

**Postini® White Paper**

# Phishing, viruses, bot-nets & more: How to prevent the “Perfect Storm” from devastating your email system

## Enterprises Face Unprecedented "Perfect Storm" Of Email Attacks In 2005

The "perfect storm" weather description, made famous by the movie by the same name, is an apt analogy for the evolving threats to email systems expected in 2005. Taken separately, spam, phishing, viruses, bot-nets and directory harvest attacks represent serious email threats. However, all of these threatening "storms" are converging on email systems in an unprecedented assault that can bring down servers, undermine confidence in email, and flood inboxes with unwanted messages.

Gone are the days when a first-generation anti-spam product could stop the spam threatening email systems. As anti-spam and email security products have grown more sophisticated, so have the spammers and hackers seeking to circumvent them. Avoiding the "perfect storm" in email threats now requires a more comprehensive and robust solution that defends email systems with multiple layers of prevention and protection.

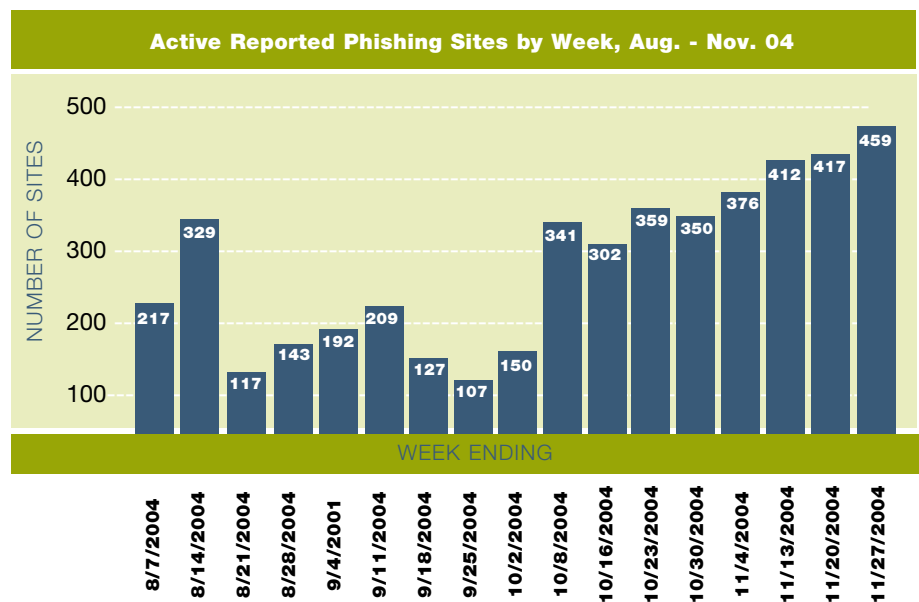
## Phishing Schemes Luring More Victims

Phishing schemes have garnered headlines in the consumer press and the attention of major financial services companies and technology vendors as reports of stolen private account information multiplied during 2004. Phishing involves using email messages to trick users into exposing their passwords or confidential information. In many cases, fraudulent emails appear to be from legitimate senders directing users to a web site where private information is requested.

The Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)), a consortium of law enforcement, financial firms and security vendors issued several statements in 2004 warning of the increase in frequency of these email scams. See Figure 1 below. Estimates of losses due to identity theft by phishing schemes varies widely, but Gartner has estimated losses to banks and credit card companies in the billions of dollars. <sup>(1)</sup>

**Figure 1 Active reported phishing sites from August-November 2004**

Source: Anti-Phishing Work Group



## **Viruses Create Bot-Nets Of Zombie Computers**

As email administrators have become more adept at identifying originating IP addresses of spammers—and shutting them down—spammers have turned to a new technique that uses viruses to take over people's home and office computers and turn them into "spam zombies". Large numbers or networks of zombie computers called "bot-nets" then serve as conduits for, or sources of, spam, viruses, and DHAs. Viruses such as bagle and netsky are recent examples.

## **Bot-Nets Amplify Spam, Phishing And Directory Harvest Attacks**

Spammers controlling bot-nets can launch spam from hundreds or even thousands of hijacked machines simultaneously, making it nearly impossible to identify and block an attack by conventional methods. Ferris Research, for example, estimates that more than half of all spam at the end of 2004 was generated through bot-nets.<sup>(2)</sup> More than one-third of IP addresses blocked by Postini's patent-pending IP Analysis engine now resolve back to cable modem and DSL line sources that should not be relaying SMTP directly—an indicator of how extensive the use of bot-nets to spread spam has become during the second half of 2004.

## **Directory Harvest Attacks Grow In Intensity**

Directory Harvest Attacks (DHAs) are the most unrecognized and underreported email threat. Used to harvest legitimate email addresses from corporate mail servers, spammers send tens 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. Harvested addresses are then compiled into lists and sold or distributed to other spammers.

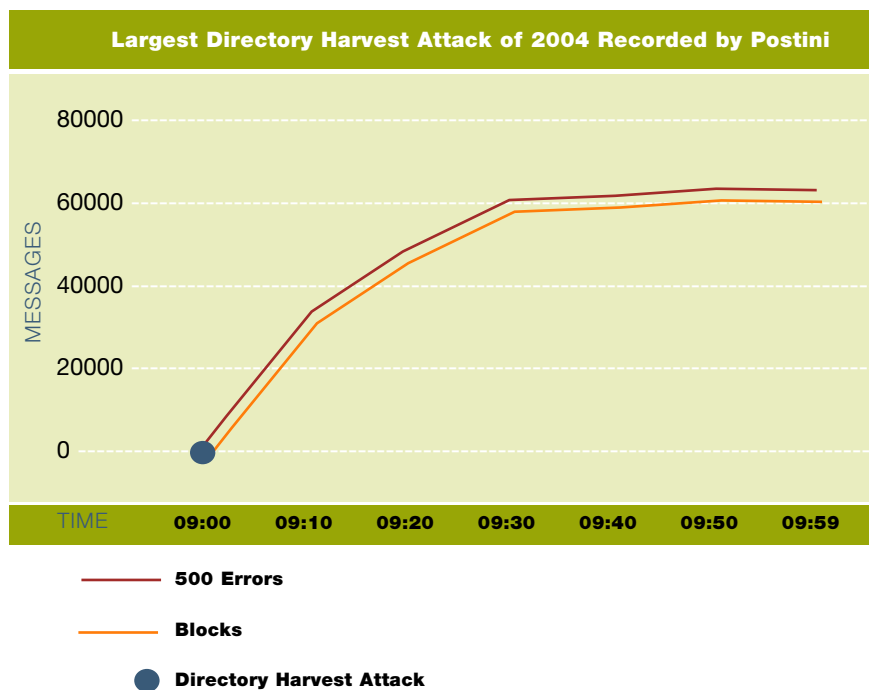
DHAs often result in very damaging side effects by consuming enormous amounts of email server resources while email servers try to cope with these probes. Lotus Domino and Microsoft Exchange, for example, typically accept all messages for their domain. This only aggravates the negative impact of a directory harvest attack because the spammer assumes all the attempted addresses are valid, and will send spam to all the addresses.

During a directory harvest attack, the Domino or Exchange server also creates non-delivery reports (NDRs) for all of the invalid addresses (virtually all of them!). If, for example, a directory harvest attack makes 10,000 delivery attempts to an email system

and only 100 turn out to be deliverable, the Exchange or Domino server will generate 9,900 non-delivery reports. In some cases, these NDRs are sent back to spoofed addresses, so they often bounce back again creating an "NDR storm." NDRs from DHAs use up vast amounts of server cycles that result in full deferral queues, and in extreme cases they can bring down email servers.

Because directory harvest attacks are often launched simultaneously, from many different computers. The resulting spike in traffic from the directory harvest attack can easily knock an email server offline. While the frequency of directory harvest attacks has been consistent over the course of 2004—the average company experiences 150 attacks per day—the severity of DHAs is increasing rapidly with the average attack consisting of more than 250 invalid address lookups.<sup>(3)</sup>

**Figure 2 Example of a severe Directory Harvest Attack.**



The largest DHA attack recorded by Postini to date occurred December 10 against a major North American retail company. The attack took place over a one-hour period, peaking at more than 60,000 delivery attempts per minute in its final phase. Such attacks are becoming more severe as spammers seek to harvest legitimate email addresses for sales and distribution to other spammers.

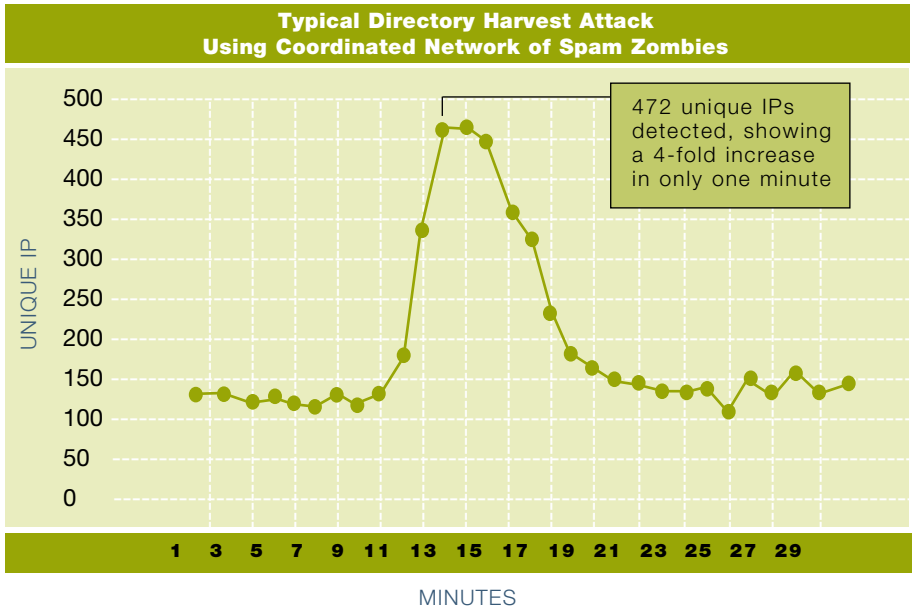
### Email Threats Converging Simultaneously

It's not unusual for spammers to make use of spam, virus, bot-net and directory harvest attack techniques all together or in various combinations to create a "perfect storm" assault on enterprise email servers.

Consider a virus outbreak such as Sobig, for example. Spammers broadcast the Sobig virus that got past anti-virus defenses, which couldn't be updated fast enough. The Sobig virus carried a payload that turned thousands of computers into zombies. This network of zombies or bot-net, was then capable of sending more copies of Sobig, as well as sending hundreds of thousands of spam messages to addresses found in their zombie computers' Outlook or Outlook Express address book.

Bot-net spam messages are sent with the 'From' address of the computer's owner, or another address in Outlook's address book. Some of these spam messages target old addresses that generate bounce back messages. Other spam messages are bounced back by anti-virus software protecting recipients. All of these rejected spam messages then bounce back to the infected computers. Multiply the bounce back messages by hundreds or thousands of users in any given company and you get a storm of activity that consumes millions of message cycles.

**Figure 3 Typical "Perfect Storm" Attack Using Coordinated Network of Spam Zombies from Hundreds of IP Addresses**



Typical anti-spam or anti-virus point products or appliances simply can't cope with these types of converging attacks—nor are they designed to. Preventing the perfect storm in email threats requires broad scope threat protection and a multi-layered approach to stopping threats before they can get inside the enterprise email gateway.

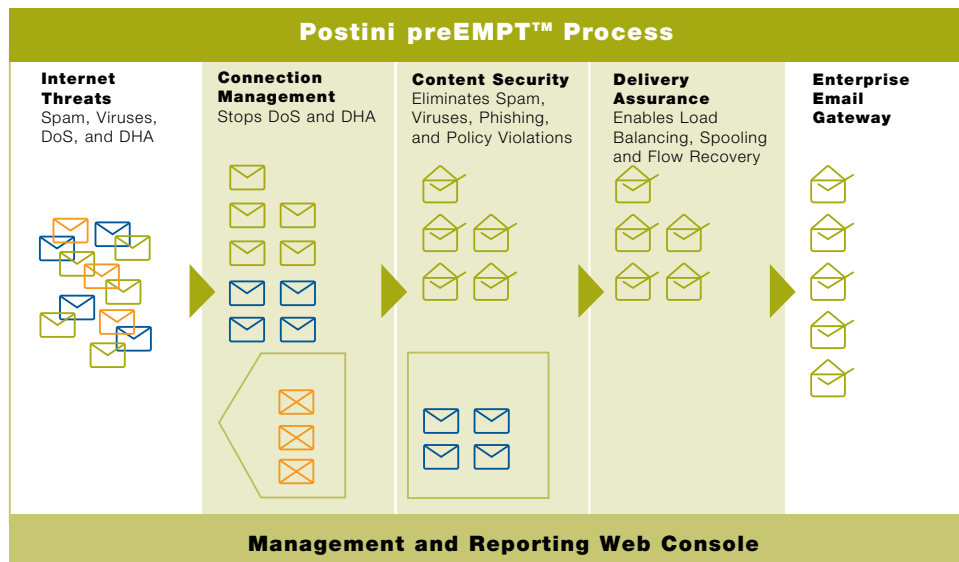
**Stopping The Perfect Storm: Postini's Preemptive, Multi-Layer Approach**

As the leading email security managed service, Postini is ideally suited to dealing with the current perfect storm of email threats precisely because it sits between the Internet and the enterprise email system. Postini catches phishing attempts, viruses, as well as bot-net spam and directory harvest attacks before they can reach an enterprise email network using a patented, multi-layer threat prevention approach.

Postini's preEMPT™ 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. Emails are initially screened at the SMTP connection point through patent-pending IP "behavior" analysis that eliminates nearly half the malicious messages. The balance are then screened through Postini's content filtering rules and heuristics to eliminate spam and other threats and enforce policy. All suspect emails are blocked, and legitimate emails are instantly forwarded to the enterprise destination mail server in real time, from memory. Depending on the enterprise's email security policy, suspicious email is either tagged and delivered or quarantined to a web-accessible storage area for user review.

Spammers and hackers manipulating bot-nets (groups of zombie computers infected with email viruses) can launch spam and email system attacks from hundreds or even thousands of hijacked machines, making it impossible for older anti-spam technologies to trace and identify the IP sources of the attacks. More than one-third of IP addresses blocked by Postini's patent-pending IP Analysis technology now resolve back to cable modem and DSL line sources that should not be relaying SMTP directly—an indicator of how extensive the use of bot-nets to "spread spam and move on" has become during the second half of 2004.

**Figure 4 Postini's multi-layer approach to protecting the enterprise**



Sitting between the Internet and the enterprise's email gateway, Postini blocks spam, phishing, viruses, and email attacks before they have a chance to impact the enterprise

### Patent-Pending IP Behavior Analysis At SMTP Connection Level

In many cases, newly evolving "perfect storm" threats such as directory harvest attacks, cannot be stopped by conventional content filtering methods typically used in anti-spam software and appliances. Nor can new spam and phishing techniques that reduce or eliminate content in a message be reliably blocked with conventional content filtering. The detection of malicious emails and DHAs needs to occur in real time, at the SMTP connection point, in order to prevent them from ever reaching the enterprise email gateway.

Unlike many anti-spam products or services, Postini is unique in conducting real time inspection of every IP address at the SMTP connection point. Only Postini offers patent-pending IP analysis based on more than two-dozen

variables to determine if the "behavior" of the message exhibits the characteristics of a spam, virus, or email attack. Based on this real time, continuous analysis, specific SMTP connection patterns are associated with malicious behavior, enabling Postini to block these connections without having to examine the actual message.

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 while the balance of messages are then screened by its award-winning content filtering. This multi-layer approach incorporating real-time IP analysis and advanced content filtering has proven to be highly effective in combating the shifting tactics of spammers and in preventing the perfect storm of email threats from harming enterprise email systems.

### **Award-Winning Content Filtering Stops Spam, Viruses, & Phishing Attempts**

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 Filtering process, where messages are screened using thousands of rules, or heuristics, constantly updated by Postini to reflect new spam types and email threats. These new rules are always immediately available to protect the enterprise without the need for the IT staff to download or install any software.

### **Postini Content Filtering Heuristics Catch Threats As They Evolve**

Utilizing thousands of heuristic expressions, Postini's content filtering engine assesses each email and computes a statistical probability by correlating a "score" against a configuration setting. Heuristics are automatically and incrementally modified based on millions of messages each day to block email threats as spammer tactics evolve.

Another unique advantage of Postini's patented method for processing email messages over other managed service providers is Postini's exclusive "pass-through" technology. Postini, in contrast, conducts all analysis of SMTP connections and email messages in real time, so that no messages get stored but rather legitimate emails are instantly passed along to their recipients. This eliminates any concerns about privacy and security, especially for those enterprises in highly regulated industries such as financial services and healthcare.

### **Multiple-layer Anti-Virus Protection**

Postini's delivers multi-layer antivirus protection coupled with patent-pending preEMPT technology to protect email systems during the critical time from the initial outbreak of a virus—its zero hour—until an antiviral signature is available. This multiple layer of antivirus protection helps to contain viruses from the instant an outbreak occurs. Partnering with McAfee and Authentium, Postini provides the latest in virus blocking technology as part of its comprehensive email security managed service.

### **Policy Enforcement Advantages**

Postini's email security managed service also provides both inbound and outbound email policy enforcement capabilities.

Outbound email filtering from Postini enables organizations to scan outbound messages for viruses and apply content policies, protecting both customers and partners and ensuring that corporate policies regarding appropriate use are observed. Inbound anti-virus scanning prevents viruses from entering a corporate network through the gateway. Outbound anti-virus scanning prevents the spread of viruses to customers and partners. This additional layer of protection helps to prevent the spread of viruses, adding security and stability of your network.

### **Anti-Spam Rated Among Highest For Accuracy And Effectiveness**

Postini is proven to be one of the most effective solutions for eliminating spam. In a comparison test of leading anti-spam products as reported in Network World magazine, December 2004, Postini rates the highest for anti-spam effectiveness—with the best overall balance of accuracy (97%) and very few false positives (.08%).<sup>(4)</sup>

### **Anti-Phishing Stops 400,000 Attempts Each Day**

Postini blocks phishing attacks by applying several hundred spam-filtering rules targeted specifically at phishing techniques. Postini estimates that its patented preEMPT technology stops 98 percent or more of email phishing attempts before they can reach the customer's network through a multi-layered approach. Postini routinely blocks more than 400,000 phishing attempts each day through a combination of sender behavior analysis, URL exploit detection, and advanced content filtering heuristics.

### **Anti-Virus Blocks Zombie Viruses**

As the incidence and severity of email viruses has nearly tripled in past year, Postini consistently demonstrates superior anti-virus capabilities, blocking more than 1 billion viruses in 2004 alone. Postini prevents viruses such as Netsky and Bagle from infecting PCs and turning them into zombies that can be taken over to send even more spam.

## About Postini

Postini, Inc. is the leading provider of email security and management services that protect email infrastructure by preventing spam and attacks from reaching the enterprise gateway. Postini's patented managed services model utilizes exclusive preEMPT transport and content filtering 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 3 billion message connections every week for more than 4,200 companies. By blocking spam, viruses and attacks before they can reach the enterprise email gateway, Postini Perimeter Manager is designed to assure complete email security while saving bandwidth, conserving server capacity and minimizing administrative costs.

For more information contact Postini at its Redwood City, California headquarters toll-free at 866.767.8461, or visit [www.postini.com](http://www.postini.com).

To find out more about Postini's secure email boundary services, visit our web site at [www.postini.com](http://www.postini.com). There you will find detailed information about Postini Perimeter Manager enterprise edition and how it can protect your organization's email system.

### References:

- (1) "Phishing on the Increase, Group Says," by Bob Francis, *InfoWorld*, Nov. 29, 2004.
- (2) Telephone interview, Richi Jennings, Lead Analyst for Spam and Boundary Services Practice, Ferris Research [www.ferris.com](http://www.ferris.com), Dec. 17, 2004.
- (3) *Postini Email Security Annual Review & Threat Report*, published January 2005, [www.postini.com](http://www.postini.com).
- (4) "Spam in the Wild: The Sequel," by Joel Snyder, *NetworkWorldFusion*, Dec. 20, 2004.



### Headquarters

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

**Toll-free** 1-866-767-8461

**Email** [info@postini.com](mailto:info@postini.com)

**Web Site** [www.postini.com](http://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](mailto:sales@postini.com), or visit us online at [www.postini.com](http://www.postini.com).**

© Copyright 2004 Postini, Inc. All rights reserved. WP25-02-0503

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.