Spam is a major operational problem for all professionals because of its waste of bandwidth; it is a significant nuisance even for non-professionals, contributing to computer-based crime and increasing doubts about e-commerce. I recently interviewed Cloudmark CTO Jamie de Guerre via e-mail and am pleased to convey our discussion in a two-part report.

1. How’s the spam? We hear estimates of anywhere from 75% to 90% of the total bandwidth of the Internet is being wasted by unsolicited commercial e-mail; what do these experts find?

Cloudmark provides spam filtering for the world’s largest e-mail providers including 11 of the top service providers in North America. Over 96% of all e-mail sent to these operators is spam today.

2. Are there regional variations in spam? That is, are different parts of the world receiving different amounts of spam and are there differences in the origination frequency by geography?

Yes, there are differences in both the amount of spam received and generated by different regions.

North America is definitely the leader in _receiving_ spam. As I mentioned, over 96% of all e-mail received by large North American operators is spam. That number is quite a bit lower in Europe – only around 85% of all e-mail received by large European operators is spam. In Asia, the number is similar, around 80% of all e-mail received by major Asian operators is spam.

The following graph shows the percentage of spam generated by several of the top sources of spam in the world, by country:
3. Has the legal situation improved any? Some years ago, I wrote a column with my favorite title of all time: “Can CAN-SPAM Can Spam?” Obviously, it hasn’t. Are there any legal measures that you think would be of any use at all in fighting spam?

Yes, the legal situation has improved; however, the impact is negligible. Efforts by organizations to track down attackers have increased. There have also been some successful prosecutions. However, these actions have had a relatively small impact on the amount of spam and on the attackers. The rate of successful prosecutions has been slower than the growth of the attacking community by orders of magnitude.

The attacking community is now a sophisticated, mature market economy. The combination of widely available services from advanced researchers enabling anyone with malicious intent to join the attacking community has dramatically lowered the barrier of entry for a wide network of wannabe hackers to conduct sophisticated and malicious attacks. While the legal situation has improved, at this point, the outlook is grim for any hope of it having real impact.

The spammer community has grown rapidly over recent years. It has perfected the underground open-market system for trading of services, wares and cash. Today, the most advanced attackers are not actually committing fraud themselves—they’re now selling their services (e.g., botnet time shares, exploits, spyware) to a broader, lower-skilled open community of new attackers. The best hackers operate research and development departments with PhD-level computer scientists. Their attacks are creative, efficient and innovative. They have expanded their services by providing customer support, reporting services and multiple pricing options for services. Meanwhile, more novice attackers are eager to join the game and they are often even more malicious than their predecessors are and increasingly creative with their social engineering techniques for persuading consumers to pay attention to their spurious offers.
4. Cloudmark has been doing a great job from my perspective: I see very little spam getting by your filters. I really like the whole principle of a community-based rapid response to new spam; anything that does get by the filters can be sent right back to your engine at the click of a button. Are you pleased with the growth of your community and the responsiveness of the members?

Definitely! (and thanks for the praise!)

Cloudmark has been growing rapidly over the past few years. Cloudmark’s solution is not only providing protection for millions of consumers using the Cloudmark Desktop toolbar in their e-mail client, but because our accuracy is significantly higher than other solutions on the market, we have been selected by the majority of the world’s largest e-mail providers to filter spam right at the source—inside network data centers. Today, large service providers around the globe have deployed Cloudmark, and we now protect over 300 million mailboxes and filter 12% of the Internet’s e-mail.

The feedback from all of the users that we provide protection for is an integral part of how we are able to provide the highest possible filtering accuracy. Typically, Cloudmark detects new threats in under a minute.

The interview concludes in my next column.

* * *

About Jamie de Guerre

As CTO, Jamie is responsible for Cloudmark’s technical strategy and roadmap. Additionally, Jamie manages Cloudmark’s Technology Services, Sales Engineering and ISP Support teams, ensuring a tight bridge between customers and internal technical development.

Since joining Cloudmark in 2003, Jamie has played a central role in shaping Cloudmark’s products and technologies. Jamie started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. Jamie was also instrumental in dramatically growing Cloudmark's Global Threat Network, with the invention of the Cloudmark Network Feedback System enabling automatic incorporation of feedback from all subscribers within a service provider's network.

Jamie has spoken at numerous industry events and panels in the areas of e-mail security, mobile technologies and future security threat vectors related to new types of messaging. Prior to joining Cloudmark, he worked at Microsoft on the .NET Compact Framework, where he first began working with service providers. Jamie holds a Bachelor degree with honors in Computer Science from the University of Western Ontario.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of
Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 Jamie de Guerre & M. E. Kabay. 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.