



510 Veterans Blvd
Redwood City, CA 94063

You **wouldn't leave your
corporate directory on
the street corner.**

**Why are you leaving
your corporate email
directory **OPEN**
for **Spammers?****



DIRECTORY HARVEST ATTACKS

Email's Silent Security Killer

Today, up to twenty-five percent of corporate email server resources are spent processing attacks intended to harvest fresh, valid, corporate email addresses. The attackers are using a particularly vicious technique called a “Directory Harvest Attack”. The goal of a Directory Harvest Attack is to steal the corporate email directory of valid email addresses. This is just one of the ways in which list brokers and spammers are exploiting the inherent vulnerabilities of current corporate email systems. Below is an explanation of how Directory Harvest Attacks work and what you can do to prevent your company from being victimized by them.

EMAIL DIRECTORY VULNERABILITY

To understand how a spammer or list broker can harvest your email address directory, you first need to understand a little about how email gets delivered. The Internet protocol used to deliver email is called Simple Mail Transfer Protocol, or SMTP. Before 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 basically asks, “Does this email address exist and can I deliver mail to it?” All email servers are programmed to respond to such requests with a simple “Yes” or “No”. If the answer is “No”, the sending server knows the address is invalid and mail for that address cannot be delivered. In email techno-jargon, this “No” answer is known as an “SMTP 500 error”. If the answer is “Yes”, the sending server knows that the address is valid and a message can be delivered.

“Everyone’s email address is vulnerable – from the stockroom to the CEO.”

Spammers, list brokers, recruiters and others exploit this functionality to probe email servers in order to “harvest” the valid email addresses from corporate directories. To find valid addresses at yourcompany.com, spammers engaging in Directory Harvest Attacks will send messages to multiple addresses like johndoe@yourcompany.com, jdoe@your-company.com, and john@yourcompany.com. Spammers note all of the addresses that do not bounce back or generate 500 class errors. Any address where a bounce message is not generated is regarded as valid. By compiling a list of all of the addresses that are valid, spammers can find nearly all addresses on a corporate email system.

A successful Directory Harvest Attack can net a spammer thousands of addresses in just a few minutes. Those users that have their addresses harvested in this way can expect to receive an ever-growing amount of junk email as spammers acquire and resell known valid addresses. In order to cover their tracks, spammers typically don’t

“Firewalls do not have the capability to prevent and protect your corporate email server from Directory Harvest Attacks.”

attack any given domain for more than a few minutes at a time. Over time, however, an aggressive Directory Harvest Attack can map an entire email directory by using brief blasts of a few hundred or a few thousand address requests from a shifting array of IP addresses.

Directory Harvest Attacks increase corporate costs not just when they are carried out, but year after year — they are a kind of “meta-spam” that allows for hundreds or thousands of new junk email messages to reach your servers and your users. When your company loses control of its directory of valid email addresses, every user will be on the receiving end of hundreds of unwanted messages that consume bandwidth, storage, and end user time.

In addition to multiplying the spam problem, Directory Harvest Attacks place heavy loads on corporate email servers, which generate thousands of bounce messages (SMTP 400 - and 500 - class errors) in response. This increase in activity creates spikes in traffic that can completely shut down an email server, causing it to send “busy signals” and to bounce email messages — even valid ones. It’s not uncommon for Directory Harvest Attacks to routinely consume up to one quarter of system resources. Fortunately, there is a way to stop these attacks.

CLOSING THE DOOR ON DIRECTORY HARVEST ATTACKS

Directory Harvest Attacks are difficult to detect and defend against because email infrastructure was built to be open, accessible, and decentralized. But today, openness, accessibility, and decentralization are vulnerabilities that make protecting and managing the email system difficult. Unfortunately for end-users, traditional approaches to SMTP perimeter protection, such as IP address blocking, are not effective. Most attackers are now using dynamic sending IPs, and distributing their IP attacks.

In fact, most email systems and email management tools aren’t equipped to detect Directory Harvest 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. The detection of Directory Harvest Attacks needs to be carried out in real-time in order to stop the attack before the attacker has collected the valid addresses.

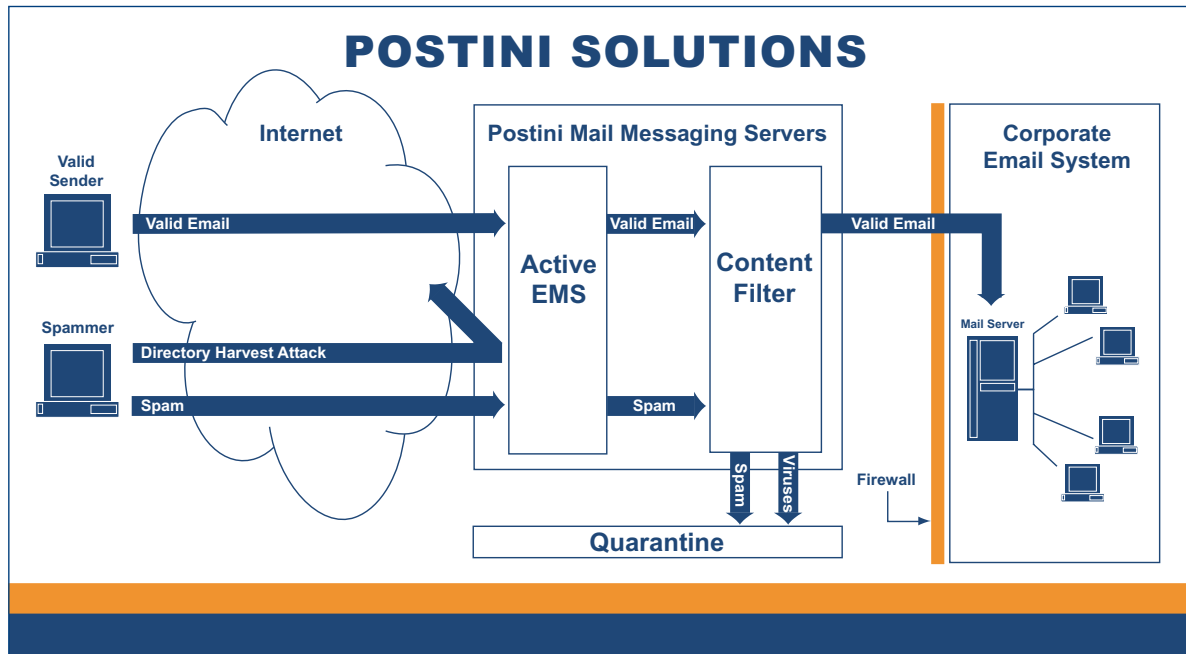
How is it possible to respond to attacks of short duration from multiple sources? The only commercially available solution today is Postini's Active Email Management System (EMS).

POSTINI'S ACTIVE EMAIL MANAGEMENT SYSTEM

Senior IT managers and email infrastructure managers in corporate and public sector organizations who need perimeter protection and management of their email system should consider Postini's Active EMS. Active EMS works in conjunction with Postini's anti-spam and anti-virus services to provide a uniquely integrated

email perimeter protection solution that delivers increased uptime load balancing and reporting. Unlike other email management systems, Postini's Active EMS works across all messaging platforms, and requires no additional hardware, software, or administrator time.

Acting as a firewall for email servers, Active EMS is positioned between the corporate email server and the Internet. It provides immediate detection of Directory Harvest Attacks and responds with a variety of defensive actions according to the corporate email administrator's preferences. Typical responses include increasing the time to reply, ignoring the attacker's requests, or bouncing all attack delivery requests. Active EMS detects the attack in real time, blocks the offending IP, stops the harvest attempt, and notifies the system administrator. Active EMS then reports the attacks, which creates documentation that often amazes administrators when they





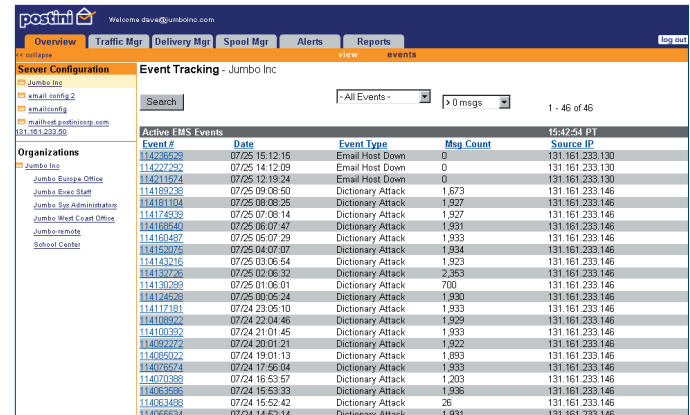
The Active Traffic Manager: Postini protects the identity of your users email addresses by blocking extremely prevalent and unknown directory harvest attacks (Dictionary Attacks).

discover the amount of load on their servers that is directly attributed to Directory Harvest Attacks.

As a service, Active EMS works with all email systems and requires no integration with existing infrastructure, or any new hardware or software. Currently, hundreds of organizations are using Active EMS to protect hundreds of thousands of email boxes.

In a recent forty-eight hour period, Active EMS blocked more than 100,000 Directory Harvest Attacks involving more than 3 million bogus address requests directed at more than 100 organizations. While substantial annual growth in email message volume is a given for most email administrators, new investments in hardware and network services could be reduced if it were possible to avert Directory Harvest Attacks. That's exactly what Postini's Active EMS does.

In blocking Directory Harvest Attacks, Postini's Active EMS preserves email system integrity, saves wasted CPU cycles and bandwidth, and allows valid email to reach its



The Active EMS Event Tracking: An example of a customer's Directory Harvest Attacks that Active EMS logged within a short period of time.

destination on time. In addition, it prevents spammers from using the addresses that would otherwise have been harvested to flood corporate email servers with wasteful commercial offers and objectionable material.

CONCLUSION

The bottom line is that junk email is theft of your email system resources. Until now, spam has simply been unsolicited junk mail arriving postage due. Directory Harvest Attacks are theft on a grander scale and present a much greater threat to corporate security and privacy, not to mention the financial impact. You wouldn't leave your corporate directory sitting on a street corner, and you shouldn't be leaving your email system open to this kind of attack.

To learn exactly how Postini can protect your email system against Directory Harvest Attacks and the associated junk email and viruses they can engender, visit www.postini.com or call 1-866-767-8461.

