The State of Spam 2009:  
Part 2 – McColo and ICANN

by M. E. Kabay, PhD, CISSP-ISSMP  
Associate Professor of Information Assurance  
School of Business & Management  
Norwich University, Northfield VT

In the next three columns, I’m reporting verbatim the responses of Cloudmark Chief Technical Officer Jamie de Guerre <http://www.cloudmark.com/en/company/staff.html> to a couple of questions I asked him about the state of spam today. Everything that follows is Mr de Guerre’s own text with minor edits.

* * *

What’s changed since last year in the fight against spam?

I think there have been several changes and a couple of events that happened in the past year that are interesting and will have an affect on how spam is sent in the coming year. Those that come to mind include:

- The McColo take down
- Changes made by ICANN to prevent domain tasting and other scams
- Spammers increasingly used free hosting services for their call to action in messages
- Spammers increasingly used free Webmail services to send spam
- Spammers targeting new media such as social networking

First, as you probably know, McColo was a Web hosting firm that was taken offline because their services were being used as a gateway for spam activity.<http://www.networkworld.com/news/2008/111208-isp-cut-off-from-internet.html> The McColo services were being leveraged to host domains used as the call to action in spam e-mails (pharmacy spam in particular), to host command and control servers for major botnets and for other malicious services like child pornography Web sites. Of these, the one that affected spam the most was the takedown of several major command and control servers for major botnets. After McColo went offline, many anti-spam vendors observed dramatic drops in the spam volumes sent to customers. Cloudmark did not see nearly as large a drop off at our major operator customers, probably for two reasons:

- Most major operators block all messages from dynamic IP addresses, which minimizes the effects of botnets, and
- The most advanced attackers conduct targeted attacks on the world’s largest operators, but do not necessarily send those attacks to businesses.

Anti-spam vendors that primarily service businesses probably saw a larger drop in spam volumes than Cloudmark did.

The effect that the McColo shutdown will have on spam in the coming year is that we will see botnets become more advanced and spammers become more careful about how they plan for fault recovery. Some major spammers had become comfortable and grown reliant on McColo without building in reliable capabilities for failover in the event that a major host is taken down. Their failure was not because of technical difficulty but because the spammers became complacent. I think that in 2009 we will see spammers become more careful, an increased use of
more advanced bots, and improved distribution and failover mechanisms. Spam volumes are already recovering quickly as spammers get existing botnets working with new command-and-control servers and deploy new botnets like Mega-D.

Second, ICANN,<http://www.icann.org/> the body that controls and regulates the naming system for the Internet, has made some positive changes to their policies that will interfere with spammers. The main change is one that should significantly lower the ability for registrars and attackers to conduct *domain tasting*. “Domain Tasting” is a practice in which someone uses the “Add Grace Period” (AGP)<http://www.icann.org/en/announcements/announcement-17dec08-en.htm> to use a domain for a short time without paying. This allows people to register and test the marketability of the domain by placing advertisements on the site. However, Domain Tasting can also be used by spammers to send out spam using the temporary domain for responses during the grace period. Spammers know that anti-spam solutions block spam messages from a known bad URL included as a call to action, and so spammers work hard to have as many different domains as possible in their spam attacks so that each message will have a different domain. Loopholes that make it easier for spammers to get domains at low cost help to facilitate the onslaught of spam.

*More next time.*

** * * *

Jamie de Guerre started as a core member of the design team writing the first design specifications for Cloudmark Server Edition and multiple versions of Cloudmark Authority. As CTO, Jamie is responsible for Cloudmark’s technical strategy and roadmap. Additionally, Jamie manages Cloudmark’s Technology Services, Sales Engineering, Product Management, and ISP Support teams, ensuring a tight bridge between customers and internal technical development. You may write to him with your comments.<mailto:jamie@cloudmark.com>

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2009 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.