[Note from M. E. Kabay: My good friend and colleague Stephen Cobb sent me this good news about progress in the fight against spam. Introducing delays into network responses is a well-established approach to interfering with automated attacks; for example, automated dictionary attacks on passwords via logon interactions can be stymied by a two- or three-minute delay every few wrong-guesses. I’m glad to see someone implementing this technique to deal with the wretched people who are abusing the ‘Net with their floods of junk.

As a matter of full disclosure, I (MK) have no commercial relation whatsoever with the vendor named in the following article. Please communicate directly with Stephen Cobb for all commentary about this article.]

* * *

Networks can use time to stop spam – and I mean this quite literally. People may argue about the definition of unsolicited bulk e-mail or spam, but nobody disputes the fact that it continues to grow in volume, month after month, despite lawsuits and legislation (spam is already illegal in 30 states and, since most spam is commercially deceptive, much of it is a violation of the Federal Trade Commission Act).

And nobody disputes the fact that spam places network administrators between a rock and hard place, where the rock is user complaints and the hard place is mail servers that are groaning and, all too often, collapsing, under the weight of expanding spam traffic. Security officers are being challenged as well, by spam’s threat to uptime and availability, and its growing popularity as a distribution mechanism for malicious code and fraudulent scams.

Unfortunately, but perhaps understandably, the most common choice for anti-spam defense is filtering. This assumes spam is akin to malicious code, something you can readily identify and quarantine. But spam is the Achilles of e-mail threats, at once more powerful and yet more vulnerable. If you doubt the power of spam, talk to your local ISP. When a spammer targets your domain you can be staring down the barrel of a spam cannon firing 6 million messages an hour (entirely possible using an OC3 and a six-pack of optimized MTAs equivalent to the Ironport A60).

Some Spam will always beat filters. This is because spam shares so much digital DNA with legitimate high volume e-mail--like this newsletter or my Discover card payment reminder--as to be practically indistinguishable. Rachet up the filters and you loose wanted e-mail. As for blacklisting as a spam defense, that is now fraught with problems too numerous to mention.

And spammers have a strong incentive to beat filters and blacklists: economics. Unlike virus writers, spammers are in it for the money. Which turns out to be good news, because that is also their Achilles’ heel. Consider what happens to a spam cannon when the target network is so slow, most of the messages don’t even leave the barrel: It moves on to the next target. In other words, if you can’t get a network to accept a high rate of messages per minute, there is clearly no
money to be made there, and you move on.

I know this because my colleagues in ePrivacy Group’s anti-spam laboratory figured out how to make a large network appear—to spammers—as though it is very slow. When they tried this trick at an ISP whose servers had been collapsing under relentless spam attacks, the effect was immediate and quite astonishing. Spam attacks were either repelled or displaced. The good e-mail came through faster, without false positives, and server loads returned to manageable levels while user complaints plummeted.

The techniques used to accomplish this, a combination of traffic analysis and traffic shaping, have now been “productized” in an appliance that can be dropped into place between the Internet and an organization’s e-mail servers. The technology, appropriately named SpamSquelcher, works best when it is applied to networks of 5,000 mailboxes or more, and it can be an effective complement to filtering strategies. That’s because spam squelching eliminates the biggest weakness of filtering: the need to receive all the messages that a spammer sends in order to then decide which are spam and which are ham.

Whether you filter in-house or through a service, the spam has to be accepted by someone before a filter can look at it—which actually tends to increase spam volumes. Besides, if your first line of defense is squelching, rather than filtering, you can not only win back valuable server capacity, but also enjoy the distinct pleasure of knowing you are making life more difficult for spammers. And maybe, if enough networks adopt this strategy, the age of spam could come to an end, finally done in by the manipulation of time.

* * *

About Stephen Cobb:

Stephen Cobb, CISSP, is the author of _Privacy for Business: Web Sites and E-mail_ (Dreva Hill, 2002) and two dozen other books. In addition to teaching Information Assurance at Norwich University, Vermont, he is a senior vice-president at ePrivacy Group, the developers of SpamSquelcher(TM). Stephen can be e-mailed as scobb at either cobb dot com or eprivacygroup dot com.

* * *

For further reading:

SpamSquelcher <http://www.eprivacygroup.com/article/articlestatic/57/1/6>


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Stephen Cobb. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.