



Spam Filtering Technology

A Securrence White Paper

The New Spam Onslaught: A Cat and Mouse Game *How One Spam Sniper Targets the Bull's-eye*

Table of Contents

Introduction	2
A Look Under the Hood	3
Two Brief Case Studies	6
Securrence Provides Complete Protection	7
Conclusion	8

The New Spam Onslaught: A Cat and Mouse Game

How One Spam Sniper Targets the Bull's-eye

Will spam – already the scourge of nearly every email inbox – ever be brought under control? In spite of increasingly sophisticated email filtering, spam continues to be a significant workplace and personal problem, and dealing with it is proving to be a cat and mouse game.

Findings from a report produced by Nucleus Research, a global research firm that recently conducted in-depth interviews with employees at 82 Fortune 500 companies, identified two startling results:

- 1) Spam is definitely on the rise. The average employee received nearly 7,500 spam messages in 2004, up from 3,500 in 2003.
- 2) Employee productivity continues to be hurt. Average lost productivity per employee was 3.1% in 2004, up from 1.4% in 2003.

It's not surprising that spam continues to present serious security and resource risks to an organization's infrastructure: overloading systems, clogging mailboxes, defrauding recipients, reducing employee productivity and draining morale. It also increases the frequency, severity and cost of virus attacks and related threats, such as the damage to an employer's reputation from inadvertently sending spam or viruses. As a result, companies are faced with the ever-increasing challenge of not only reconciling inherent problems caused by spam, but also protecting themselves from on-going attacks. With such a foreboding technological landscape, at times even the most tech savvy IT administrators are hard-pressed for what to do.

What's even more disturbing about the rapid proliferation of spam is the highly evolved nature of spammer tactics. Originally, spammers used their own servers and thereby devised techniques to avoid blacklists, a feature of anti-spam software that allows users to designate IP addresses, domain names, and individual email addresses from which no mail will be accepted. The spammer then advanced to disguising messages and disabling spam filters. Today, they rely on virus writers and hackers to provide a constant supply of servers to hide their identity and generate huge volumes of mail. This is not a pretty sight.

Consider this: A typical spam message combines several techniques to elude capture. It might originate from a virus-infected or hijacked system on a consumer or business network, for example, or incorporate multiple redirected URLs to avoid detection of known spam Web sites. Spammers also might use both text and HTML message obfuscation techniques to disguise content. To avoid signature detection, spammers are incorporating multiple hashbuster strings or adding a “word salad,” a term given to a spammer technique that is supposed to fool filters into not tagging a message as spam. The technique involves hiding or attaching a list of supposedly non-spammy words to spam messages.

Indeed, industry experts estimate that approximately 40% of spam is now sent from hijacked consumer systems with more than 800 new viruses discovered each month – many looking for new ways to take control of computers for the purpose of sending spam. Once infected, these hijacked computers act as “zombies,” waking up and operating at the virus writer’s or hacker’s command, providing a service to spammers until they are disinfected from within the organization or blocked by blacklists. In addition, viruses often include methods to replenish the supply of zombie machines, such as using built-in Simple Mail Transport Protocol (SMTP) engines to forward themselves to email addresses found on a user’s hard disk.

Through these means, spammers gain ready access to a constant supply of servers that can act as proxies and relays to hide message routing. Or, better yet, spammers simply steal the identity of the original owner’s server and use their legitimate credentials to bypass blacklists or take advantage of whitelists – trusted external email addresses, IP addresses, and domains – to get their messages through.

It is because of these innovative and chameleon-like spamming techniques, along with the continuous rise of spam itself, that anti-spam and anti-virus filtering companies have become vital to enterprises, government institutions and educational organizations. Vendors are responding to new, more complex spamming techniques by developing new, equally sophisticated detection methods. Therein lies the cat and mouse game.

A Look Under the Hood

How do anti-spam and anti-virus filtering companies keep spammers in their sights? One such spam sniper is Minneapolis-based **Securance**, a leading provider of email filtering (anti-spam, anti-virus software) and Web filtering services that include email protection and security services for small businesses, enterprises, and educational and government institutions worldwide. The company’s unique solutions help protect companies and their employees by

scanning email and eliminating threats, such as viruses, worms, malicious content and attachments, and other junk mail before reaching the end user.

Before taking a closer look at Securrence, a quick aside on how email is delivered. In today's email world, all mail is born either legitimate or illicit. From here, the delivery process is rather straightforward. The originating mail server delivers email to the destination mail server via SMTP, with both servers having an IP address. Simply put, think of two phone numbers trying to connect.

In the case of a company using Securrence's email filtering solution, SecurrenceMail, when an email is sent to its mail server, the email is initially redirected to Securrence through its MX record, which is short for *mail exchange record*, an entry in a domain name database that identifies the mail server responsible for handling emails for that domain name. (The MX record points to an array of servers that run in Securrence's data centers in Minneapolis and Milwaukee.) Before an email can be accepted by Securrence's system and delivered to the recipient, a series of steps must occur to ensure "clean" delivery. This cleansing process is also known as "filtering."

"What we're basically doing," says Travis Carter, VP of Technology at Securrence, "is looking for internet rodents."

Assuming an optimal configuration environment, as soon as an outbound mail server connects to Securrence, the first thing Securrence does is determine its IP address. "If someone wants to send an email to Johnny@domain.com through our system, we need to identify the server managing the incoming domain's mail," he says. "While the server managing the domain's mail oftentimes isn't the same as the one that sends the messages out, we know the difference."

Next, Securrence evaluates the settings applied to the receiving domain. If Securrence determines that the IP source is on a Real-time Black List (RBL), a vast, ever-changing, yet publicly available list of IP addresses that are known as spam sources, it disconnects immediately from the originating mail server and, as part of the SMTP protocol, the sender is informed that the message was refused as well as why. (Some industry experts also refer to this list as a DNS Black List, or DNSBL).

Once the IP source has been authenticated, Securrence applies a whitelist filtering application. All mail from these addresses is delivered, thus bypassing the spam filters. However, the whitelist is only applied *if* the IP address was not listed on an RBL.

Once the RBL and whitelist filtering actions have been conducted, a process called User Verify follows. Here, Securrence attempts to verify if the user is on a special list that consists of pre-determined email addresses for a single domain. “If you’re not on the list, then you don’t get in,” Carter says.

“User Verify is an extremely effective anti spam method,” Carter says. “It’s responsible for blocking over half of all our spam volume, and it keeps spammers guessing when they try email harvesting, such as a dictionary attack.” (A dictionary attack is a program that bombards a mail server with millions of alphabetically generated email addresses in the hope that some addresses will be guessed correctly, such as Bob@domain.com, Bob1@domain.com, Bob2@domain.com, and so on. This technique is also used to crack passwords.)

Adds Carter, “Another benefit of User Verify, from an IT administrative support viewpoint, is that a company’s email server only receives mail from real users. This is nice because it means that tech support will only see email for known valid users in their quarantine or forward sandboxes. Relaying these to their rightful owner can be quite labor and resource intensive.”

After these two counter-measures have been deployed, Securrence applies still another filtering method called Spammer Tricks, which is meant to catch spam tactics that try to bypass mail servers and filtering procedures. If an email is given the green light, it is still subject to yet another RBL/User Verify screening, followed by a static whitelist and static blacklist filtering process. Finally, Securrence applies a spam signature test, which is the single largest difference between its solution and that of other competitors on the market.

“All of this may seem over the top, but spam is a serious problem, and we take it very seriously,” Carter says.

Once an email has successfully passed these anti-spam filtering stages, meaning no trigger was activated that resulted in the message being deleted or quarantined, the email enters its final leg of the cleansing process, namely, an anti-virus scan. As part of the SecurrenceMail

anti-spam and anti-virus solution, Norman AntiVirus and Clam AntiVirus are deployed. Norman not only disinfects an email, but also uses Sandbox technology to spot viruses that don't yet have a signature. Clam, on the other hand, which cannot disinfect, is useful in searching for viruses because of its open source architecture, like the popular Linux operating system. Clam has advanced mechanisms that protect against new types of malware, including image and HTML exploits, as well as phishing attacks. (Phishing, pronounced "fishing," involves creating a replica of a legitimate web page to hook users and trick them into submitting personal or financial information or passwords.) By combining these two anti-virus technologies with a number of anti spam filtering techniques, SecurrenceMail delivers a powerful solution fast – usually in less 700 *milliseconds* – and one that boasts a 98% success rate with virtually zero false positives.

"This is where the rubber meets the road," Carter says. "The entire email filtering process is for naught, no matter who goes about doing it or how, if legitimate email is being trapped." One month recently Securrence had more than a billion emails run through its system with only 117 false positive tickets.

Two Brief Case Studies of Organizations Using SecurrenceMail

The RE/MAX International network of about 85,000 Sales Associates in more than 4,600 offices in 44 countries is as culturally and ethnically diverse as the communities in which Securrence affiliates serve. With unsolicited email at an all-time industry high in the summer of 2002, ensuring the safety, security, and confidence of RE/MAX's 43,000 email accounts became a challenge that could no longer be ignored. According to Kristi Graning, Vice President of Web Services & IT Marketing at RE/MAX, "Spamming companies figured out that we had a naming scheme under remax.net, and so they systematically generated email addresses that were associated with it and then sent out spam accordingly."

Adding to RE/MAX's woes, says Graning, after these spammers found out which email addresses were valid, they started selling those email names to other spammers, which only compounded the problem. In searching for a solution, "we became very frustrated, especially because of the high figures quoted by third parties," Graning says.

After RE/MAX tested SecurrenceMail for a one-week period, the real estate company made the move permanent. "During the first day, we saw a 59% drop in the load on our email server," Graning says. Initially, Securrence engineers were surprised at such a low number because most industries have a spam infiltration rate of plus 90%. However, after detailed

reports came in, everyone was assured the figure was accurate and no false positives were being reported.

RE/MAX agents were delighted. “They didn’t know what we had done,” Graning says. “Within 48 hours, we were receiving phone calls from them, saying, ‘Something’s different. What did you do?’ Or, ‘Is there something wrong with my email? I’m hardly getting any spam.’”

Another example of an organization that experienced immediate relief when using SecurrenceMail is Albuquerque Public Schools (APS). With an email platform of 10,000 users, APS found themselves hard-pressed in the fall of 2003 to effectively cope with the relentless amount of spam they were receiving. According to Demetrius Brandon, APS Manager of Core Services, user and end-user complaints had reached unacceptable levels. “Massive amounts of spam were reaching their desktops on a daily basis,” he says. “It was not just a nuisance anymore, but rather a real productivity issue.”

Up to this point, no formal anti-spam solution had been deployed at APS. Instead, Brandon offered advice: “Be conscious of who you share your email address with.” However sound that advice, it was time for a change. Even his supervisor requested he look into the ever-present spam situation.

After Brandon researched several email filtering options, he decided to try two solutions under a two-week free trial program: SecurrenceMail and Barracuda. “When we gave Securrence a try, spam levels dropped from 15,000 a day to less than 100,” Brandon says. “(Securrence) did very well. Plus, it was easy to set up and the cost was very competitive.

“Then we tried Barracuda; I had read a positive review about them in an industry trade magazine. But we didn’t get kind of results we expected. Unacceptable spam levels were still reaching our users desktops, and so we went with the more cost-effective solution. Looking back, we’re very pleased with our decision. Securrence has consistently performed well in addressing our spam issue and on-going management has been minimal.”

Securrence Provides Complete Protection

Securrence is a trusted, global provider of integrated anti-spam and anti-virus solutions. The company’s unique solutions help protect organizations by scanning email and eliminating threats, such as viruses, worms, malicious content and attachments, and other junk mail before

reaching the end user. To this end, Securrence is uniquely positioned to deliver the experience and technology needed to secure organizations against the risks posed by the new spam economy.

“We are dedicated to analyzing new threats and developing effective detection methods with rapid response procedures to ensure that customers are automatically protected as new tactics arise,” Securrence’s Carter says.

SecurrenceMail provides total protection against spam and viruses at the gateway. It typically blocks over 98% of spam and allows businesses to create and enforce custom email policies to further reduce the threat of unwanted email entering or leaving an organization.

SecurrenceMail is complemented by round-the-clock virus protection through Norman AntiVirus and Clam AntiVirus. This integrated multi-layer technology is fully scalable with flexible administrative management tools. By providing consolidated protection against the convergence of spam and virus threats, Securrence offers organizations significant business and operational efficiencies, and lowers the total cost of ownership of anti-spam and anti-virus security.

Conclusion

Spam and viruses are a growing and rapidly evolving security threat. With the increasing aggressiveness of spam campaigns and the high level of sophistication of spammer networks, businesses need an email protection vendor with expertise in all the areas related to the spam problem. Securrence’s advanced technologies provide effective consolidated protection – not just against spam, but also against viruses – in helping businesses stay one step ahead of the spam onslaught.