

The Silent Killer: How spammers are stealing your email directory

There is a “silent killer” unleashed by spammers that is threatening to steal your email directory addresses through what is known as a “directory harvest attack”(DHA). You may have already observed some of the symptoms of these virtually undetectable attacks on your email systems.

Have you ever had your end users complain about how slowly your email system seems to be responding when you have no visible reason for this problem in performance? Have you ever had an end user ask why he or she is getting a completely blank message? No content, nothing? Or, have you observed sudden bursts or spikes in activity on your email system that last just a few minutes and subside for no apparent reason? Are your Microsoft Exchange® server deferral queues constantly full, slowing server performance to a crawl?

All of these are signs that spammers are probing your email system in an attempt to identify and “harvest” legitimate email addresses from your organization. Unfortunately, these directory harvest attacks (DHAs) are difficult to detect, and often go unnoticed by most email administrators, while potentially creating problems that are as bad—or worse—for your email system as conventional spam.

Processing more than 1 billion SMTP email connections per day, Postini, the leading Integrated Message Management provider, has observed a dramatic increase in directory harvest attacks at the end of 2005.

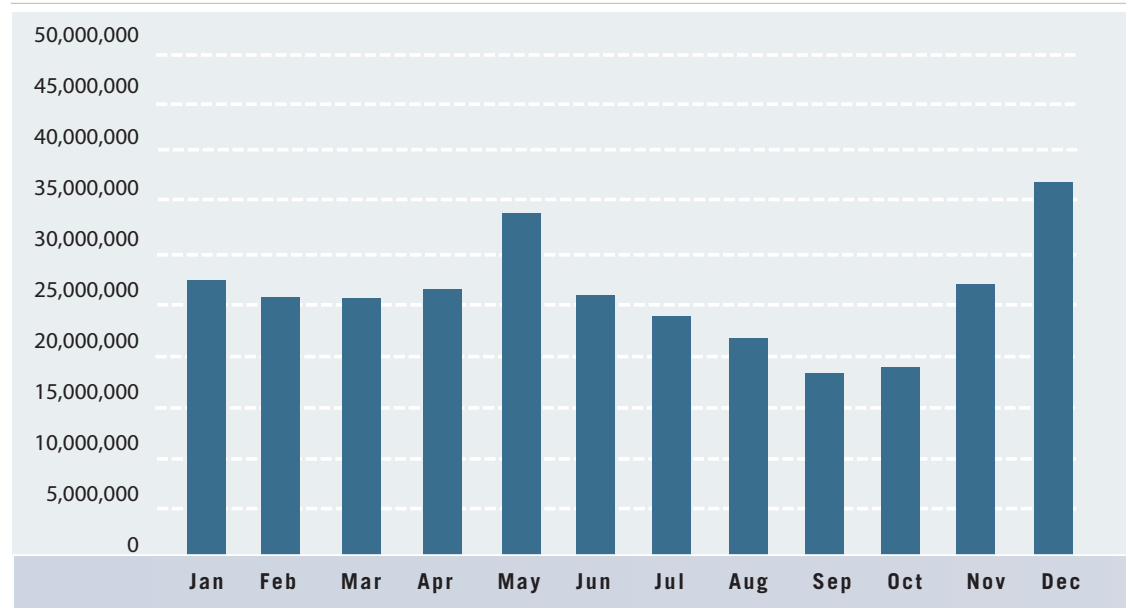
As Figure 1 illustrates, the number of directory harvest attacks increased dramatically in December of 2005, even as the severity of attacks have been getting smaller to avoid detection. Postini’s exclusive Sender Behavior Analysis™ is able to identify and block DHAs at the SMTP connection level, measuring this type of activity and preventing these attacks for customers worldwide. Chances are you’ve already experienced such an attack and probably were not even aware of it except for the symptoms described above.

WHAT KIND OF ATTACK?

To understand how a spammer or list broker can harvest your email address directory, consider the basics of how email gets delivered. Before the Internet protocol SMTP can deliver email to a server, it must first check to see if the delivery address is valid. It does this by sending a “delivery attempt” request. This request essentially asks, “Does this email address exist, and can I deliver mail to it?”

An open source or stand alone Mail Transfer Agent (MTA) typically responds to delivery attempt requests with a synchronous “yes” or “no”. If the response is “no”, the sending server gets an SMTP 550 error message since the address is invalid and mail for that address cannot be delivered. If the sending server gets a “yes”, it knows the address is valid and a message can be delivered. Spammers, list brokers or other unscrupulous culprits can exploit this simple functionality to probe your email servers and harvest legitimate email addresses from your corporate directory.

TOTAL VOLUME OF DHAs BY MONTH - 2005



Source: Postini 2006 Message Management & Threat Report

Figure 1: Total Number of DHAs or other Connection Point threats 2005

While DHAs appeared to be declining over the course of the year, they increased dramatically in December of 2005 when Postini recorded more than 8 billion invalid look up attempts across more than 46 million attacks. These statistics suggest that spammers increased their efforts to harvest legitimate email addresses in the last month of the year, possibly as part of the holiday season, in order to glean as many legitimate addresses as possible for further spamming activity.

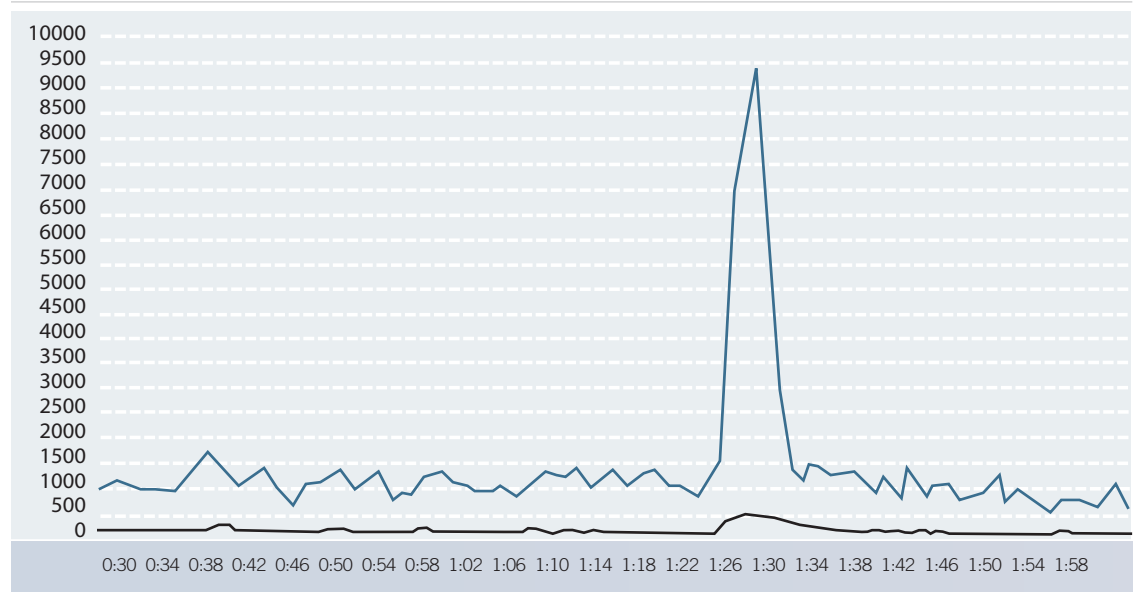
To do this, they engage in a directory harvest attack that sends thousands (or even hundreds of thousands) of messages to multiple addresses such as johndoe@yourcompany.com, or jdoe@yourcompany.com. While spammers typically don't attack any given domain for more than a few minutes, over time an aggressive DHA can map an entire email directory using brief blasts of a few hundred or thousand address requests from a shifting array of IP addresses. Spammers track all of the addresses that do not bounce back or generate 550 errors, and consider these as valid addresses, which are then compiled into lists that are then sold or distributed to other spammers. Users that have their addresses harvested through DHAs can expect to receive even more spam and unwanted junk email!

LOTUS/DOMINO AND EXCHANGE SERVERS ARE EVEN MORE VULNERABLE

In contrast to sendmail or stand-alone MTA email servers, Lotus Notes® and Exchange servers 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.

During a directory harvest attack, the Domino or Exchange server asynchronously creates non-delivery reports (NDRs) for all of the invalid addresses (which can number in the thousands or tens of thousands). If, for example, a directory harvest attack makes 10,000 delivery attempts to your email system and only 100 turn out to be deliverable, your Exchange or Domino server will generate 9,900 non-delivery reports.

DIRECTORY HARVEST ATTACK PROFILE



Source: Postini

Figure 2: Invalid Lookups by Unique IPs over time in minutes

DHAs exhibit “bursts” in messaging traffic, causing harmful traffic spikes that can quickly overload servers, severely slowing performance or shutting servers down.

These voluminous NDRs use up valuable server cycles and result in deferral queues being full. Even worse, the Domino or Exchange NDRs are sent back to what is typically a fraudulent or bogus “From” address, and consequently bounce back to the Domino or Exchange server again—generating yet another set of NDRs. In our example of 10,000 delivery attempts, a server will end up having to handle nearly 30,000 inbound and outbound messages from this one DHA attack, plus all the following spam. That kind of traffic volume can easily strain the capacity of a server and can result in server crashes, database corruption and user complaints about slow email system response. The net affect of a DHA on a Domino or Exchange server is equivalent to a self-inflicted denial of service attack as messages and NDRs slingshot back and forth between the sender and the email system.

NOT JUST AN EMAIL INBOX ISSUE, BUT A QUALITY OF SERVICE PROBLEM

Because of the harmful impact from DHAs on email system performance, directory harvest attacks must be treated as more than just an email inbox or end user annoyance issue. Directory harvest attacks cannot be stopped by conventional content filtering by appliances or software since there is no “content.” Traditional approaches to SMTP perimeter protection, such as IP address blocking are also not effective, since most spammers are now using dynamic sending IPs and distributing their IP attacks. While it’s possible to get some sense of the scale of the problem by checking email server logs at the end of the week for bounce responses, by the time the log analysis identifies a suspect IP barraging the server with invalid delivery attempts, the valid addresses have long since been harvested and/or server cycles have been wasted in a vicious cycle of response and bounce back messages.

The detection of DHAs needs to occur in real-time, at the SMTP connection point, in order to prevent them from ever reaching your email gateway. Conventional anti-spam appliances and software operating inside the email gateway, however, can't prevent directory harvest attacks or their devastating side effects.

PREEMPTIVE PROTECTION FROM DHAs AND OTHER THREATS—ONLY FROM POSTINI

Only Postini's Integrated Message Management technology offers a viable solution. That's because Postini's patented managed service is able to identify and block DHAs at the SMTP connection level—before they can even reach your email gateway. As Figure 3 illustrates, Postini Perimeter Manager's Sender Behavior Analysis™ capability detects and blocks directory harvest attacks and Denial of Service attacks (as well as some spam) all without ever looking at the message contents.

Patented technology makes this possible by examining the behavior of the sending computer. Specific SMTP connection patterns are indicative of malicious behavior, enabling Postini to block connections without seeing the actual message. Attacks are detected by the Postini managed service in real-time, the offending IP is blocked, the harvest attempt stopped, and the email administrator notified and a report is produced providing details of the attack.

Processing more than 1 billion inbound SMTP connections daily, Postini currently blocks more than 50 percent of SMTP connections without having to examine the messages themselves. Throughout 2006, for example, Postini has been blocking more than 18 million directory harvest attacks on average each month.

Once an SMTP connection is validated or the sending IP address has not been identified as having engaged in damaging behavior, the message data is passed through Postini's Content Analysis (Figure 3) process, filtering messages to eliminate viruses and spam using thousands of rules, or

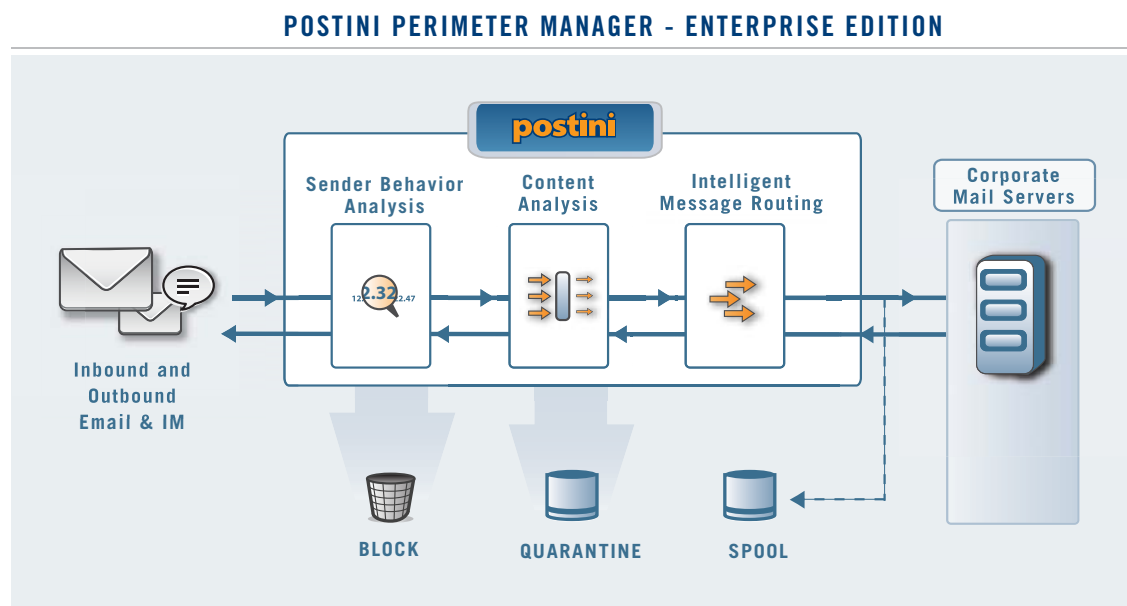


Figure 3: Postini Perimeter Manager® patented technology blocks attacks at the connection point with its exclusive Sender Behavior Analysis. Emails are then screened through Content Analysis to eliminate spam and quarantine questionable messages.

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 Intelligent Message Routing (Figure 3) 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.

- Saves your email infrastructure from wasting cycles and bandwidth responding to directory harvest attacks and probes.
- Reduces costs and the workload of your IT staff since it requires no integration with existing email infrastructure, no software and no hardware.
- Helps you maintain the email performance and quality of service vital to supporting your business.

To learn more about Postini's Integrated Message Management services please visit our Solutions Overview online at www.postini.com.

NO NEED TO RISK HARM OR THEFT FROM DIRECTORY HARVEST ATTACKS

As the risks and impacts from directory harvest attacks continue to grow, Postini offers a proven email security solution through its managed service model that prevents threats from ever reaching your email gateway. Postini's Integrated Message Management managed service:

- Prevents the "silent killer" directory harvest attack from overloading your servers and stealing addresses from your email directory.
- Stops spammers from using addresses that would have been harvested to further flood your email system with unwanted messages.



ABOUT POSTINI

As the leader in Integrated Message Management, Postini managed services protect businesses from a wide range of IM and email threats, provide message archiving and encryption, and enable the management and enforcement of enterprise policies to meet regulatory compliance requirements.

Corporate Headquarters

San Carlos, CA USA
Toll-free: 1-866-767-8461
Email: info@postini.com
www.postini.com

EMEA Headquarters

London, UK
Tel: +44 (0)20 7082 2000
Email: info_emea@postini.com

Asia Pacific Headquarters

Tokyo, Japan
Tel: +81 80 3089 7470
Email: info_apac@postini.com