December 2003

Spam: A Security Issue

Introduction

Spam has become a plague for email users around the world. The sheer volume of spam is annoying as users have to clean their inboxes from these unwanted messages on a daily basis. In addition, the aggressive and often sexually explicit nature of spam is offensive and frustrating to most end users. Spam is clearly a nuisance, but in this white paper, we will demonstrate how spam has evolved into a true security issue for organizations.

We begin with defining email security, followed by an analysis of spam, spam-related threats and some of the tools and methods used by spammers. Finally, we discuss next generation email threats and the requirements to protect an organization's email infrastructure appropriately.

Email Security Defined

In order to provide secure email services, an organization's Information Technology department must be able to proactively support three essential security measures: Confidentiality, Integrity and Availability. Failure by an organization to provide effective email security measures will compromise the value of email as a critical business tool. The evolution of spam has had a direct impact on email services by breaching these measures. See Table 1.

Security Measures	**Description**
Confidentiality	Protection of email messages and systems from unauthorized access.
Integrity	Guarantee that email messages and systems are not distorted or destroyed in an unauthorized way.
Availability	Ensure mail servers and directories meet the committed service level.

Table 1: Email Security Measures

Corporations have deployed firewalls to enforce network level security, but are limited in terms of analyzing the actual content of email that is transmitted. Technically, a firewall interprets email as data packages from outside the network directed to a dedicated mail server on port 25 inside the network. These data packages receive only the most rudimentary scrutiny, leaving email vulnerable to a variety of threats. In this white paper we will examine these threats as they are related to spam.

Spam and Related Email Threats

In this section we begin by describing the email security threat spam, followed by intrusion, denial-of-service, and viruses and worms.

Spam

Every day, when people open their e-mail inboxes, they find numerous messages from unknown parties soliciting a range of services and products - they find spam. The definition of spam is neither clear nor consistent, however it can best be described as unwanted email messages. The majority of these unwanted messages are of commercial nature, hence the name "unsolicited commercial email."

Until recently spam was considered a minor nuisance. However the scale and the effect of the spam epidemic suggests that it is no longer simply a nuisance, but has become a large-scale network problem. According to the Radicati Group, spam costs corporations an estimated $49 per user per year[1] in the form of additional mail servers required to handle the increased load.

People who send spam (spammers) don't do it for fun, but to earn money. Spamming is an actual business process, and like most businesses, the goal is to make a profit. Spammers profit when the spam they send equals the revenue from sales generated from a spam campaign, less the cost of sending spam. Let's assume that one in every 10,000 people who receive spam purchase a product or service as a result of a spam campaign. If the profit per item to the spammer is $10 and he sends 1,000,000 spam messages, he will quickly generate $1,000. A spammer can send 1,000,000 spam messages in a matter of hours, and if he triples that number, his profits would nearly triple as well, as the incremental cost of sending more email is close to insignificant.

[1] RADICATI GROUP, " The IT Cost of Spam", August 2003

To generate higher profits, spammers must simply increase the volume of spam they send. This has been validated by research conducted by CipherTrust. Spam currently accounts for over 50 percent of an organization's email traffic. The increased volume of spam consumes an organization's messaging infrastructure, requiring more server capacity and network bandwidth - in other words, it has a direct impact on the availability of email. It also erodes user productivity as workers waste their employer's time managing spam and occasionally being diverted to a Web site offering a desirable product or service. Lastly, the sexually-explicit nature of much of the spam exploits potential liability issues for an organization.

An increasing number of organizations have realized the threat spam imposes on their organization and are looking at deploying spam protection solutions. Spammers constantly change their spam-sending methods and create new techniques to masquerade the content. The industry continues to respond with a myriad of various detection techniques such as blacklists, whitelists, statistical analysis, signature-based filters, keywords, etc., but there is no silver bullet against spam. Each technique has proven to be effective against specific types of spam, but has done poorly against others, resulting in weak performance against the overall spam problem.

To address this effectiveness issue, anti-spam solutions must deploy techniques that answer four basic questions about a message:

1. Who is the message from?
2. How was the message sent?
3. Where was the message sent?
4. What is in the message?

The highest spam filtering success rate (a function of the spam detection rate and the false positive rate) can be achieved by combining results from multiple detection techniques into one aggregated score. The score identifies the likelihood of a message to be spam, and if it meets or exceeds the threshold for what should be considered spam, an action should be performed on the message such as: quarantine, delete, log, subject-line insertion or x-header insertion.

With the rapid evolution of spam, anti-spam solutions must deliver continuous detection technique updates in order to maintain their accuracy levels. In addition, the solutions must be designed to accommodate new, innovative techniques that will employ new spamming methods against future spam attacks.

Intrusion

Intrusion occurs when unauthorized users gain access to an organization's infrastructure. As it relates to spam, this typically means that spammers break in to a mail server to gain control of it for the purpose of sending spam, or to harvest email addresses. In some cases, spammers will also plant computer code on PCs across an organization, turning them into spamming machines, also called drones. This was demonstrated with recent worms such as Sobig and Swen.

Hackers and spammers gain access to systems by taking advantage of known weaknesses in an application's code. For example, hackers might open a legitimate communication channel with a sendmail mail transfer agent (MTA) (by sending what at first looks like a normal email), but instead of sending a bona fide email, the hacker sends malicious instructions that - because of weaknesses in sendmail - get executed. Now the sendmail MTA starts running the hacker's program, which can take control over sendmail, instructing the MTA to re-direct all mail to the hacker instead of the original recipients, or to send confidential files to a hijacked server. These actions have a negative effect on the confidentiality and integrity of email.

Another point of intrusion to an email system is webmail. Many organizations today allow their mobile workers to access corporate email through a Web browser using Outlook Web Access (OWA) or iNotes, both of which require a Web server such as IIS. This is an environment that has a vast number of vulnerabilities. See Table 2 for some examples.

Vulnerability	**Description**
Cross-packet attack	An attack distributed across multiple TCP/IP packets.
Directory traversal	“Traversal indicators” (../) following a valid path statement in the URL of a browser.
Path obfuscation	Replace an ASCII text string (that might identify their attack) with hex, double hex, or Unicode equivalents.

Table 2: Webmail vulnerabilities

According to CERT®, there have been 41 IIS-related vulnerabilities discovered since year 2000, three known OWA vulnerabilities since 2001 and three known iNotes vulnerabilities in 2003[2].

The impact of intrusion can be devastating to an organization. It can result in the loss of confidential information, exposure of user data, and the decline of user productivity as the email system becomes busy sending spam, and the email administration team works to resolve the issue.

To protect against intrusion, organizations must deploy solutions that meet the following security criteria: validate connections over POP3, IMAP4, HTTP and SMTP; prohibit access to the mail server over telnet and ftp; protect against buffer overflows (when a program or process tries to store more data than a buffer, or temporary storage area, can hold) than it was intended to hold.; defend against relay abuse; avert password cracking attempts, and provide a proxy for OWA and iNotes.

Denial-of-Service

A Denial-of-Service (DoS) attack is when a hacker intentionally tries to bring a mail server or MTA to a halt. Hackers use a myriad of different techniques to accomplish DoS, but typically they exploit vulnerabilities in a mail server such as the inability to deal with a malformed MIME message, or buffer overflow constraints.

[2] CERT/CC vulnerability database at http://www.kb.cert.org/vuls

They can also simply flood a mail server with more SMTP connections or SMTP instructions than the server can handle. Many mail servers and MTAs collapse under such attacks, either by crashing or allowing themselves to receive and execute unexpected commands which may be malicious in nature.

A DoS could have two main objectives. First, a number of hackers either find amusement in destroying an organization's email infrastructure and the ability to utilize email services, or they like to show off their capabilities to their "colleagues". Second, DoS can be a door-opener for hackers who intend to break into an organization's network, which is more important in the world of spam.

For corporations, the most obvious impact of DoS is the lack of availability and compromised integrity of mail servers. DoS on an Exchange or Domino server can lock out all users on that server. Additionally, a DoS attack on an Internet email gateway such as sendmail can result in Internet email delivery being halted. Depending on the email server configuration, this can affect both an organization's inbound and outbound traffic.

To protect against DoS, organizations must deploy a solution that accomplishes two goals. First, the Internet email gateway application should run on a hardened operating system to prevent DoS at the perimeter. Second, inbound Internet email packages must be scrutinized as payload for malformed messages and other threats to mail servers behind the DMZ.

Viruses and Worms

The proliferation of viruses and worms in Internet email has reached new heights in the last few months. A computer virus is a program that carries out a specific function and infects other computer programs in the process. There are essentially two classes of viruses: those that are designed to merely replicate themselves and those that are designed to destroy data stored on a hard disk, rendering the computer useless. A computer worm is similar, but does not infect other computer programs and is self executing. One of the most infamous worms is Sobig.F, which hit the Internet in August of 2003. It was a self-replicating worm that spread when unwary users opened file attachments in emails with subjects such as "Re: Details" "Thank You!" or "Re: That Movie." Once the attachment was opened, the worm resent itself to email addresses harvested from the infected computer's address book. The worm writer did not exploit any vulnerability in Outlook, but instead counted on the message recipients being deceived by the subject line. Sobig.F has been classified as the fastest replicating worm in history, outpacing Klez, LoveBug and Kournikova. Viruses and worms compromise the integrity and availability of email systems.

Traditionally, virus creators have been motivated by either demonstrating their skills within the hacker community, or simply satisfying their destructive minds. Spammers, on the other hand, are in business to earn money. As spam and viruses converge, virus creators start to see a financial incentive for their activities.

To protect against multi-faceted threats such as Sobig.F, proactive solutions that look beyond conventional message analysis are required. These next generation solutions must address all email threats, including anomaly detection to identify suspicious and unusual email patterns, create or automatically deploy email policies that address new threats, and deliver a rigorous security approach to ensure the integrity of the email infrastructure.

A Spammer's Toolkit

A few years ago, spammers did not have to worry whether their messages would arrive at the intended destination, as organizations had no spam protective measures deployed. However, the rapid increase in spam since then has convinced organizations to deploy countermeasures aimed at blocking spam before it reaches the recipient. New anti-spam measures have led to the development of new spamming techniques that fall into two categories- message content distortion and sending techniques.

Message Content Distortion

The first generation anti-spam tools typically looked for keywords such as "sex" or "enlargement," etc. in the subject or body of a message. Spammers quickly circumvented these anti-spam tools by breaking up the words with spaces or intentionally misspelling a word, like "s e x" or "seks." Anti-spam vendors responded with techniques that detected these new spamming methods, starting the cycle all over again with the spammers creating new, ingenious ways distorting the content of messages in order to trick the filters. With the proliferation of HTML, a highly flexible language that defines how text and images are displayed in email, Web pages and documents, spammers have found endless ways to trick anti-spam filters. Table 3 below list some of the most common message content distortion techniques that CipherTrust observes on a daily basis.

Technique	**Description**
Scramble text	Insert spaces or other characters, such as asterisks (*), to break up a word.
Invisible Ink	Insert words intended to throw off statistical analysis tools and use same color for text font as background (typically white text on white background) to hide the text when rendered by the email client.
Split words	Separate words commonly used in spam, such as Viagra, by interrupting them with HTML tags.
Letter randomization	Long garbage text strings designed to throw off message signature-based filters.
Character set encoding	Use base64 and quoted printable character set encodings to “hide” words from clear text format.

Table 3: Common message content distortion techniques

Sending Techniques

All it takes to send spam is software, an address list, a product or service to sell and an Internet connection. Typically, spammers will not operate their own mail servers, as it would be too easy to trace them. Instead, they sign up with any of the thousands of available ISPs, and once an Internet connection has been established, they can use several techniques to gain access and use the mail servers at ISPs and corporations that are not properly protected against intrusion. For some frequently used sending techniques, see Table 4.

Technique	**Description**
Open relay	A standard email server that allows anyone to connect to and distribute email, either by design or oversight. If the latter, the email server administrator has not correctly configured the server to prevent unauthorized resource access and usage.
Open proxy	A server that acts as an open relay but through TCP/IP ports other than 25 (used by SMTP). An open proxy provides communication abilities to other internal servers such as email servers. Open proxies provide a backdoor for spammers to access email servers that are otherwise protected from relaying.
Drive-by	Unprotected wireless LAN access points at organizations that unintentionally enable external parties to access internal corporate IT resources, including mail servers.
Drones	Unguarded PCs accessible over the Internet that are penetrated to install and activate SMTP server code to send spam at a level that is unnoticeable to the PC user.

Table 4: Common mail server access techniques

In addition to using mail servers from other organizations, spammers frequently masquerade their identity to appear legitimate by spoofing header information in an email message. Some of the most commonly spoofed header fields[3] can be found in Table 5.

Header Field	**Description**
Date:	The date and time when the mail servers communicated with each other.
From:	The sender’s email address.
To:	The recipient’s email address.
Received: from	The sender’s name and the reverse- DNS lookup of the sender’s IP-address. A “received: from” is added at each mail server hop the message passes along the way.
Return-path:	The sender’s desired email address for reply.
Content-type:	The type of attachments the message contains.

Table 5: Email message header fields

[3] For more information about Internet headers, see RFC821 http://www.faqs.org/rfcs/rfc821.html and RFC822 at http://www.faqs.org/rfcs/rfc822.html

Spammer's Software & Resources

There is no lack of tools for spammers to get into business. Several vendors offer bulk mail software, address lists and "tips&tricks" literature on how to send bulk email. For a feature list of various spam software packages, visit http://www.gammadyne.com/gm-comparison.htm.

There are numerous discussion groups on the Internet for spammers and hackers to exchange their experiences, ideas and code. Virus creators want to learn about spamming techniques for faster and broader distribution of malicious code and spammers are curious about virus techniques that help them stay under the radar and erase any trails of messages they send.

In essence, hackers and virus writers have finally found a profitable business where they can collaborate to increase their opportunities for success.

When Spammers Target Anti-Spammers

As anti-spam filtering tools are becoming more intelligent and effective at blocking spam, spammers have shifted their targets to the anti-spam service providers. Recently, spammers have conducted DoS attacks on servers at organizations that host blacklists for subscription, with the goal of making the blacklist provider inaccessible to its subscribers. Spammers can then target those subscriber organizations in a second stage of the operation. This last DoS technique has been quite successful, causing several blacklist providers such as Osirusoft and Monkeys.com to shut down their operations.

CipherTrust expects to see an increase in DoS attacks on anti-spam service providers. This will particularly hurt the blacklist providers that operate with limited resources and have difficulties securing their environment. Over time, more sophisticated DoS attacks will be aimed at hosted anti-spam service providers, threatening to potentially shut down their servers and expose their customers' email traffic.

The Evolution of Email Security Threats

Spam, DoS, intrusion, viruses and worms are today's email threats. CipherTrust believes email threats will evolve in three other areas: "Phishing", spamming viruses and perhaps not so much of a threat, but a development that will require action by any organization using email, regulatory compliance.

Phishing

Phishing, (also called "carding") is a scam that uses spam to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive information. Typically, the perpetrator sends out legitimate-looking emails appearing to come from a well known Web site, such as PayPal or Yahoo, in an effort to "phish" for personal and financial information from the email recipient.

Phishers use different social engineering and email spoofing tactics to trick their victims. The Federal Trade Commission (FTC) reported a case[4] where a 17-year-old male sent messages purporting to be from America Online (AOL) claiming a billing problem with recipients' AOL accounts. The email message contained AOL logos and legitimate URLs. However, when a recipient clicked on the "AOL Billing Center" link, he was redirected to a spoofed AOL Web page requesting personal information such as the user's credit card number, PIN, social security number, bank account number and password. A number of unsuspecting AOL users were deceived by this scam, losing both money and confidence in the security of their service provider.

As ecommerce and online banking continues to gain popularity, phishing incidents will undoubtedly increase.

Spamming Viruses

The convergence of spam and viruses will lead to spam attacks that spread faster and are harder to detect. Spammers will learn how to better masquerade the message origin and will create spamming infrastructures consisting of a number of hijacked computer hosts that will operate in tandem to trick anti-virus and anti-spam software. This was recently demonstrated in an attack against Spamhaus.org, a blacklist provider. They recently announced[5] that it was the target of a widely distributed DoS attack created by the W32.Mimail.E virus. The virus is designed to infect computers worldwide, instructing each affected computer to send overwhelming amounts of bogus requests to Spamhaus.org's Web server, www.spamhaus.org. The goal was to shut down Spamhaus.org's blacklist service.

Regulatory Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) provides legislation to protect the integrity, confidentiality, and availability of electronic health information. HIPAA, as it relates to email security, is an enforcement of otherwise well-known best practices that include:

- Ensuring that email messages containing confidential information are kept secure when transmitted from one point to another.
- Ensuring that email users are properly authenticated so that confidential information does not get into the wrong hands.
- Protecting email servers and databases containing confidential information.

HIPAA is to the healthcare industry as the Gramm-Leach-Bliley Act (GLBA) is to the financial industry. GLBA includes three simple requirements to protect personal data for individuals:

- Banks, brokerage companies and insurance companies must securely store personal financial information.
- They must advise their clients of their policies on sharing personal financial information.

[4] FTC “Identity Thief Goes “Phishing” for Consumers’ Credit Information”, July 21, 2003

[5] SPAMHAUS.org “Spammers Release Virus to Attack Spamhaus.org”, November 02, 2003

- They must give their clients the opportunity to opt-out of some sharing of personal financial information.

The requirements of HIPAA and GLBA have a direct impact on an organization's email usage. Email systems must be protected against intrusion, and email communications over the Internet must be conducted securely using encryption.

In wake of privacy as well as national security concerns, CipherTrust expects new federal regulations to be proposed that protect email communications for all types of organizations.

The Impact of Spam and Related Threats on Email Security

In this white paper we have discussed the email security threats that organizations are facing, both today and in the future. These attacks will become more sophisticated and more frequent as spammers, hackers and virus creators collaborate and discover new ways to profit from their activities. These threats are truly real and have a direct impact on the email security measures we defined in the beginning of this paper. See Table 6 for a few examples.

Security Measures	**Spam-Related Threats**
Confidentiality	Intrusion (mail server hijacking and email address harvest attacks)
Integrity	Intrusion, virus/worms, DoS (crashing email servers)
Availability	Spam floods, virus/worms attacks

Table 6: Security measures and their email threats

Spam Protection Today & In The Future

Any respectable anti-spam solution should detect and filter spam, but a more comprehensive solution is needed to address the overall email security threat. Protecting email servers from intrusion and being turned into spam-sending devices, and preventing corporate email directories from being harvested are also critical security concerns for organizations. The right solution should have the following characteristics:

- *Gateway Protection.* The solution should be deployed at the Internet email gateway, or if the solution contains an internet email gateway, in the DMZ.
- *Perimeter Security.* The Internet email gateway should prevent unauthorized access and run on a secure and hardened platform.
- *Extensible Protection Framework.* The solution should provide applications that can protect against today's email threats and should be easily extended with new applications against future threats.
- *Administrative Control.* The solution should work out-of-the-box, but must also be fully configurable to meet an organization's unique requirements.
- *Regular Update Service.* As email threats rapidly evolve, the solution should provide automatic updates at all levels including filter and application updates.

Finally, true protection is only as strong as the weakest link in the system - a fact that hackers and spammers have learned to exploit. Security conscious organizations must be aware of all the email-related threats and prepare to address them appropriately.

IronMail Is a Comprehensive Email Security Solution

CipherTrust's award-winning email gateway, IronMail, is an email security appliance designed from the ground up to provide high performance gateway protection for demanding messaging environments. IronMail is an innovative solution using the latest generation software. It is designed to evolve as new email security threats develop and can be tuned to meet the diverse needs of the enterprise.

To learn more about CipherTrust and IronMail, please visit our Web site at http://www.ciphertrust.com.

CipherTrust®

ENTERPRISE EMAIL SECURITY

www.ciphertrust.com