

# Spam slammers

BY RICH FREEMAN

Photograph by Robert Houser

F5 and Secure Computing are teaming up to help businesses stop unwanted e-mail from burdening their networks—and IT budgets.

**WANT TO KNOW** one of the tech industry's dirtiest little secrets? Spam may be one of the best things that ever happened to it. Not that IT vendors have the slightest fondness for spam, mind you. But there is no denying the positive impact junk mail has had on their cash flow.

According to Stamford, Conn.-based analyst firm Gartner Inc., up to 70% of a typical organization's incoming e-mail is spam. And research from Secure Computing Corp., a leading enterprise gateway security company based in San Jose, Calif., shows that the volume of spam hitting most corporate networks doubles every six to nine months. To process all of those unwanted messages, businesses must spend heavily and continually on bandwidth, e-mail servers, antispam solutions, and



Secure Computing's Farzad Tari (left) and F5's Phil de la Motte say their companies' collaboration helps to stem messaging infrastructure costs for customers.

other network resources they wouldn't otherwise need.

Working in partnership, however, Secure Computing and F5 Networks have found a novel but powerful way to spare businesses from the high price of keeping pace with spam: Stop spam from reaching the network in the first place.

### Spam-induced spending

F5 first began thinking about spam late in 2005, when a large customer struggling to keep ever-increasing torrents of junk mail from bogging down its network made a plea for help. "They said it was the equivalent of a perpetual denial-of-service attack," recalls Phil de la Motte, a business development manager at F5 who works with Secure Computing.

Many other F5 customers were in the same boat. Numerous vendors, including Secure Computing, make sophisticated content inspection appliances that reliably filter spam out of the e-mail stream. Like all network devices, however, such systems have capacity limits, so the more spam a business gets, the more antispam devices it must buy.

And the spam-induced spending doesn't end there. Many organizations are

subject to strict government regulations requiring e-mail retention practices (for example, Sarbanes-Oxley section 404, SEC 17a 3&4, NASD 3110, FDA 21 CFR Part 11, and HIPAA). In some cases, companies store every message received, whether spam or not.

Complying with such mandates forces organizations to purchase huge amounts of additional storage capacity. "That's extremely expensive, and it's data they're just going to erase eventually anyway," observes Alan Murphy, a technical marketing manager for security at F5.

Of course, if businesses could block even a portion of spam at the edge of the network—before it impacted their infrastructures—they could slash their need for all those costly, added resources. A thought soon occurred to F5's engineering team: Why not add message filtering functionality to BIG-IP? After all, BIG-IP already sits at the network's border, inspecting incoming traffic. All it needs to become a powerful spam reduction tool is a reliable means of distinguishing good e-mail from bad.

That is exactly what Secure Computing's TrustedSource™ service provides. TrustedSource is an identity reputation engine that helps organizations evaluate whether or not to accept an inbound message based on the sender's past behavior. Drawing on a rich historical database of legitimate and illegitimate messages, TrustedSource dynamically ranks IP addresses as good, bad, or suspicious.

"Put simply, we look at the host sending an e-mail, and if it's coming from a reputable sender, we take it. If not, we don't," says Farzad Tari, Secure Computing's vice president of business development. "It's

like a credit score, but for Internet identities," adds Dmitri Alperovitch, a principal research scientist at Secure.

TrustedSource isn't the only reputation engine on the market, but extensive research soon convinced F5 that it was the right one for its needs. "We definitely did our homework," de la Motte says. "We decided that Secure Computing not only had the best technology, but they were the best known in the market. We wanted to go with someone everyone knew and respected."

### Putting brakes on infrastructure growth

F5 and Secure started developing their network-edge message filtering product—ultimately named BIG-IP Message Security Module (MSM)—early in 2006. By November they were finished.

Tari gives much of the credit for that quick turnaround to the spirit of camaraderie between the two companies. "The working relationship has just been amazing," he says. Further credit, he adds, belongs to F5's flexible architecture, which made developing MSM extremely fast.

For spam sufferers, that simple script delivers big benefits: MSM helps businesses keep around 70% of spam outside the firewall. Leveraging TrustedSource's highly granular IP address scoring, MSM also gives network administrators fine-tuned control over the messages they do accept. For example, they can configure the system to route suspicious messages to a quarantine site for closer inspection, forward less dubious messages to the next layer of antispam inspection devices, or even fast-track messages from particularly trustworthy sources to a fast-track pool of antispam systems.

Technicians can also take advantage of BIG-IP's traffic management functionality to load balance their antispam appliances, diverting traffic away from overloaded machines.

All of that adds up to substantial savings on infrastructure expenses. "We allow customers to stop growing their messaging security infrastructure, or at least slow down the growth significantly," says de la Motte.

In fact, according to data from Secure Computing, TrustedSource alone can save a typical business with 5,000 users more than \$145,000 a year on bandwidth, storage, and antispam hardware.

Among the companies eagerly anticipating such returns is F5 itself, which is currently rolling out MSM internally. According to Casey Scott, a network administrator in F5's IT group, deploying a new MSM device takes him no more than an hour. "Not having to roll out another antispam server for the next year or two by doing an hour's worth of work now is fantastic," he says.

So is relieving the strain on F5's e-mail servers, he adds. "If we can cut the load on those servers in half, we're going to immediately see a significant financial benefit," Scott predicts.

For his part, Tari expects MSM to be the first of many instances in which F5 and Secure Computing help businesses improve their efficiency and save money. "Both companies have a history of innovation," he notes. "Given that shared heritage, we're sure to continue innovating again and again." \*

*Rich Freeman is a Seattle, Wash.-based freelance writer who specializes in business and technology.*

#### Additional resources

**Online tool for calculating the likely ROI on a TrustedSource solution**  
([www.trustedsource.org/roi\\_calc.php](http://www.trustedsource.org/roi_calc.php))

**A white paper on MSM**  
([www.f5.com/solutions/technology/msm\\_wp.html](http://www.f5.com/solutions/technology/msm_wp.html))

**A white paper on TrustedSource** ([www.f5.com/solutions/partners/tech/trustedsource\\_wp.pdf](http://www.f5.com/solutions/partners/tech/trustedsource_wp.pdf))