

## Less Screaming, More Screening

Messaging **security platform** protects Burlington Coat Factory from the cyber elements

BY M.V. GREENE

Like many organizations with sophisticated enterprise network investments to protect, Burlington Coat Factory Warehouse has drawn a line in the sand against spam.

Matt Marchione, MIS security analyst for the Burlington, N.J.-based clothing, footwear and accessories retailer, cringes at the impact of the seemingly endless, un-



ton and other organizations are up against. Image spam, in which a message is embedded in wallpaper within an e-mail, is a relatively new kind of spam issue – and a troublesome one, as the embedded images are often able to bypass many spam filters.

McAfee Avert Labs, a security threat and research organization operated by Santa Clara, Calif.-based security technology firm McAfee, found that image spam



## Spam and other network intrusions are more sinister than at any time in the past

solicited and typically fraudulent e-mail his corporation has to contain amid the hundreds of thousands of inbound messages it receives each day.

“Nuisance, junk, garbage” are the terms Marchione uses when characterizing spam. He expresses greater amazement at the misdeeds of cybercrooks who seek to contaminate corporate enterprises with viruses, parasitic malware, bots and rootkits. Then there is phishing, whereby bogus sign-in pages are

created in an attempt to extract personal and financial information from the unsuspecting.

“You’re trying to clean up the junk that finds its way into people’s inboxes and keep people productive,” Marchione says. “If they’re spending their time having to clean up all this unwanted garbage, then that is less time that they’ve got to be productive.”

A recent surge in the use of so-called “image spam” illustrates what Burling-

accounted for up to 65 percent of all spam during the first half 2007, compared with 10 percent in 2005. Image spam typically is used to advertise stocks, pharmaceuticals and degrees, according to McAfee Avert Labs. The image can triple the size of an e-mail message, thus absorbing significantly more network bandwidth.

As it lacks a searchable URL or a consistent HTML pattern, image spam is typical of how spammers currently op-

erate, Marchione says. "They've become much more sophisticated and much more prevalent, and you're seeing a major increase in volume," he says. "They're always out looking for the latest operating system vulnerability to ... exploit."

### Attack the postmaster

Besides serving as a distracting nuisance, spam guzzles resources from an organization. One spamming technique, for instance, is to go after the network's postmaster, sending spam from a non-existent person in one organization to someone in another. The message gets bounced back to the webmaster of the initial organization as undeliverable. "We have to take it back, even though we never sent it," Marchione says.

In June, the New Jersey state Senate unanimously approved a bill that would expand on provisions of the federal CAN-SPAM Act of 2003 by establishing criminal and civil penalties for activities often involved in the widespread distribution of spam. The bill would prohibit using a computer located in New Jersey to relay or transmit multiple commercial spam messages to mislead recipients or service providers about their origins.

It would also ban registering for multiple e-mail addresses or domain names with false information to transmit spam

or accessing another computer without authorization and using it to transmit multiple spam e-mails.

While laws like CAN-SPAM are helpful, corporate enterprise security analysts continue to plow ahead to ensure the security of their respective networks.

"There is always some kind of new little technique that the spammer can sit there and try until he is successful in reintroducing his old messages again," Marchione says.

In its quest to trump the spammers, Burlington contracted with Cupertino, Calif.-based Proofpoint, a provider of large-enterprise messaging security solutions, in 2005, and recently upgraded to the latest version of Proofpoint's messaging security platform, Proofpoint Protection Server 4.

Proofpoint says traditional anti-spam solutions evaluate limited attributes in messages and typically are not able to decisively classify spam. The result is low effectiveness and a high number of misclassified messages. Its solution had an average effectiveness rate of 99.6 percent during March 2007, the company says.

Marchione says it was vital to find a solution that minimized manual intervention and maintenance while still providing a superior level of protection and user flexibility. "You don't want to have someone having to baby-sit the thing

24/7 or on a daily basis," he says. "You basically want to empower the user. They should have control [over] what they want to let through and what they don't want to let through."

### More sinister

The bottom line, Marchione adds, is that the solution "has to let the legitimate stuff through and keep the junk out."

Steve Gottwals, Proofpoint director of product management, says spam and other network intrusions are more sinister than at any time in the past. Approximately four years ago, spammers and cybercriminals shifted their focus from shutting down an organization's network for the sheer joy of it through now-legendary worms like "Love Letter" and "Melissa" to seeking opportunities to capitalize financially through identity theft and credit card misuse.

"Some of the old patterns would bring down a host or bring down a server and they would become obvious," Gottwals says. "The new attacks are very, very dangerous in that they want to remain hidden beneath the covers on the computer." **STORES**

---

*M.V. Greene is an independent writer and editor based in Owings Mills, Md., who covers business, technology and retail.*

# proofpoint<sup>™</sup>

## US Worldwide Headquarters

Proofpoint, Inc.  
892 Ross Drive  
Sunnyvale, CA 94089  
United States  
Tel +1 408 517 4710  
Fax +1 408 517 4711

## Asia Pacific Headquarters

Proofpoint, Inc.  
56 Berry Street  
North Sydney  
NSW 2060  
Australia  
Tel +61 02 9455 0289  
Fax +61 02 9455 0001

## Japan Headquarters

Proofpoint Japan K.K.  
906 BUREX Kojimachi  
3-5-2, Kojimachi, Chiyoda-ku  
Tokyo, 102-0083  
Japan  
Tel +81 3 5210 3611  
Fax +81 3 5210 3615

<http://www.proofpoint.com>  
[info@proofpoint.com](mailto:info@proofpoint.com)