TECHNOLOGY

By John Draper

Guerrill@Tactic$

War on spam may see no end

as both sides build arsenal

UNSOLICITED bulk e-mail aimed at selling the recipient everything from hot stocks to pills enhancing sexual performance threatened the whole foundation of Kyle Bender's business model.

"I do e-mail blasts for customers that have lists of up to 5,000 customer e-mail addresses, and I was getting spam on returns from their e-mail servers. I would get hundreds of unsolicited offers coming in, so I would have them go to a spam folder," says Bender, president of Puyallup-based Pacific eMarketing. "These spammers would then affect the way my e-mail server was being perceived. I started getting more blacklist notices, which hurts my deliverability ratio for my customers. It was a vicious cycle."

Bender is not alone; spam seems to be everywhere online these days. Dealing with spam's pervasiveness has spawned a cottage industry in preventive software. But perhaps even more valuable are third-party companies that manage spam.

A growing number of companies offer services to keep the spam out of your in-box. International Data Corp. (IDC), an Internet research firm, estimates worldwide revenue for anti-spam solutions will exceed $1.7 billion in 2008, far surpassing the $300 million generated in 2003. IDC cites the development of spam from a mere nuisance to an increasingly serious problem that is the driver for explosive revenue growth, innovation and investment in the anti-spam market. IDC further suggests that worldwide revenue for antispam solutions will have a compound annual growth rate of 42 percent through 2008.

The problem is that, as with viral strains in the biological world, spam is mutating. Spammers, for example, are avoiding anti-spam spotlights by hiding content in pictures, and they are multiplying in countries such as Russia, China and Nigeria. Bill Gates once said spam would be gone by 2006, but today spam accounts for as much as 80 percent of all Internet e-mail. (Spammers can churn out 200 million or more messages a day, and all that is needed to make a handsome profit is less than a 1 percent return.)

"I think of it as an 'arms race,'" says Oren Etzioni, a University of Washington professor of computer science and an Internet expert. "Filtering technology gets better. Then the spammers figure out a way to defeat it. Then filtering technology gets better again, and so on.

"As long as there is a strong economic incentive for sending spam and people respond to it, then spammers will find a way to continue. Unlike direct mail or telemarketing, e-mail marketing has very low marginal cost. As a result, despite extremely low response rates, spammers can make a profit fairly easily. The more e-mails a spammer can send, the greater his profit, while the cost remains nearly constant."

CRAWLING FOR ANSWERS

The spammers use software "spiders" to harvest e-mail addresses off the Internet. The spiders methodically scan websites, gathering e-mails along the way. Also, the spammers have programs that generate millions of e-mails using combinations of letters and numbers, such as "johndoe@companyX.com."

The most common anti-spam approach is filtering, where spam is weeded from incoming mail. This legwork is done by third-party companies such as Puyallup's Big Mountain Web Hosting and Design.

"Most of my customers have started assuming that spam is a normal course of everyday business that they don't have much control over. But after having their mail filtered for them by Big Mountain, they realize how nice it is to not have to deal with it," says company president Jon Clayton.

Big Mountain offers two services. "If we are providing your e-mail service, then we can take all your inbound messages and put them through our firewall, which has several layers of protection. Then we will forward the mail through our server, which has another spam filtering system. Then the e-mail is delivered to the customer's in-box. Secondly, if we are not providing your e-mail service, we can pass your e-mail through our firewall and then send it to the customer's server," Clayton says.

CHALLENGE AND RESPONSE

But filters can run the risk of inadvertently blocking desirable e-mail, and spammers have become increasingly adept at creating spam that masquerades as ordinary e-mail, Etzioni says. Still, Clayton says his company can block 98 percent of the incoming spam.

While filtering services such as Big Mountain provide the bulk of anti-spam service, a new upstart known as "challenge/response" is emerging.

"The problem with filtering is that it is a constant battle to outsmart the spammers," says Daryn Nakhuda, CTO of Seattle-based challenge/response provider SpamArrest LLC of Mercer Island. "They [spammers] can install the exact same filters on their end and tweak their messages to get by them. There are newer classes of learning/statistical filters that are better, but they are still subject to the same problems."

The way challenge/response works is that when someone who is not on your approved contact list tries to send you an e-mail, the challenge-response system will immediately e-mail them asking them to identify themselves. The system will ask them to fill in a code in a puzzle – known as a challenge graphic. This is meant to discern human e-mail senders from machine-generated spam lists. Then they are added to your contact list, and the e-mail is sent. When SpamArrest's clients send out e-mail, the recipients are automatically added to the "okay to send" list, so that they do not need to authorize themselves in order to reply.

UPPING THE ANTE

Yet, faced with this big weapon, spammers are coming back with an even bigger one: hiring sweatshop workers to manually respond to the puzzle.

"Challenge-response is far from perfect, but in our implementation, which has been in use for five years now, we've addressed many of the complaints. Properly configured, a SpamArrest account can block 100 percent of the spam and have zero false positives," Nakhuda says.

The counter-argument? Communication slowdown and fewer sales. Clayton says potential customers will bail out if they have to do more. Either way, the cost to companies is substantial, particularly when the number of employees having to identify and delete spam reaches the billions. There's also the financial burden on the companies that operate within the Internet infrastructure. Hotmail, for instance, estimates that it receives more than one billion spam messages a day, and that number is growing.

Etzioni and Nakhuda hold out little hope that the battle against spammers is winnable as long as spammers can make money from spamming.

"In the end, the only thing that will beat the spammers is the easiest thing. Don't read the spam, don't fall for their scams and never buy anything from a spammer," Nakhuda says. "It is hard to believe, but people do buy from them, and the cost/profit ratio to the spammer is so small that as long as they can lure a few suckers in, it's worth it to them to keep sending millions of e-mails out."

John Draper is a Puyallup-based freelance writer.