

Postini® White Paper

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, going 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 400 million SMTP email connections per day, Postini, the leading preemptive email security and management provider, has observed a dramatic increase in directory harvest attacks over the past six months.

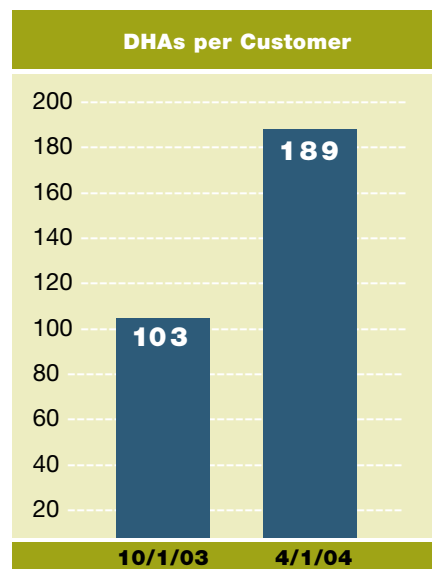


Figure 1
Directory Harvest Attacks are increasing at an alarming rate

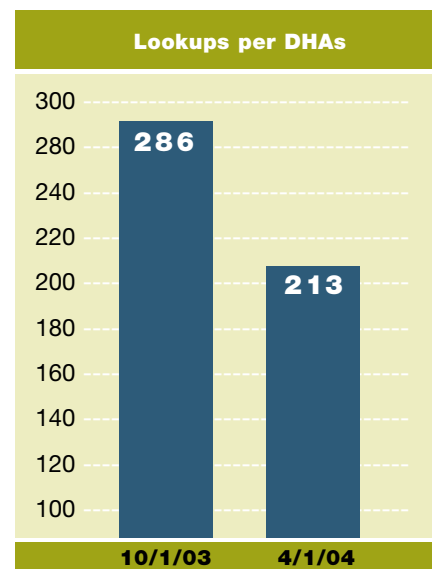


Figure 2
DHAs now occur in smaller volumes to avoid detection

As Figures 1 and 2 illustrate, the number of directory harvest attacks has nearly doubled in the past six months while attacks have been getting smaller to avoid detection. Postini's exclusive Preemptive Email Protection Technology (preEMPT™) is able to identify and block DHAs at the SMTP connection level, measuring this type of activity and preventing these attacks for more than 3,300 customers. If you are not currently using Postini's email security managed service, chances are you've already experienced such an attack and probably were not even aware of it except for the symptoms described above.

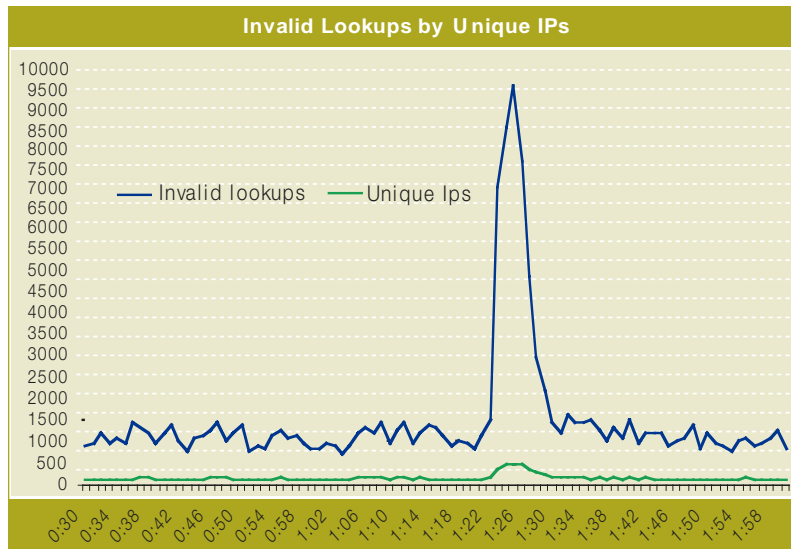
What kind of attack?

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

Figure 3 DHAs exhibit "bursts" in messaging traffic, causing harmful traffic spikes that can quickly overload servers, severely slowing performance or shutting servers down



servers and harvest legitimate email addresses from your corporate directory. 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.

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.

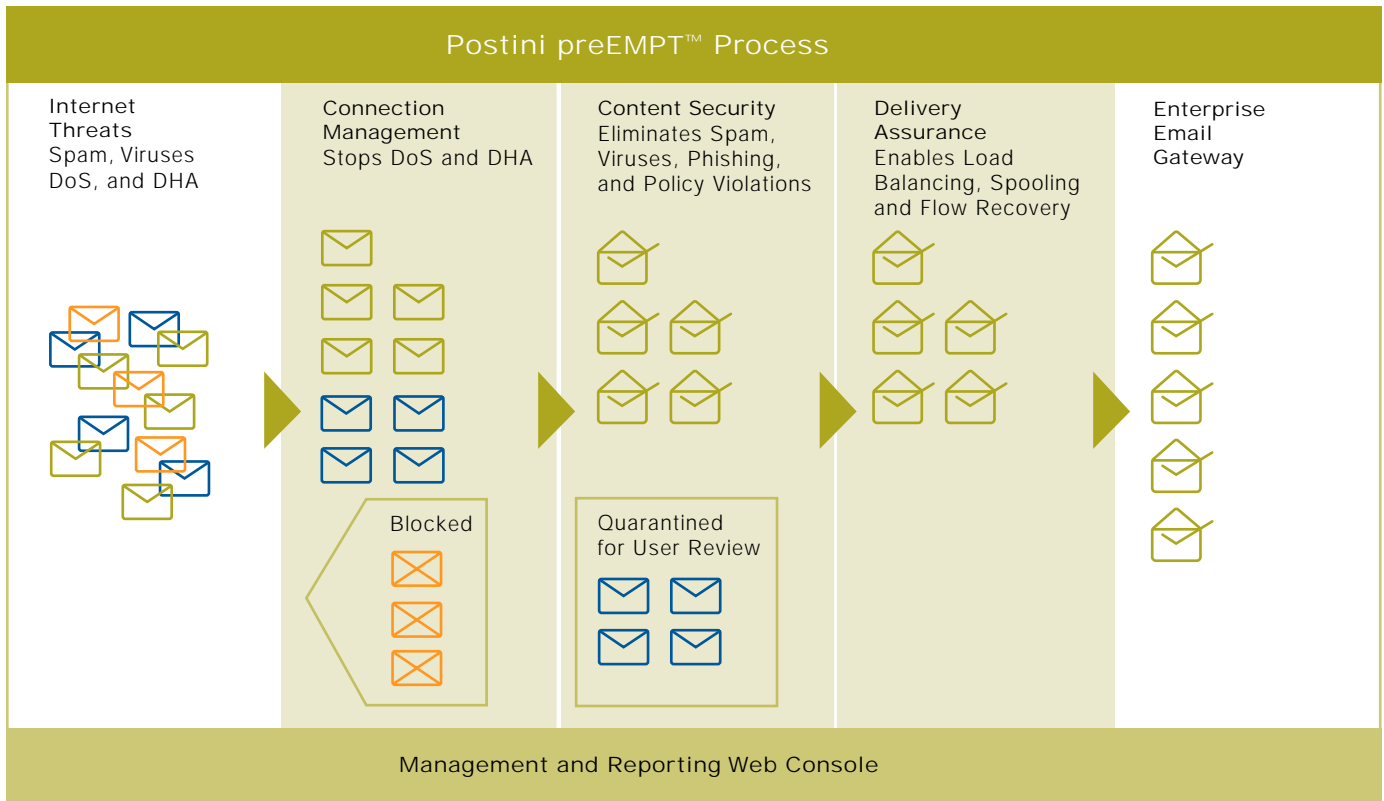
Not just an email inbox issue, but a Quality of Service problem

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

Figure 4 Postini's patented preEMPT™ process identifies Directory Harvest attacks and blocks them at the SMTP connection level, prior to content filtering, and ensures that none of these types of attacks reaches the enterprise email gateway.



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 preemptive email protection 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 4 illustrates, Postini's Connection Management 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 400,000,000 inbound SMTP connections daily, Postini currently blocks more than 50% of SMTP connections without having to examine the messages themselves. In one 48-hour period, for example, Postini blocked more than 100,000 directory harvest attacks involving 3 million bogus address requests directed at more than 100 organizations.

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 Security (Figure 4) 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 4) 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.

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 preemptive email protection:

- 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.
- 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.

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 one billion email messages per week for more than 3,300 companies.



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. WP08-01-0406

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.