The State of the Spam: 
An Interview with Jamie de Guerre (2)

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

What does the future hold for fighting spam? My two-part interview with Jamie de Guerre, CTO of Cloudmark, concludes today.

5. How do you see Cloudmark evolving? I know that you issue periodic updates to the software — what have you been doing to improve the product?

For e-mail threats, Cloudmark is continuing to innovate. This includes several new road map areas:

1. Cloudmark Sender Reputation

Cloudmark just launched the Cloudmark Sender Reputation Service, a feature shipping on our edge mail transfer agent (MTA) solution, Cloudmark Gateway. This service identifies sources of spam almost instantly around the globe, including rapidly evolving botnets. Cloudmark’s solution traditionally worked at the content layer by filtering messages based on the contents of the message and identifying messages sources in the Cloudmark Global Threat Network as spam, phishing or virus.

2. Outbound Protection, Zombie Identification and Remediation

Cloudmark will be offering service provider a Zombie Identification Service that identifies and remediates bots within their network.

3. Cloudmark ActiveScan

Cloudmark ActiveScan enables highly efficient rescanning of messages—so that even if a spam message gets through initially, Cloudmark can still take action on it as soon as the spam is discovered.

In addition to these improvements in Cloudmark’s e-mail security solutions, we are expanding into other messaging markets that need the same leading edge security that Cloudmark provides for e-mail. The first of these markets is mobile messaging. In many parts of Asia, people already get more spam on their mobile phone over Short Message Service (SMS) than they do in e-mail. This problem is going to grow elsewhere with the growing popularity of mobile messaging and as mobile-service providers enable new services like mobile e-commerce.

Cloudmark’s solution is flexible in filtering any messaging threat. Therefore, Cloudmark will evolve into other new markets that are also start to have security issues and are increasingly attacked by spammers, phishers and other attackers. Stay tuned—you may hear some announcements in this area soon.

6. How do see the battle against bots? Are you focusing on outbound spam?
Yes, as part of Cloudmark’s sender reputation strategy, we are working to identify zombie PCs and providing a real-time Zombie Identification Service to operators as part of our outbound protection offering. We are also partnering with several companies that provide automated remediation solutions and transparent proxy solutions that can filter outbound spam sent on networks that have not closed port 25 (i.e., open spam relays).

7. What's your long-term view of the spam fighting project? Do we have any hope?

Fundamentally, spam is all about economics. As long as e-mail is one of the most popular applications on the Internet attackers will be motivated to evade the latest defenses and find ways to monetize the medium. Therefore, Cloudmark believes in creating security solutions that can evolve and respond quickly to these adaptations and design solutions to enable the fastest possible protection.

8. Will IPv6 significantly improve our chances of winning the battle?

IPv6 will dramatically increase the addressable IP space for the Internet. With IPv4, there are 4,294,967,296 possible unique addresses. IPv6 increases that to $2^{128}$. As it relates to spam, several orders of magnitude more addresses means dramatically more IP space to hide in, making sender reputation based techniques for stopping spam much less effective. Support for mobile handsets, means more sources and destinations for spam and thereby a bigger pool of devices for spammers attack. Finally, IPv6 means that spam will have other media to mutate into including voice and video.

While there are some additional security mechanisms built into IPv6, these do not make a significant difference for spam. So unfortunately, IPv6 increases the threat space and makes things more difficult as opposed to improving our chances of winning the battle on spam.

[Note from MK: for the record, I have no involvement with Cloudmark other than as a paying user of their services.]

* * *

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.