html rendering, especially by Internet Explorer, can be avoided entirely from coming in as a result of receiving a specially crafted email. Unfortunately, it is improbable that many organizations will choose to enforce this technique due to the abundance of legitimate mail that uses html. The ease and convenience of this feature will often win out over the technical and security benefits that it provides.

In Outlook 2002 SP1 or later, html rendering can be disabled by applying the following registry key: HKEY_CURRENT_USER¥Software¥Microsoft¥Office¥10.0¥Outlook¥Options¥Mail DWORD of READASPLAIN Value of 1.

In Outlook 2003, go to Tools > Options > Preference > E-mail options and check the option to read all mail as plain text.

As a potential compromise between turning off HTML altogether, scripting and other programmatic controls within the html rendering engine can be disabled in Outlook. This is done by going to Tools > Options > Security > Zone: Restricted sites and then using the zone settings to ensure that all scripting and controls are disabled by default.

Furthermore, it would be prudent to configure Outlook to not send mails in anything other than plain text. To do so, follow these steps from within Tools > Options > Mail Format:

- Compose in this message format: Plain Text
- Deselect "Use Microsoft Word to edit e-mail messages"
- Deselect "Use Microsoft Word to read Rich Test e-mail messages"

- Internet Format > Convert to plain text format

While the tips and suggestions discussed above focus on the usage of Microsoft Outlook, the underlying principle applies to any mail client and some consideration and research should be given to discovering the options available for your companies mail readers to see what configuration settings might help to meet the same goals and to see if there may be even better or more detailed controls that can even further enhance the security of your companies mail reading environment.

Reading and responding to SMTP Headers

By learning to read SMTP headers, we can better prepare ourselves to correct interpret and respond to spam messages. The information contained within SMTP headers provide solid evidence about the true source of spam emails and are essential when responding to or reporting spam messages within an abuse reporting environment. A very detailed explanation of SMTP headers is available at http://www.stopspam.org/email/headers.html.

7. Responsible mass email

Up to this point we have spent a lot of time discussing the elements that help to identify spam and how to defend against them. A complete discussion about spam as a concern is incomplete without discussing how an organization can send mass marketing or mass distribution emails without becoming part of the problem. Unfortunately, many reputable and well meaning organizations can be at risk of being classified as a spammer if they do not responsibly handle their email marketing campaigns. This section seeks to provide some guidance to an organization who feels the need to have such a mass marketing or mass distribution email program that has a legitimate desire to do so in a responsible manner.

Double opt-in

A double opt-in process is appropriate to use when a user is added to a mass by way of some online form. Any time a user is being required to provide an email address, perhaps because they are purchasing some product from your web site, they should be required to select a check box in order to be added to the list. Note that this check box should never be checked on by default or else this would be an opt-out site not an opt-in site. Now, following submission of this web form, the user should then be sent a confirmation email that explains they are being added to an email distribution list. In order to complete the process of being added to the distribution list, the user should be required to respond to this email by either a response email or by going to a provided unique web link. Users should NOT be added

the mail list until they have completed the second process of validating that they do indeed wish to be on the distribution list. This process helps to increase awareness that the user is being added to the list and significantly reduces the likelihood that someone other than the person who has legitimate access for the email address is the one signing up to be on the list.

Do not buy mailing lists

Responsible organizations should never buy a list of email addresses. Doing so opens the door for a significant amount of liability since the organization receiving the email list has no control over whether the email addresses were gathered responsibly. There is a high probability that purchased email lists are being obtained from companies that utilize address harvesting techniques described earlier. Any and all email addresses on such a mass marketing or mass distribution email program should be obtained by way of direct gathering techniques between the company using the list and the person being added to the list.

Consider using listservs

Listservs, in this context, are any email distribution group application that allow users to directly signup or remove themselves from the distribution by way of email based commands. Listservs can be moderated or un-moderated and can allow open, approval based or invitation only based membership. These applications are less useful for marketing type of email programs, but are very useful for knowledge based groups such as news or technical support based email programs. However, these programs should be considered for any mass marketing or mass email program,

especially ones that will typically send multiple emails in a single day or even week, as they can offer a lot of flexibility to the subscribed members to control how the mail is received and to be able to directly remove themselves at any time. Another reason why listservs work well to avoid being classified as spam is that membership typically requires specific and direct action to be taken by the person signing up (typically a double opt-in type process) in order to be added to the list.

Periodic purge

Email lists, with a possible exception for listservs, should periodically be purged to remove bad email addresses or addresses for individuals who no longer wish to be on the list, but who have not taken steps to unsubscribe. The rate at which a purge should occur is going to be dependant upon the type of list and rate of emails. Listservs will typically work fine with a very long period (possibly measured in years) between purges. However, more advertising or marketing based distribution lists should look at a purging process measured more in months (perhaps 6) than years. The purging process should involve sending out an email (or maybe even a series of emails) that require a user to take a specific action (such as click on a link or respond) in order to remain on the list. Users who fail to take this action should then be removed after a specified period of time that is dictated in the email. This process is important as users are being trained (and should be trained) to avoid "unsubscribing" from lists that they perceive as spam. While a spammer looks for and desires a positive response to "unsubscribe", a responsible organization will implement a periodic process that will truly unsubscribe an email address based upon a lack of response.

Protect your mailing list

Users who sign up to receive emails from your organization will have signed up for receipt of emails from ONLY your organization. While many companies will offer opt-in processes by which a user authorizes the organization to share their email address with partners, this is a very dangerous practice. Once your mailing list has been provided to a partner, your organization no longer has any control over where and how that email address is used. Remember that even reputable companies may fall into spam-like tactics and could unwittingly provide fuel to organizations or people who knowingly and intentionally engage in spam practices. Ultimately, if this happens as a direct or indirect result of someone providing their email address to your organization, your organization will have its image reduced in the eyes of the spam recipient.

Immediate unsubscribing

While thorough awareness programs will train end users to not "unsubscribe" from spam lists, this doesn't mean that legitimate companies shouldn't offer them. The difference between a spammer and a legitimate organization is that a spammer will identify "unsubscribed" addresses as confirmed accounts and the end result will be an increase in the amount of emails received, on the other hand a legitimate company will IMMEDIATELY remove the email address from the distribution and discard the information about the email address altogether.

Do it in house

When sending emails, the actual systems and personnel that send them should

preferably be under the direct control and employment of your organization. By doing so, your company retains complete control over the mass marketing and mass emailing program. Using a third party "advertising agency" may be dangerous as these advertising agencies may in fact be the spammers from which we are trying to protect ourselves. If you permit such a third party organization to run your email marketing campaign, you will also be providing them with your email distribution lists. A responsible organization should make a sincere effort to develop the expertise and necessary equipment to have direct control over the entire process of actually sending the emails.

Consider rate limiting

The rate at which email is being sent can have an impact on the bandwidth of the end user and, more importantly, your own organization. If the amount of emails being sent is truly massive, then mechanisms should be identified and implemented that will provide some type of rate limiting the throttle the rate at which the emails are sent.

Hide the recipients (BCC or otherwise)

Any time an email is being sent where multiple recipients will receive the email, care should be taken to ensure that recipients will not receive the list of other people who are receiving the email. Doing so will amount to providing your email distribution lists to third parties which was already mentioned as a thing to avoid. Furthermore, if you are setting up a distribution group, especially if the distribution group email address is set as the "reply-to" address, ensure that

only specific authorized individuals within your company have the ability to send to that list. Even if the membership is hidden, failure to protect who can send to such a distribution list will invariably result in a flood of emails coming back to list as a result of recipients' vacation messages or other automated responses. Failure to block who can send to these distribution lists again violates the principle of not providing email addresses to third parties in an indirect manner. If all else fails, you can use the BCC field which will ensure that the identity of the recipient is protected.

Use legitimate DNS domains matching to appropriate IPs

Many mail servers will reject any and all emails that are not coming from IP space or from an IP with a DNS record that is not legitimately registered as being associated with the apparent sender. While this process currently will result in blockage of may legitimate emails, it is something that should be taken into consideration. In an ideal world, the mail server that sends mass marketing or mass distribution emails for your organization should be on address space that you own according to the IP registration details. However, in many cases this is impractical. In the real world, at minimum, servers that send email should preferably have DNS A records appropriate for your companies DNS domain and the PTR record for the IP address associated with the email server should point to the A record. Lack of a PTR record is often used as a reason for which a mail server may reject the receipt of an email. Again, this practice is prone to many false positives, but it is a fairly widely used technique to help significantly reduce the number of spam messages received by an organization. This is because there is a very high percentage of "zombie" systems from which spammers send mail for which

there is no PTR record. On the other hand, a very high percentage of legitimate mail servers will have a PTR record.

As a final note for consideration, review the earlier discussion about RFC4008 for SPF (Sender Policy Framework). This RFC shows a lot of promise in being a very effective weapon against email spoofing. While this RFC is not yet a standard, there is nearly no negative impact to implementing them for your environment.

Consult with legal counsel

In the United States, CAN-SPAM is directly applicable and very important to consider when sending mass marketing emails. While it would be very difficult to provide every existing law related to spam to cover every nation or region, it is easy to provide the recommendation that any such program should involve communication with legal counsel to ensure legal compliance with any national or localized laws for your situation.

Monitor blacklist sites

No matter what you do, there is a very real threat that your company may be listed on a blacklist somewhere. Unfortunately, many blacklists have a very bad tendency to have a very high rate of false positives. If you are running a mass marketing or mass email program your companies mail server will almost definitely be listed on a blacklist at some point in time regardless of how far you go to

follow the advice given above and how responsibly your organization act. This is ultimately because many blacklists sites out of necessity will not take any measures to validate the legitimacy of emails that are submitted to them. Unfortunately, many corporate environments will use blacklists as a sole reason for blocking mail without understanding the high false positive rate issue. In order to mitigate against this as a concern for your organization, blacklists should be regularly checked to determine if your organization has been listed and to allow you to take steps to remove your organization from these lists. Two sites to help you check if your companies mail servers have been listed are available at the following URLs:

- http://relays.osirusoft.com/cgi-bin/rbcheck.cgi
- http://www.tqmcube.com/rblcheck.php

8. Conclusion

The SPAM battlefield is in a constant state of flux. As better defensive weapons are built on the defense side, spammers are constantly building better weapons to overcome these defensive measures on the offensive side. Unfortunately, this means that organizations must continue to be proactive in updating their defenses to try and prevent being deluged with time wasting and potential security threat vectors from entering the environments. By becoming and staying informed about the offensive and defensive weapons of both spammers and anti-spammers, we can prepared ourselves and our organizations to take direct measures to reduce the proliferation of SPAM. Finally, by understanding the elements that define what a spam message is and the tactics that spammers use, responsible organizations who feel they have a legitimate need to send mass marketing or mass distribution email scan consciously take steps to avoid being classified, and thus treated, as spammers.

9. References

1. "Award-Winning Spam Filter for Microsoft Outlook." InBoxer. 21 Oct. 2006 <http://www.inboxer.com/products.shtml>.

2. Babener, Jeffrey A. "Identifying Illegal Pyramid Schemes." MLMStartup. 21 Oct. 2006 <http://www.mlmstartup.com/articles/b24ho.htm>.

3. "CA Anti-Spam (Formerly Qurb)." 21 Oct. 2006 <http://www.qurb.com/>.

4. Coulter, Shannon. "CAN-SPAM Timeline." Lyris. Lyris Technologies. 21 Oct. 2006 <http://www.lyris.com/resources/articles/200412canspam.html>.

5. "DNSBL Database Check." Osirusoft. 21 Oct. 2006 <http://relays.osirusoft.com/cgi-bin/rbcheck.cgi>.

6. "Federal Bureau of Investigation - Press Room - Headline Archives." FBI.Gov. 10 Nov. 2004. 21 Oct. 2006 <http://www.fbi.gov/page2/nov04/warspammer111004.htm>.

7. "FTC Adopts Rule That Requires Notice That Spam Contains Secually Explicity Material." 13 Apr. 2004. Federal Trade Commission. 21 Oct. 2006 <http://www.ftc.gov/opa/2004/04/adultlabel.htm>.

8. "How Do Spammers Actually Make Their Money?" Ask Yahoo. 21 Oct. 2006 <http://ask.yahoo.com/20050103.html>.

9. "I'M Getting Spam From PsychPage." PsychPage. 2 May 2006. 21 Oct. 2006 <http://www.psychpage.com/spammer.html>.

10. Lemke, Tim. "Spammers Make Profits Without Making a Sale." Washington Post. 21 Oct. 2006 <http://www.washtimes.com/business/20030803-110550-8329r.htm>.

11. Mike. "Techdit: Spammers Make Profits Without Making a Sale." Techdirt. 21 Oct. 2006 <http://www.techdirt.com/articles/20030804/0239218.shtml>.

12. "Multi-RBL Checker." TQM^3. 21 Oct. 2006 <http://www.tqmcube.com/rblcheck.php>.

13. "Nigerian Scams - 419 Scam Information." Hoax-Slayer. 21 Oct. 2006 <http://www.hoax-slayer.com/nigerian-scams.html>.

14. "NPR: Penny-Stock Spam Yields Profits." National Public Radio. 25 Aug. 2006. 21 Oct. 2006 <http://www.npr.org/templates/story/story.php?storyId=5711560&ft=1&f=2>.

15. "Open Relay Database - Welcome to the ORDB.Org - the Open Relay DataBase." ORDB. 21 Oct. 2006 <http://www.ordb.org/>.

16. "Re: Spam Blocking." 6 Dec. 2002. 21 Oct. 2006 <http://archive.cert.uni-stuttgart.de/archive/intrusions/2002/12/msg00114.html>.

17. "Reading Email Headers." Stopspam.Org. 21 Oct. 2006 <http://www.stopspam.org/email/headers.html>.

18. Sauver Ph.d., Joe S. "The Economics of Spam." University of Oregon. 21 Oct. 2006 <http://cc.uoregon.edu/cnews/summer2003/spameconomics.html>.

19. Shim, Richard. "'Wardriving' Conviction is First Under Can-Spam | Tech News on ZDNet." ZDNet. 30 Sept. 2004. CNET News.com. 21 Oct. 2006 <http://news.zdnet.com/2100-1035_22-5390722.html>.

20. "Spam (Electronic) - Wikipedia, the Free Encylopedia." Wikipedia. 21 Oct. 2006 <http://en.wikipedia.org/wiki/Spam_%28electronic%29>.

21. "Spam - Defitions From Dictionary.Com." Dictionary.Com. 21 Oct. 2006 <http://www.dictionary.com>.

22. "Spam Bully - Email Spam Filter for Outlook and Outlook Express." Spam Bully. 21 Oct. 2006 <http://www.spambully.com/>.

23. "Spam List of Emails." 21 Oct. 2006 <http://home.versanet.de/~pdietrich/spam-block.html>.

24. "Spammimic." 21 Oct. 2006 <https://www.spammimic.com/>.

25. "SPF: a Sender Policy Framework to Prevent Email Forgery." Openspf.Org. 21 Oct. 2006 <http://www.openspf.org>.

26. "The CAN-SPAM Act: Requirements for Commercial Emailers." Federal Trade Commision. 21 Oct. 2006 <http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm>.

27. "Tip 140: Read as Plain Text." Outlook-Tips. 21 Oct. 2006 <http://www.outlook-tips.net/archives/2004/20040603.htm>.

28. Turner, Aubrey. "TenTenTwelveCorp." Aubreyturner.Org. 21 Oct. 2006 <http://www.aubreyturner.org/index.php?/orglog/comments/1377/>.

29. "Urban Legends Reference Pages: Computers (National Do Not E-Mail Registry)." Snopes. 5 Feb. 2004. 21 Oct. 2006 <http://www.snopes.com/computer/internet/unsub.asp>.

30. "Urban Legends Reference Pages." Snopes. 21 Oct. 2006 <http://www.snopes.com/>.

Last Updated: August 18th, 2009

Upcoming SANS Training

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

SANS Critical Infrastructure Protection at Oceania CACS2009	**Canberra, Australia**	**Sep 10, 2009 - Sep 11, 2009**	**Live Event**
SANS Network Security 2009	**San Diego, CA**	**Sep 14, 2009 - Sep 22, 2009**	**Live Event**
SANS WhatWorks in Data Leakage Prevention and Encryption Summit 2009	**San Diego, CA**	**Sep 14, 2009 - Sep 15, 2009**	**Live Event**
Paul A. Henry's Virtualization and Security Operations co-located with GovWare	**Suntec City, Singapore**	**Oct 05, 2009 - Oct 07, 2009**	**Live Event**
SANS Forensics Egypt 2009	**Cairo, Egypt**	**Oct 11, 2009 - Oct 15, 2009**	**Live Event**
SANS Tokyo 2009 Autumn	**Tokyo, Japan**	**Oct 19, 2009 - Oct 24, 2009**	**Live Event**
SANS Chicago North Shore 2009	**Skokie, IL**	**Oct 26, 2009 - Nov 02, 2009**	**Live Event**
The 2009 European Community SCADA and Process Control Summit	**Stockholm, Sweden**	**Oct 27, 2009 - Oct 28, 2009**	**Live Event**
SANS Middle East 2009	**Dubai, United Arab Emirates**	**Oct 31, 2009 - Nov 11, 2009**	**Live Event**
SANS Oslo in cooperation with Mnemonic	**Oslo, Norway**	**Nov 02, 2009 - Nov 07, 2009**	**Live Event**
SANS Sydney 2009	**Sydney, Australia**	**Nov 09, 2009 - Nov 14, 2009**	**Live Event**
Hong Kong Advanced Forensics Seminar	**Hong Kong, Hong Kong**	**Nov 09, 2009 - Nov 14, 2009**	**Live Event**
SANS San Francisco 2009	**San Francisco, CA**	**Nov 09, 2009 - Nov 14, 2009**	**Live Event**
SANS Vancouver 2009	**Vancouver,**	**Nov 14, 2009 - Nov 19, 2009**	**Live Event**
SANS Virginia Beach 2009	**OnlineVA**	**Aug 28, 2009 - Sep 04, 2009**	**Live Event**
SANS OnDemand	**Books & MP3s Only**	**Anytime**	**Self Paced**