



Take Back Control of Your Email

Best Practices for Stopping Spam

White Paper

November 2004

Table of Contents

- Introduction 3**
 - Spam—A Growing Problem 3
 - Why Spammers Spam 3
 - The Cost of Spam and Viruses 3

- Evolution of Spam 3**
 - Phishing 4
 - Spoofing 4
 - Viruses 4

- Anti-Spam Strategies 4**
 - SMTP Layer Management 4
 - Virus Protection 6
 - Analysis Engine 6
 - Policy Enforcement and Regulatory Compliance 7
 - Per-User Controls 8
 - The Future of Spam Protection 8

- About Mirapoint 8**
 - Sharpening Your Defense Against Spam 8
 - RazorGate Email Security Appliances 8
 - Mirapoint Message Server Appliances 9

- Conclusion 10**

Introduction

Spam—A Growing Problem The Gartner Group estimates that between 60 and 75 percent of all incoming email is spam, which can cost a company with 10,000 employees more than \$13 million in productivity each year. In addition to loss of employee productivity, added administrative time, additional messaging infrastructure needed to handle the deluge of spam, response to viruses that spam often contains, and the legal consequences of offensive spam all impact the bottom line. Legislative solutions appear unlikely to solve the problem. Spam will only get worse. Organizations must protect themselves.

This document focuses on the challenges of spam and best practices for stopping it.

Why Spammers Spam

Spamming is a business, and spammers are in it to make money. Whether part-timers looking for some extra cash (the majority of spammers), or full-time operators, they send out millions of unsolicited emails hoping that a few recipients will reply to offers for merchandise. Most spammers work through affiliate programs as contractors, receiving a commission on sales generated from the spam, or on the number of leads brought to a website; i.e., click-through rate. Other spammers sell their own products. Nearly all spammers sell lists of email names they have “harvested” to other spammers.

Although response rates and profit margins are very small, so too are the costs. Start-up investment for purchasing huge lists and software programs (known as Ratware) to send millions of emails per hour may be less than \$1500. Even very low responses return a profit. The lure of spamming is simply too strong to resist.

The Cost of Spam and Viruses

The economic impact of spam on enterprises can be significant. Organizations suffer lost productivity as

employees spend time opening and deleting spam from their mailboxes each day. Productivity is also lost from downtime caused by spam-related viruses that turn computers into spam zombies. PCs become compromised by Remote Access Trojans (RATs) and are used by spammers to relay vast amounts of email without detection. According to Sophos, one-third of all spam currently circulating the Web is relayed through PCs that have been compromised by RATs. System administrators must “debug” each RAT-infested PC found, while the user waits—further reducing corporate productivity.

PCs that are infected with Ratware can pump out millions of spam. Combined with a steady flow of incoming spam, the added volume of emails can place a huge strain on enterprise messaging and network infrastructure. There is a cost to supporting this large message flow when heavy volumes of spam force IT to purchase additional bandwidth.

Even more costly, phishing activities by spammers (discussed in the following section) can lead to employee identity theft.

Beyond spam and viruses, offensive material and corporate exposure can create liability issues for enterprises. Organizations may find themselves legally liable for emails circulated internally that contain off-color or offensive material, resulting in costly litigation. Organizations may also face the unauthorized distribution of intellectual property when employees send out sensitive information that they shouldn't.

Evolution of Spam

Spam is continuously changing and evolving. No longer a simple solicitation to purchase merchandise, today's spammer is often after much more, including the theft of personal identity information and the

hijacking of unsuspecting users' PCs. Organizations have to learn to aggressively adapt in this escalating war where old solutions no longer work. Techniques used today by spammers include phishing, spoofing, and viruses that use hijacked PCs to distribute spam.

Phishing

Targeting businesses and consumers, phishing is one of the fastest-growing Internet scams. Phishers use spoofed email to provide links to counterfeit Websites that appear to be authentic banks or company sites. The spammer/phisher asks recipients to update or confirm personal or financial data associated with a credit card, bank account, or Social Security number. The phishers can then use that information for financial gain. According to the latest report from the Anti-Phishing Working Group, an informal organization that includes computer security companies, banks, and law-enforcement agencies, phishing attacks are growing at 52 percent per month.

Spoofing

Similar to phishing, users receive spoofed email that appears to have originated from one source when, in fact, it was sent from another. Email spoofing is often an attempt to trick the user into doing something the recipient shouldn't do, such as opening up an executable file attached to the email that contains a virus. It is easy to spoof email because SMTP (Simple Mail Transfer Protocol) lacks authentication. If a site has configured the mail server to allow connections to the SMTP port, anyone can connect to the SMTP port of a site and (in accordance with that protocol) issue commands that will send email that appears to be from the address of the individual's choice; this can be a valid email address or a fictitious address that is correctly formatted.

Viruses

Nearly one-third of all spam contains viruses (like Fizzer and Sobig). While the "mission" of these viruses may vary, the most common purpose is to enlist unsuspecting users' in their spamming efforts by turning computers into spam zombies.

Anti-Spam Strategies

Defending against spam requires a multi-layered approach, relying upon not one solution but a combination of solutions across the messaging infrastructure and at all levels. This approach to spam protection encompasses the SMTP layer, virus protection, an analysis engine, content filtering, policy management, and per-user controls.

SMTP-Layer Management

Experts agree that the cost of spam and viruses is higher the further they penetrate into the enterprise's network. If spam or viruses pass the perimeter, network resources are affected due to the volume of data transported. If they get into the message store, they can consume disk storage resources and processing overhead. If they get to the users' desktop, employee productivity will suffer and IT will be forced to deal with removal of viruses.

EDGE PROTECTION

An SMTP connection is the front door to an organizations messaging infrastructure. Spam and viruses are free to enter unless some mechanism is deployed to challenge them. An organization needs a first layer of defense for dealing with unwanted email before messages get passed on to the firm's other anti-spam and anti-virus filtering systems. The technology should only accept messages from verified senders and valid mail servers. Once a valid system is identified, it automatically bypasses the SMTP security layer in the future.

CLOSED RELAY

Once, virtually every mail server was an Open Relay, allowing the third-party relay of email messages through those servers, and opening themselves up to spammers using their mail server to propagate spam. Today, there very few Open Relay mail servers remaining—mostly outside the US. However, organizations should make sure that their mail servers are not Open Relays.

IP AND DNS BLACK AND WHITE LISTS

Messaging systems should be able to create lists of IP addresses, domain names, and individual email addresses from which no mail will be accepted (black lists), or lists that are trusted and accepted without passing through filters (white lists). When an email address or domain is added to a black list, an email that matches the return email address or the sending domain should be automatically tagged as spam, regardless of whether the message would have triggered the spam scanning engine based on content.

SENDER AUTHENTICATION

Enterprise messaging systems should utilize Sender Policy Framework (SPF) to control spam. SPF is an extension to SMTP that makes it easy to counter most forged “From” addresses in email, thereby countering spam. Normal SMTP without SPF allows any computer to send email claiming to be from anyone. Thus, it’s easy for spammers to send email from forged addresses. This makes it much more difficult to trace back to where the spam originates from, and easy for spammers to appear to be senders the receiver would ordinarily trust. SPF makes it more difficult for spammers to send spam, because if they simply forge a “From” address from an address that implements SPF, receivers that implement SPF will know to ignore the message.

SMTP-LEVEL ENCRYPTION

Ensuring secure communications with partners or remote employees is critical. STARTTLS should be supported to enable an SMTP session to be encrypted upon request by the server sending the email. Transport Layer Security (TLS), which utilizes Secure Socket Layer (SSL) encryption technology, can provide authentication (e.g., identification of the communication partner), privacy (e.g., ensure the message is not intercepted), and integrity (e.g., make certain the message is not modified).

DIRECTORY HARVESTING PROTECTION

Spammers use a variety of software tools to discover or “harvest” email addresses from corporate messaging systems, such as bombarding email systems with thousands of generated email addresses hoping to find some matches. Messaging systems should be able to prevent email addresses from being harvested by checking the validity of the recipient at the edge and targeting obvious directory harvesting and dropping email from unknown recipients. In addition they need to verify that their edge message transfer agent (MTA) has disabled SMTP commands such as VRFY and EXPN. In situations where directory harvesting is indicated, the system can progressively slow down SMTP connections until the connection becomes unusable to the external IP address.

RBL SUPPORT

These systems should be able to use Realtime Blackhole Lists (RBLs), commercial lists of networks that either allow spammers to use their systems to send spam or have not taken action to prevent spammers from abusing their systems, to block spam from entering their messaging system. A real-time blackhole differs from a blackhole list in that it keeps track of addresses known to send spam or host spammers. Enabling such a list results in all mail from those addresses being refused or tagged based on the administrators preferences, including valid email.

PASSWORD PROTECTION

The system should be able to help ensure password protection and prevent directory harvesting through alerts that advise IT personnel when an external party is using the system as a proxy, when multiple failed logins occur, or when messages are sent to user names that don't exist on the system.

Password protection should also provide protection against outbound spam, and PC zombies, through a "sender is valid recipient" feature. By asking for SMTP authentication of each session, only authorized users can send mail. Zombies, which do not know the user's password, will be unable to initiate spam, and mail can be forced to have legitimate rather than forged email addresses.

Virus Protection

Spam and viruses are inextricably linked. It is estimated that 99 percent of email viruses are designed to send spam from users' computers. Viruses can target corporate networks looking for email addresses and passwords and hijack PCs to send out millions of spam messages on behalf of the spammer. It is useless to deal with spam protection without also dealing with virus protection. Messaging systems must be able to clean, discard, or quarantine messages that contain viruses.

Analysis Engine

Using heuristic and lexical rules-based scanning, the system should analyze messages at the server level based on information in the header, envelope, subject, and message, and then score the risk accordingly. The spam engine should optionally be able to query Vipul's Razor to match suspected spam signatures. If the score exceeds a defined threshold, which can be adjusted by both administrators and end-users, the message can be tagged as spam and the appropriate action taken on the message.

Scoring is typically done only once, at the server level, increasing performance and throughput. Evaluation of the scores should be done at both the domain and user levels. In a secure system, tagging and filtering are hierarchical; i.e., domain filtering can be more restrictive than system filtering, and end-user filtering can be more restrictive than system or domain filtering. An end-user, for example, can set their spam threshold to a more restrictive setting than the system threshold.

The system should have easy-to-use tools that allow IT managers and end-users to identify spam and report newly identified spam characteristics. New spam rules can then be created that are automatically provided to customers via network-based updates.

VIPUL'S RAZOR

Sources of spam are continuously changing. To detect spam, black lists must change as well. Vipul's Razor is a distributed, collaborative spam detection and filtering network. Through user contribution, Vipul's Razor establishes a distributed and constantly updated catalogue of spam in propagation that is consulted by email clients to filter out known spam. Detection is performed with statistical and randomized signatures that efficiently spot mutating spam content. User input is validated through repudiation assignments based on consensus on report-and-revoke assertions that is, in turn, used for computing confidence values associated with individual signatures. To effectively block spam from their messaging systems, organizations should have a system that uses the signatures stored on the Vipul's Razor site to mark a message as spam.

VELOCITY-BASED ARRIVAL

In addition to Vipul's Razor, messaging systems should also be capable of supporting Velocity-based Arrival technology. This technology continually gathers signatures of emails being sent from around the world and forwards them to a central collection point

for analysis. Using sophisticated algorithms, the technology can differentiate legitimate bulk mail from spam based on the arrival time of messages from multiple sources and notify messaging systems of spam attacks within seconds.

CUSTOMIZABLE TAGS

A good spam protection system should be able to label spam messages in the header, and optionally in the subject line, notifying recipients that the message has been determined to be spam.

CONTENT FILTERING

A truly secure system should enable both end-users and IT staff to define and customize spam protection. Black and white lists should exist at both the user and domain levels to trigger filter actions just as if the message was (not) spam. End-users, for example, should be able to develop their own black and white lists and create personal filtering rules. IT managers should additionally be able to adjust the spam threshold to optimize it for their organization's message traffic and develop unique domain or system-level black and white lists based on the email sender.

Content filtering increases the spam catch rate, but at the same time it also helps users manage their mailbox. Users, for example, should be able to manage how incoming messages are handled through customizable rules. Filtering should be done by message body, header, subject, as well as the "to," the "cc," the "from" field, and the "reply to" field. Based on that information, users can then initiate a custom action by message, such as sending to a specific folder, deleting, forwarding, or copying. Messages could be quarantined; i.e., placed in junkmail folder or administrator folder for analysis.

Key sample content filtering features include wiretaps, blocked address filters, blocked message filters, blocked attachment filters, redirected

attachment filters, corporate word list filters, and objectionable word list filters.

TRUSTED PARTNER WHITE LISTING

Organizations may have established relationships with customers, partners, and vendors whom they wish to receive emails from without content filtering. A messaging system should enable companies to establish white lists of trusted organizations.

Policy Enforcement and Regulatory Compliance

Organizations must be able to protect themselves against liabilities relating to the dissemination of offensive materials or the unauthorized distribution of intellectual property. Flexible content filters allow enforcement and creation of corporate policies, and can provide powerful management tools for the end-user. The ideal system should be configurable at the domain level or by the end-user allowing actions to be taken based on content embedded in the header, body, or attachment of a message.

Systems should also have pre-defined content filters to make policy enforcement easier for the administrator. Such policy enforcement tools can help companies manage employee email usage, prevent sensitive information leaks, address regulatory compliance requirements, and protect against harassment and other types of email abuse.

Based upon policies, the system should be able to remove or "strip" objectionable attachments from messages including JPEGs, encrypted documents, and Visual Basic Scripts (.vbs), Program Information File (.pif), and Screen Saver (.scr). Systems should also provide wiretapping capabilities to store copies of messages transparent to the user.

Per-User Controls

Individual users should be able to customize the level of spam control. An end-user, for example, should be able to set their spam threshold to a more or less restrictive setting than the system threshold, create their own black and white lists, and choose where emails are sent; i.e., to a folder or cell phone.

The Future of Spam Protection

One of the biggest issues facing anti-spam efforts are computers that have been taken over by hackers and used to send spam without the owners' knowledge through worms or viruses, themselves embedded within spam. Spammers also have other means of taking over other user's computers, such as hijacking mis-configured web proxies and email relay servers. These attacks often succeed because email recipients have no reliable means of authenticating the sender of a message. A new defense in the war against spam is Sender Auth.

Two technologies have been developed for sender authentication. The first is IP authentication, in which the receiver authenticates the sending computer using the sender's IP address. This was developed from Sender Policy Framework (SPF), authored by Meng Wong, co-founder and CTO of Pobox.com.

The other technology is cryptographic authentication of the contents of a message. The leading example of cryptographic authentication is DomainKeys from Yahoo. Organizations should look for messaging systems that will support Sender Auth.

About Mirapoint

Mirapoint is the only vendor in the industry with complete, end-to-end email and security solutions for any size organization. The RazorGate email security appliances are designed to complement any mail

server with multi-layered protection at the network edge. The Message Server is designed to support any enterprise, service provider, government or education customer trying to deliver email to a broad base of users that demand anytime, anywhere access to carrier-grade email services.

Sharpening Your Defense Against Spam

Mirapoint provides powerful, Full-Spectrum technology to block spam, including capabilities for blocking known users and domains and support for real-time blackhole lists. Mirapoint offers personalized spam controls, such as individual black and white lists and content filters, so end-users can better manage their incoming email and define what is and what is not spam. For additional spam defense, Mirapoint supports Simple Mail Transfer Protocol (SMTP) authentication to guarantee only approved users can send email through the Mirapoint gateway. Mirapoint's integrated anti-spam features dramatically improve overall email performance and system reliability by reducing the resources wasted on unsolicited emails.

RazorGate Email Security Appliances

The family of RazorGate™ Email Security Appliances provide the best spam, hacker, and virus protection in a remarkably easy-to-use design that can be deployed in minutes to secure hundreds to millions of mailboxes.

The RazorGate appliance offers DirectPath™, a patent-pending technology that allows real-time scanning without having to worry about queue management or storage and backup of mail in a queue. With DirectPath, the MTA guarantees that no inbound messages are lost. The MTA does not allow a message to be acknowledged as being accepted by

the RazorGate appliance until the message has been fully delivered and acknowledged by the recipient mail server.

This concept is similar to a two-phase commit process in the database world. If a RazorGate appliance were to lose power, any message that was in process by the RazorGate appliance would never have been acknowledged as being accepted, and delivery would be re-attempted by the sending server using standard SMTP behavior.

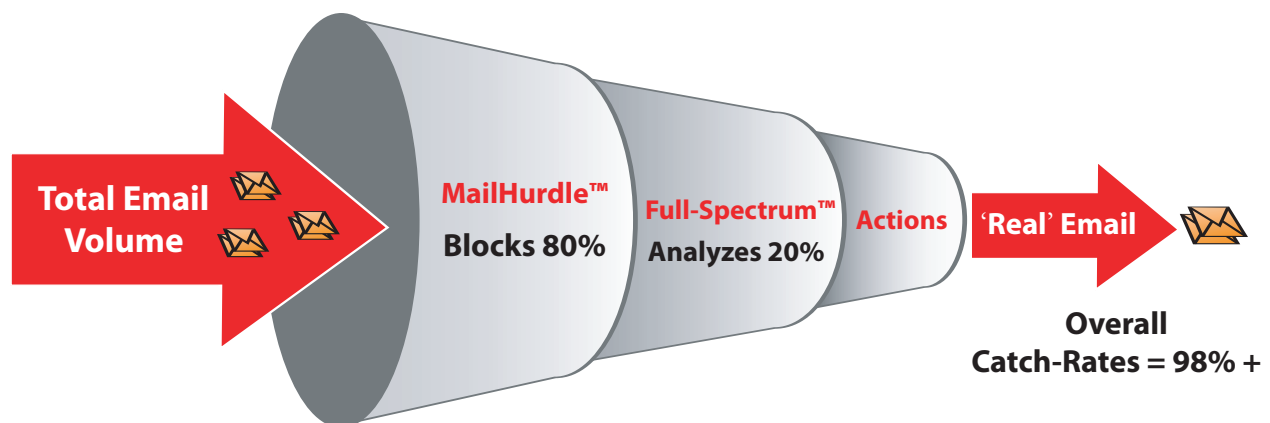
For administrators that require a message queue, an option that includes queue and queue management tools, as well as integrated LDAP-based routing capabilities, is also available.

Mirapoint's MailHurdle (see Figure 1) technology provides an industry-leading approach that drops up to 80 percent of threats at the network edge before network bandwidth, storage, processor, and administration resources are wasted. In combination with Mirapoint's Full-Spectrum email security technology, customers can achieve overall catch-rates

of 98 percent with virtually zero false positives. Automated updating provides the latest and greatest protection against new and evolving spam threats.

Based on the RPD technology licensed from Commtouch, Mirapoint's Rapid Anti-Spam technology uses information collected on a global basis from network probes to identify spam and virus outbreaks in real-time. With Rapid Anti-Spam, no updates or ongoing maintenance is required and customers can be confident they have a security defense in place that is impervious to future attacks and evolving techniques exploited by spammers and many virus writers. Furthermore, since the intelligence behind Rapid Anti-Spam is based on real-time outbreak information not analyzing individual message content, the approach delivers zero false-positives, works with any type of message content and language, as well as effectively distinguishes between legitimate bulk mailing and spam. Rapid Anti-Spam is tightly integrated into Mirapoint's secure, hardened appliance platform for performance and reliability optimization, as well as simplified management made possible with Mirapoint's existing unified management tools.

Figure 1: Mirapoint's Unique MailHurdle™ Technology



Mirapoint Message Server Appliances

The Mirapoint Message Server appliance offers the lowest TCO in email server solutions while maintaining high performance and reliability. The message server offers a rich set of features including desktop email as well as web and wireless access with group calendaring, shared folders and an address book. It also contains the same email security technology as RazorGate to block spam, viruses, and hacker attacks.

Conclusion

Today's organizations must find ways to protect themselves and their email systems from spam and viruses, while also addressing increasing regulations governing email traffic.

Mirapoint's next-generation solution delivers a comprehensive, integrated, multi-layered approach to defending against spam and viruses with purpose-built components tailored to meet the continually evolving threats and economic impact spam and viruses represent. Mirapoint's feature-rich systems are designed for quick and easy rollout of spam, virus, and policy enforcement features. Mirapoint backs up these features with high availability, scalability, reliability, and world-class performance.

Mirapoint additionally provides seamless integration with existing infrastructure, while powerful centralized management capabilities help manage costs and simplify administration, enabling the deployment of spam and virus protection throughout the network with ongoing updates. If you are looking for increased protection against spam and viruses, Mirapoint is the right solution.

For more information on how Mirapoint can reduce spam and improve the security of your message network, visit our Website at www.mirapoint.com, or call us at 408-720-3700.



Mirapoint, Inc.
909 Hermosa Court,
Sunnyvale, California 94085 USA
Tel: 800-494-8965
Tel: 408-720-3700
Fax: 408-720-3725
email: info@mirapoint.com
www.mirapoint.com

For local and international office locations
please see www.mirapoint.com

© Copyright 2005 Mirapoint, Inc. Mirapoint, RazorGate, MailHurdle, Rapid Anti-Spam, MessageBase, Full-Spectrum, Messaging Operating System, DirectPath, DirectAccess and logo are trademarks or registered trademarks of Mirapoint, Inc. WP-Spam-0205