

Postini® White Paper

Email Intrusion Prevention: Stop Malicious Threats before They Harm Your Email System

Spammers and Hackers Shifting Tactics

Junk email or spam and email borne viruses are a problem. A big problem. Nearly every organization has experienced the frustration of spam and unwanted emails clogging their email inboxes, and the latest email borne virus threatening to bring down their networks. Many are attempting to respond by purchasing anti-spam appliances, software, or desktop products to implement an in-house solution. Meanwhile, the spammers and hackers who make a habit—and a business—out of exploiting the vulnerabilities in our email communications systems have not been idle.

Techniques such as "hash busting" and Bayesian Poisoning have become familiar to most anti-spam vendors and countermeasures incorporated into their products. However, spammers are becoming even more covert in their tactics these days. Going beyond fooling anti-spam filters with creative subject or word combinations, spammers are taking a more personalized as well as a minimalist approach to get past content filters.

The logic behind these new spamming techniques is simple: take away or reduce the context of a message to a degree that confuses the content filtering method just enough to allow a message to get through. Because anti-spam products must handle messages for hundreds or even thousands of users, it is difficult for the IT departments to increase the sensitivity of these filters to catch these techniques. That's because increasing filter sensitivity also increases the risk of blocking substantial numbers of legitimate emails—known as false positives. (See Postini White Paper "Shifting Tactics of Spammers" June 2004 at www.postini.com)

The New "Silent Killer" Email Threat: Directory Harvest Attacks

During the first half of 2004, spammers and hackers have gone beyond message content gimmicks to focus on the SMTP or Port 25 connection point in their endless quest to overcome content filtering technology. Spammers are now launching what are known as directory harvest attacks (DHAs), designed to net spammers lists of valid email addresses to which they can send more spam or sell to other spammers.

You and your users have probably already seen the symptoms of directory harvest attacks. For example, have your end users complained about how slow your email system seems when you have no visible reason for performance problems? Have your end users asked you why they are getting completely blank messages? Or, have you observed sudden bursts or spikes in activity on your email system that last just of few minutes and subside for no apparent reason? Are your Microsoft Exchange or Domino server deferral queues constantly full, slowing server performance and delaying message delivery?

In a directory harvest attack, spammers, and unscrupulous list brokers exploit email systems by sending thousands (or even hundreds of thousands) of messages to multiple addresses such as johndoe@yourcompany.com, or jdoe@yourcompany.com. Spammers track all of the addresses that do not bounce back or generate errors, and consider these valid addresses. These valid addresses are then compiled into lists that are sold or distributed to other spammers.

Directory harvest attacks also have a very damaging side effect: consuming enormous amounts of email server resources while email servers try to cope with DHA probes. Lotus Notes and Exchange servers, for example, generally accept all messages for their domain by default. This only aggravates the negative impact of a directory harvest attack because the spammer assumes all the attempted addresses are valid, and thus will send more spam or sell the attempted addresses to others. Even worse, for every attempted delivery, Domino and Exchange systems generate a Non-Delivery Report (NDR). Thus, every DHA attack can produce thousands of NDRs that clog server message queues and slow email server performance to a crawl—creating the equivalent of a self-inflicted Denial of Service attack on your own email system.

Trying to Manage New Email Threats In-house is a Losing Battle

In most cases, conventional approaches to SMTP perimeter protection, such as IP address blocking that rely on known spammer addresses, are no longer effective in blocking these attacks since most spammers now use a rapidly changing range of IP addresses to distribute their email attacks. While it's possible to get updated blacklists from vendors, by the time a suspect IP address is identified and incorporated into the filtering software, the spammer has attacked, harvested and moved on. Even worse, valuable server cycles have been wasted in a vicious cycle of response and bounce back messages, and NDRs.

In one dramatic example, a public media company saw their email traffic surge early in 2004—at times growing by 10,000 emails a day as a result of DHAs. Attempting to deal with the problem using an anti-spam appliance, the company's email infrastructure was simply overwhelmed. "It was like trying to drink from a fire hose," according to the firm's vice president of information technology. The company was forced to add inbound and outbound email servers to handle the increasing traffic and because of NDRs caused by the directory harvest attacks, its outbound email queue was constantly full, resulting in email delivery delays of up to 45 minutes.¹

Content Filtering Alone Can't Cope

Unfortunately, directory harvest attacks cannot be stopped by conventional content filtering found in appliances or software since there is no "content". Nor can spam messages that reduce or eliminate "content" in a message be reliably blocked by content filtering without the risk of increasing false positives to unacceptable levels. In short, the conventional approach to blocking spam and viruses through content filtering inside the email gateway is no longer sufficient for coping with newly evolved spam and hacker tactics.

That's because by its very nature, conventional anti-spam and anti-virus filtering whether at the desktop or on email servers is reactive, rather than preventive. Anti-spam software and appliances must accept all email traffic, store it on a server and then examine it or filter it to identify and

block suspicious or malicious messages. The burden this approach places on your IT staff and email infrastructure is both frustrating and costly. Companies are spending millions of dollars in valuable IT staff time and email infrastructure resources attempting—and far too often failing—to stop intrusions from spam and email borne viruses. That's in addition to the millions and perhaps billions of dollars in lost employee productivity...time wasted sorting through and deleting unwanted messages.

Problems with Reactive Approach of Conventional Content Filtering

Given new spam and virus techniques and directory harvest attacks, the limitations and disadvantages of conventional content filtering have become apparent on several levels:

Additional Email Infrastructure Costs:

Experts estimate that the growth in spam traffic now requires companies to budget anywhere from 5 to 10 times the amount of messages on their email servers that they might normally expect. That means additional in-bound and out-bound email servers that must be bought, maintained, tuned and patched.

Excessive Demands on IT Staff Time:

Valuable system administrator time must be taken up with keeping content filtering systems maintained, and updated. Black lists and white lists must also be updated. In many cases, content filtering relies on Bayesian formula techniques that must be "educated" as to what constitutes

spam. As soon as the content filter learns of one technique, however, the spammers have already moved on to new methods. It's an endless game of catch up that you can never win.

Email Queue Backups and Delivery Delays:

As noted earlier, directory harvest attacks can create literally thousands of incoming (harvesting probes) and outgoing messages (NDRs) during the day. When deferral queues become overloaded, system performance and availability are jeopardized. Legitimate messages get held up in the queue and productivity suffers.

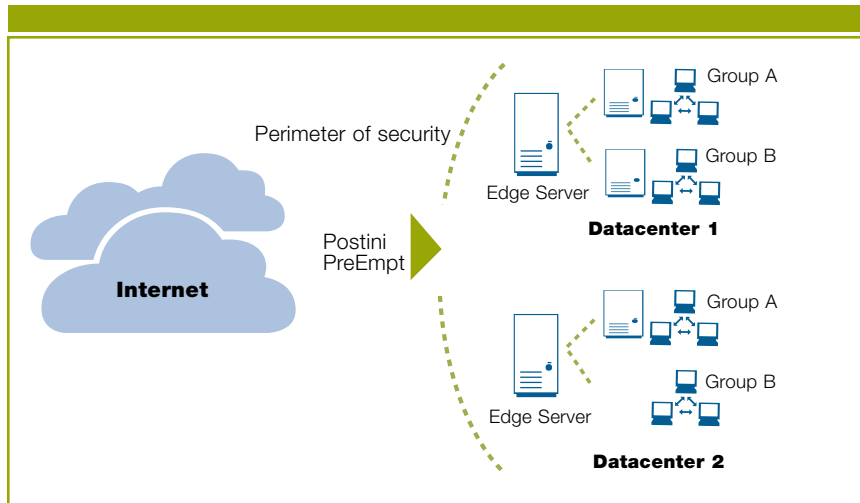
Unwanted Complexity:

Many organizations have a mix of email platforms inherited through mergers and acquisitions over time. In some cases, organizations have been forced to devote staff just to deal with a variety of user desktop products and/or to maintain content filters on a variety of appliances and server platforms.

Bottom Line: Reactive Approach to Email Intrusions is Costly and Inefficient:

There is a bottom line to all of these problems—although appliances and desktop or server software filters may have worked in the past, your email systems are constantly being hit with new modes of attacks at a faster rate than ever before. Reactive approaches that rely solely on content filtering have rapidly become both costly and inefficient.

Figure 1 Postini resides between the Internet and your network email servers, preempting email threats before they reach your infrastructure.



Clearly a more proactive approach is necessary; an approach that focuses on email intrusion prevention as the optimal method for avoiding the problems experienced with conventional content filtering. As you will see, a preventive approach to email threats and intrusions ends up being both more efficient and much more effective.

Beyond the Reactive Approach: Postini's Email Intrusion Prevention System

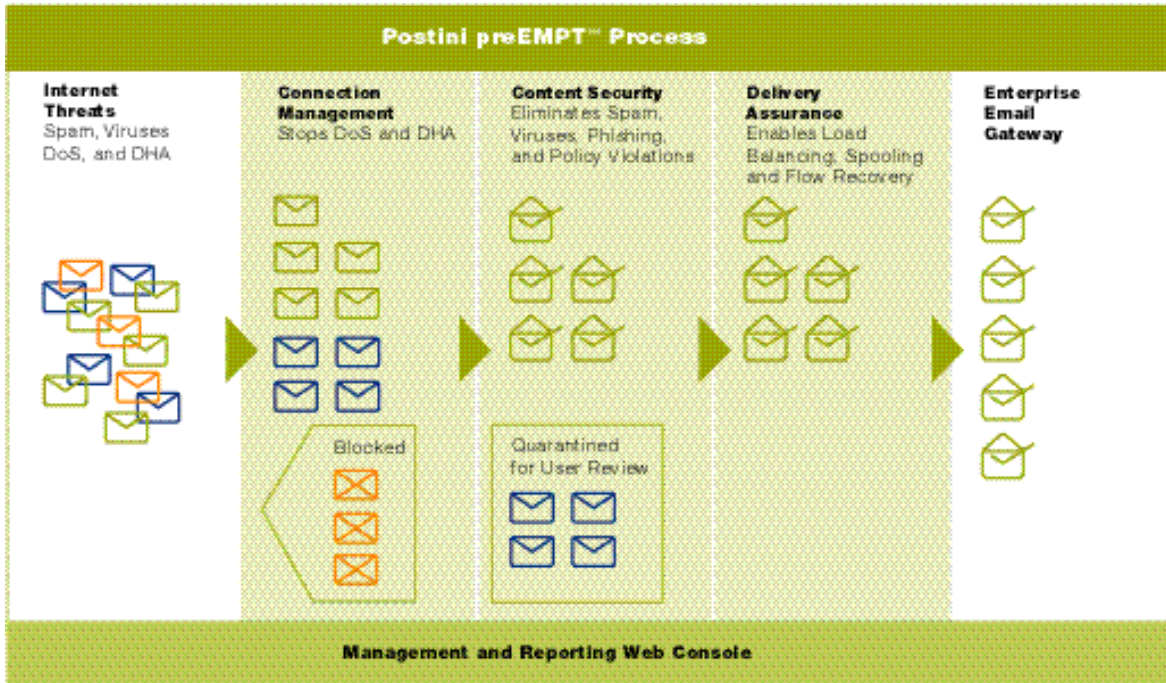
Email intrusion prevention overcomes the problems of relying solely on content filtering by moving the battle against spam and viruses outside of your email gateway and network perimeter. In this way, spam and new email threats are effectively dealt with before they have a chance to impact your network. That means utilizing a managed service such as Postini, the world's first and largest email security and management service, to stop threats outside the network perimeter—between the Internet and your network mail servers—analyzing and filtering all messages before they reach your enterprise.

Postini's patented pass-through technology processes email in real-time, through a highly secure system architecture that operates with no detectable latency, no data loss, and no security compromises. Legitimate email is instantly forwarded to each customer's destination mail server from memory. Depending on customer preference, suspicious email is either tagged and delivered or quarantined to a web-accessible storage area for client review. (See Figure 2)

Stopping New Threats Dynamically at the Connection Point

Email Intrusion Prevention means identifying and blocking malicious or suspect behavior before it can ever reach your email gateway. In the email environment that means identifying and blocking suspect messages by IP address origin at the SMTP connection point (Port 25) in real time. Note this can only happen if your organization is using a managed service such as that provided by Postini.

Figure 2 Postini's patented preEMPT™ process eliminates threats at the SMTP connection point, filters content to remove or quarantine spam and suspect emails, and assures proper delivery of messages.

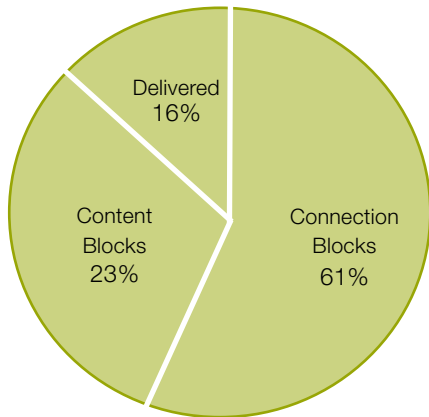


During pass-through processing, messages are examined at the SMTP connection point using patented IP analysis to determine if their behavior exhibits the characteristics of spam or

a virus threat. Up to 50 percent of all messages coming in through the Internet at this point are blocked, without Postini ever having to examine the content of such messages.

How can so much traffic be eliminated right off the bat? This is possible because Postini's patented technology is capable of examining the behavior of the sending computer in real time based on more than two-dozen variables. Postini maintains a real time inspection of every IP address that connects through its managed service. Based on this analysis, certain SMTP connection patterns are indicative of malicious behavior, enabling Postini to block connections without seeing the actual message. In fact, Postini's patented preEMPT technology is the only commercially available solution that can effectively block DHA, DoS attacks, and spam messages containing little or no content in the message.

Figure 3 Postini is able to block more than half of SMTP connections without looking at the message—something content filtering technologies cannot do.



APRIL, 2004

Source: 400 million SMTP connections handled by Postini

Processing more than 400 million inbound SMTP connections every day from 10 to 15 million distinct IP addresses, Postini currently blocks more than half of SMTP connections without having to rely on filtering the message content. (See Figure 3)

Because of its vast experience observing hundreds of millions of delivery attempts from millions of IP addresses, Postini is able to analyze traffic patterns and connection behaviors from a global perspective. Thus, Postini customers gain the advantage of a vast pool of spam and virus intelligence that each customer individually could never hope to attain, even by subscribing to software updates.

Once an SMTP connection is validated or the sending IP address has not been identified as having engaged in recent damaging behavior, the message data is passed through Postini's Content Security (Figure 2) process, filtering messages to eliminate viruses and spam using thousands of rules, or heuristics, constantly updated by Postini to reflect new spam types. These new rules are always immediately available to customers without the need for their IT staff to download or install any software.

Finally, Postini's Delivery Assurance (Figure 2) capability ensures that legitimate messages are delivered in a way that helps email servers perform at peak efficiency. Postini helps to balance inbound message loads across multiple email hosts, regardless of the email hosts' geographic location or operating system. Postini can also identify server outages, alert the administrator, and

automatically spool messages so that no email messages are ever bounced. Postini stores the spooled messages until servers are once again able to accept messages.

Security and Privacy Ensured by Pass-Through Technology

One unique advantage of Postini's patented method for processing email messages over other managed service providers is Postini's exclusive "pass-through" technology. Other managed service vendors accept all messages and store them on disk. The messages are then analyzed and forwarded to the customer. This storing of messages can create security and privacy risks that are a legitimate concern for IT managers.

Postini, in contrast, conducts all analysis of SMTP connections and of messages in real time, so that no messages get stored but rather legitimate emails are instantly passed along to their rightful recipients. This eliminates any concerns about privacy and security, especially for those customers in highly regulated industries such as financial services and healthcare.

Email Intrusion Prevention Advantages from Postini

Postini now offers companies email intrusion prevention through a comprehensive email security and management service that delivers several critical advantages over conventional, reactive appliances and software products.

- Provides an Email Intrusion Prevention System based on patented, real time IP analysis processing more than 400 million inbound SMTP connections every day from 10 to 15 million distinct IP addresses.
- Stops new and evolving threats such as Directory Harvest Attacks and Denial of Service attacks at the SMTP (Port 25) connection point before they can impact your network. This can reduce your email traffic by thousands of messages per day.
- Prevents spam and email borne viruses from ever reaching your email gateway, including minimal and no content spam messages.
- Delivers Email Intrusion Prevention services through a unified email security platform that provides a common management interface, along with real time monitoring and reporting. Compatible with all email servers and operating systems.
- Assures the fastest, most up to date IP analysis and content filtering rules to combat newly evolving threats.

Email Intrusion Prevention ROI

How do you realize a return on your investment from an email security solution? When you move from a reactive approach that relies solely on content filtering to one that is preventive, the payoff becomes clear in terms of reduced costs and increased efficiency and effectiveness.

Pays for itself with lower infrastructure costs.

By keeping spam, email borne viruses and attacks from ever reaching your email servers you can eliminate or avoid purchasing additional servers since email traffic is significantly less. In one recent example, a company was able to eliminate 4 email servers after the Postini email security and management service was activated.

Relieves the administrative burden on IT staff.

By eliminating the burden of maintaining your own in-house anti-spam infrastructure, your IT personnel are free to devote more time to supporting business objectives, and concentrating on revenue enhancing tasks.

Restores productivity of users.

Beyond the direct cost savings for email infrastructure and IT staff timesavings, Postini's email protection service more than pays for itself with improved productivity by all users. In some cases, Postini's email protection service has saved individual workers as much as a half-hour to an hour each day.

Eliminates the complexity of managing and maintaining products in-house.

Because the Postini email protection service operates outside of your network, there are no internal management or infrastructure issues to deal with. The service can be activated in days with only minimal IT time required on your part. And, it works regardless of the mix of email platforms or operating systems in the customer's environment.

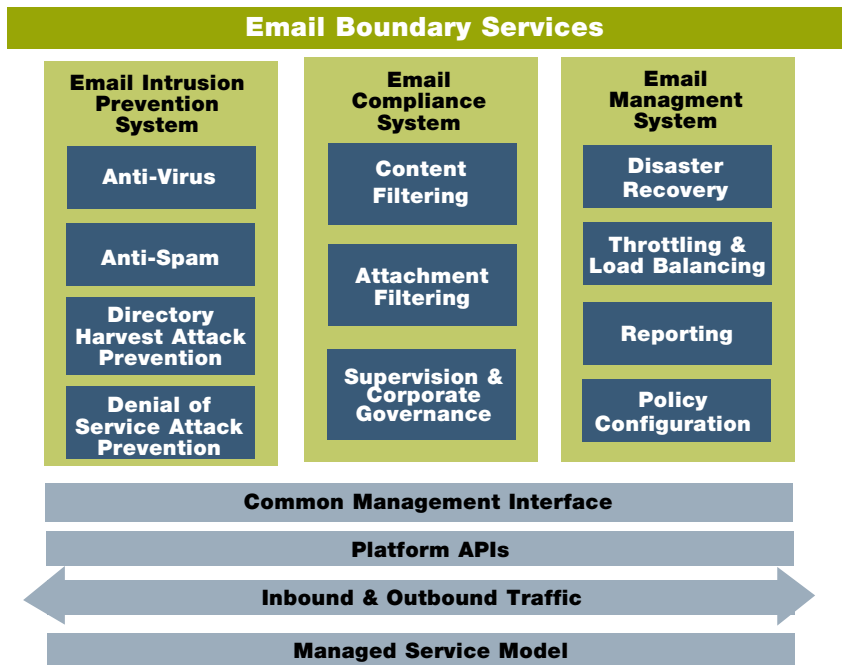
Minimizes the risk of email system performance degradation or failure

Since intrusions from spam, email borne viruses and directory harvest attacks never reach your email gateway, your network cannot be overloaded or comprised from these threats. The financial benefit from avoiding email slowdowns or system downtime adds up very quickly. As long as email communications continues to be a vital part of doing business, its contribution to top line revenues and productivity cannot be overestimated.

No Reason to Struggle with Costly and Inefficient Reactive Approaches

Michael Osterman of Osterman Research, a firm that helps organizations understand the markets for messaging, directory and related products, recently wrote in *Network World's Messaging Newsletter* that "Spam is very definitely a game of cat and mouse in which the mouse is getting smarter at evading the cat." He noted that many anti-spam content filtering systems in use today require IT staff resources to maintain filters and keep up with what spammers are doing to circumvent them. ²

Figure 4 Postini's comprehensive email security and management services secure your email boundary through email intrusion prevention, policy compliance and email system management services.



The bottom line," he concluded, "is that spam control, virus control and related activities should require a minimum of IT staff time to maintain, since eliminating this junk from your e-mail is simply treading water; no matter how well you do it, it adds no competitive value to your organization."

As one VP of Information Technology fighting on the frontlines of the email communications battlefield noted, "We were looking for a way to fight this war on someone else's territory. The whole idea of Postini keeping spam and viruses completely off our system is very appealing. We are committed to keeping our IT resources focused on growing revenue and shareholder value, and there's simply no business value in trying to manage spam and email attacks internally...believe me we tried it for almost a year. If I can push the spam and junk email problem out to an expert like Postini, that's a huge win for me and my staff," he said.

"An internally hosted anti-spam appliance or software doesn't solve the problem of NDRs, directory harvest attacks or virus attacks. In my wildest dreams I can't imagine anyone who would want to try and manage spam and email threats internally...not when you've got a managed service like Postini as an alternative," he concluded.

Securing Your Email Boundary: More than just a "spam" problem

Because of the harmful impact from Directory Harvest Attacks and other newly evolving spam tactics on email system performance, these threats must be treated as more than just an email inbox or end user annoyance issue.

Email security and management must become more than spam blocking in order to properly protect your email boundary and keep your email system at optimal performance levels.

As such, Email Intrusion Prevention is only one aspect of a complete email security and management service offered by Postini. As seen in Figure 4 below, Postini helps secure your email boundary with unmatched services at three critical levels. (See Figure 4).

First, as described in this white paper, Postini provides unmatched Email Intrusion Prevention through its patented preEMPT technology that provides protection from spam, email borne viruses, Denial of Service and directory harvest attacks. Second, Postini helps enforce email system compliance through content and attachment filtering for both inbound and outbound email traffic. Third, Postini helps you improve your email system management through proper configuration, analysis and reporting, load balancing and disaster recovery services.

References:

(1) Telephone interview with Mark McKeen, VP of Information Technology, Jefferson-Pilot Communications, August 3, 2004.

(2) "Blocking spam gets harder for some," by Michael Osterman, Network World Newsletter, 8/10/04.

The Email Communications Utility Analogy

The concept behind Postini's preemptive email protection system corresponds to the analogy of your water utility. Imagine if homeowners had to build their own water filtration system in the backyard—constructing and maintaining it—in order to assure decent quality drinking water. Or, if they tried to put filters on every intake and faucet in the house to ensure clean water. The cost of doing it themselves would be staggering...and the process totally inefficient. Instead, homeowners rely on a utility as the experts to clean and purify water at a filtration plant that supplies water for home consumption—and they pay only for the water they use. In the same way, Postini customers rely on our patented email security service to "clean and screen out impurities" from their email communications. They are assured a flow of clean, legitimate messages, and pay only for what they use.

About Postini

Postini, Inc. is the industry's leading provider of email security and management solutions that protect email communications infrastructure by preventing spam and other SMTP attacks from reaching the enterprise gateway. Postini's patented managed services model utilizes exclusive preEMPT™ technology to eliminate spam and viruses, stop DoS and directory harvest attacks, safeguard content, and improve email performance. Founded in 1999, Postini processes more than 1.3 billion email messages per week for more than 3,800 companies. By blocking spam, viruses and attacks before they can reach the enterprise email gateway, Postini Perimeter Manager™ assures complete email security while saving bandwidth, conserving server capacity and minimizing administrative costs.



Headquarters

Postini, Inc., 510 Veterans Boulevard, Redwood City, California 94063

Toll-free 1-866-767-8461

Email info@postini.com

Web Site www.postini.com

For more information or to see if your organization qualifies for our free 30-day, no-risk trial of Postini Perimeter Manager, call toll-free 1-888-584-3150, email us at sales@postini.com, or visit us online at www.postini.com.

© Copyright 2004 Postini, Inc. All rights reserved. WP13-02-0408

Postini, the Postini logo and Postini Perimeter Manager are registered trademarks or service marks of Postini, Inc. preEMPT is a trademark of Postini, Inc. All other trademarks listed in this document are the property of their respective owners.