December 2009 Spam Report

McAfee Labs Discovers and Discusses Key Spam Trends

By Adam Wosotowsky and Elan Winkler

Key Findings

Despite the six-year-old CAN-SPAM Act, spammers routinely abuse the law and continue to deliver their obnoxious email.

One year ago, a major spam-hosting ISP was shut down, causing an impressive drop in botnet activity. Today, however, spam authors are more active and smarter than ever.

Spammers love to tailor their messages to the news and the season. With new online shopping offers, jingle bell spam has begun to ring.

Table of Contents

CAN-SPAM Act of 2003

January 1, 2010, will mark the sixth anniversary of the under-enforced CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act of 2003. During these six years millions of new Internet users have joined the email ranks, and we have seen the amount of spam sent to the average email address rocket upward to peaks as high as 92 percent of all traffic only a few months ago. While we complain about the lack of international support to combat this scourge, we overlook spammers who sit comfortably in the United States, sending out thousands of emails that blatantly disregard the law by keeping their message volumes just below the radar.

Let's look at one of those spam campaigns and see how it breaks the first requirement of the CAN-SPAM Act.

Two noteworthy requirements affect spammers. Each separate email in violation of the act is subject to penalties of up to US$16,000, so failure to comply can be costly. But following the law isn't complicated. Here's a rundown of CAN-SPAM's requirements Nos. 1 and 7:[1]

1. Don't use false or misleading header information. Your "From," "To," "Reply-To," and routing information—including the originating domain name and email address—must be accurate and identify the person or business who initiated the message.

7. Monitor what others are doing on your behalf. The law makes clear that even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.

The latter point is less a requirement and more a threat from the government to tell corporations that ignorance of spam activity is not a defense that can avoid the $16,000 fine *per* spam email sent.

Twitter recruiting spams

The campaign we're following is "Twitter Job" spam. Twitter job spam is not advertising jobs for the Twitter company. It is a scam to get people to create Twitter accounts and send spam to their Twitter followers. Here is an example:

This particular piece of spam gives us two items of information that we can use to determine its identity and hosting:

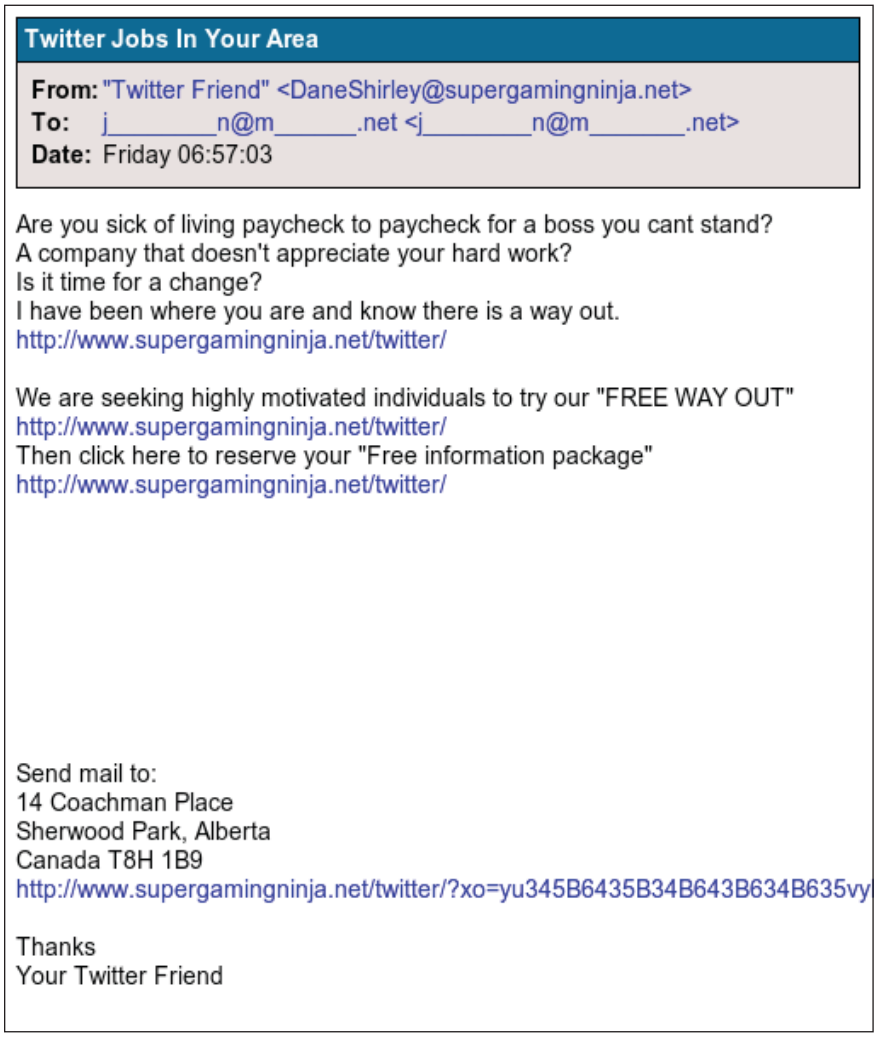
- A received header that shows the message being delivered from the IP address 208.185.61.214
- The domain name supergamingninja.net

The sending IP address

The sending IP address is located in the United States. It is in a subnet that appears to be owned by the Metromedia Fiber Network. Our data indicates that each IP in that subnet from 208.185.61.5 to 208.185.61.244 is involved in sending this exact same spam, well over a million copies in a few days. If they sent only 1,000,000 spam mails, then the fine could be as high as $16 billion.

The spammers won't be there for long, though. These sorts of spam campaigns often move from subnet to subnet as blacklist servers block the mail. Twitter job spam didn't start recently; it has been ongoing for months. Having an entire subnet get blacklisted damages the reputation of the subnet so much that future owners of the address space may find themselves spending considerable time trying to atone for the sins of the previous owner. Companies purchasing address space would be wise to check for blacklisting before finalizing a deal.

1. "The CAN-SPAM Act: A Compliance Guide for Business," Federal Trade Commission. http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtm



Twitter Jobs In Your Area

From: "Twitter Friend" <DaneShirley@supergamingninja.net>
To: j_____n@m_____.net <j_____n@m_____.net>
Date: Friday 06:57:03

Are you sick of living paycheck to paycheck for a boss you cant stand?
A company that doesn't appreciate your hard work?
Is it time for a change?
I have been where you are and know there is a way out.
http://www.supergamingninja.net/twitter/

We are seeking highly motivated individuals to try our "FREE WAY OUT"
http://www.supergamingninja.net/twitter/
Then click here to reserve your "Free information package"
http://www.supergamingninja.net/twitter/

Send mail to:
14 Coachman Place
Sherwood Park, Alberta
Canada T8H 1B9
http://www.supergamingninja.net/twitter/?xo=yu345B6435B34B643B634B635vy

Thanks
Your Twitter Friend

Figure 1: A Twitter spam message.

The domain name

Each one of the 240 IP addresses in the 208.185.61.0/24 subnet that are delivering this spam has a separate domain name associated with the IP address (and the spam inside it). The data associated with these domains is basically the same.

There is a lot of information that can be determined from the domain name; the first is the "whois" information:

Domain Name: SUPERGAMINGNINJA.NET
Registrar: MONIKER ONLINE SERVICES, INC.
Whois Server: whois.moniker.com
Referral URL: http://www.moniker.com/whois.html
Name Server: NS1.MXGAMES40.NET
Name Server: NS2.MXGAMES40.NET
Status: clientDeleteProhibited
Status: clientTransferProhibited
Status: clientUpdateProhibited

Updated Date: 11-nov-2009
Creation Date: 11-nov-2009
Expiration Date: 11-nov-2010

Moniker Online Services will hide the actual identity of the domain's owner, so the latter will appear anonymous to the outside world. This domain was purchased immediately before the spam campaign started. The nameserver associated with supergamingninja is mxgames40.net. The registration information on that domain indicates that it was purchased a couple of weeks before this campaign started.

Each domain is associated with an MX record, naming where it receives email. For supergamingninja that domain name is mx.mxgames40.net. That domain resolves to the IP address 208.73.210.50, which is also known as urlforwarding.moniker.com. This is the common nameserver that Moniker uses to tell web browsers where to go when they want a domain purchased from Moniker. This nameserver does not listen for email, which means that there is no place that the supergamingninja domain gets mail, and no way for a recipient of an email address from that domain to reply to the sending email address. This is a clear violation of CAN-SPAM requirement No. 1, which explicitly prohibits the use of an invalid sending email address.

The web page

The link in the email is just a URL forwarder that sends the browser to a different website. No matter which of the domain names used in this campaign you click on, they all end up at the same URL: securelp.com. Securelp was also purchased a few days before the spam campaign began. The authoritative nameserver for the securelp domain name is 72.32.52.210, otherwise known as web1.prowealthsolutions.com.

Prowealthsolutions.com has a web page that claims not to send spam and implies that only the craziest rogue members of their organization who do send spam would be subject to immediate termination and a paltry $500 fine. According to CAN-SPAM, however, this claim does not diminish Prowealthsolutions' culpability for the actions of their advertisers.

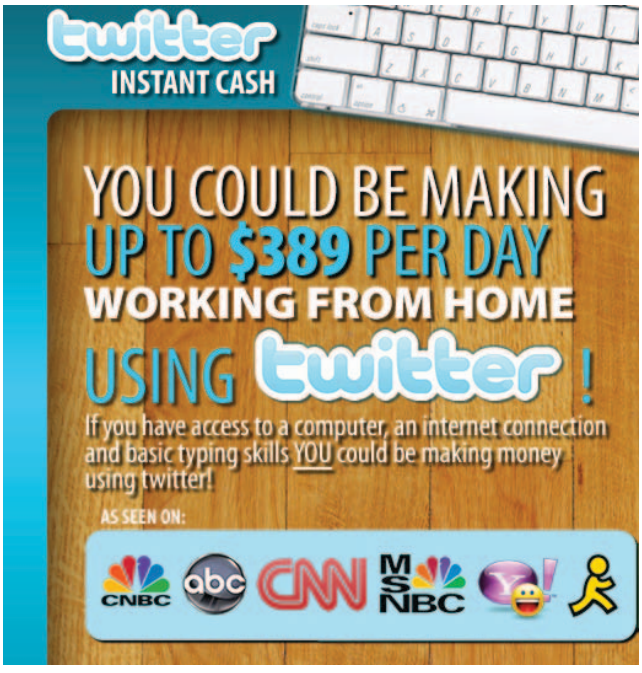


Figure 2: Twitter recruitment web page.

Respect for the law

Spammers find the United States provides low-cost and reliable hosting and anonymous domain registration. The fact that this country is consistently the world's top source for spam shows how little spammers respect the nation's laws. Without ownership transparency in hosting and domain registration, the average spam recipient doesn't know whom to complain to about the spam that they see. Our example is not rare; it is extremely common to see spam campaigns shift from subnet to subnet and from domain to domain as they leave a trail of blocked and useless IP addresses behind them.

The McColo Effect: One Year Later

One year ago, email administrators were astonished to notice the amount of spam hitting their mail servers had plunged precipitously. Email volumes dropped as much as 60 percent to 70 percent. The reason: McColo, a major spam-hosting ISP, had been taken offline. The shutdown started with the work of *The Washington Post*'s investigative journalist Brian Krebs, who drew attention to the hosting company's overwhelming usage of servers associated with scams, phishing, and malware. Three of the largest spam-sending botnets at the time—Rustock, Srizbi, and Mega-D—lost their command-and-control machines that were hosted at McColo. As a result, Mega-D's volume dropped by more than 95 percent and Srizbi volumes dropped by more than 80 percent.

The aftermath

Only days after McColo was taken offline, it was reconnected for a brief period (about 12 hours) by its uplink provider, giving just enough time for the Rustock botnet owners to communicate with their infected machines and point them to command centers at other service providers. Rustock quickly regained its status as a top spam distributor. The Mega-D botnet owners also bounced back, until they were shut down in November. Srizbi, which once accounted for more than 50 percent of spam volume, never recovered and is no longer a factor in today's spam wars.

What has happened since McColo was shut down? Did spam volumes ever recover from the loss of three of the largest spam-sending botnets? Not only did spam volumes recover quickly, unfortunately, but they have greatly surpassed the volumes that we saw before McColo was taken offline.

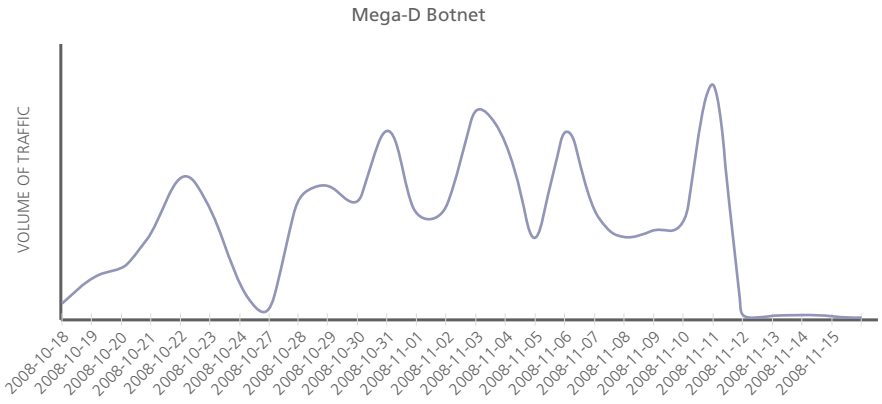


Figure 3: Traffic from botnet Mega-D declined rapidly after the McColo shutdown.

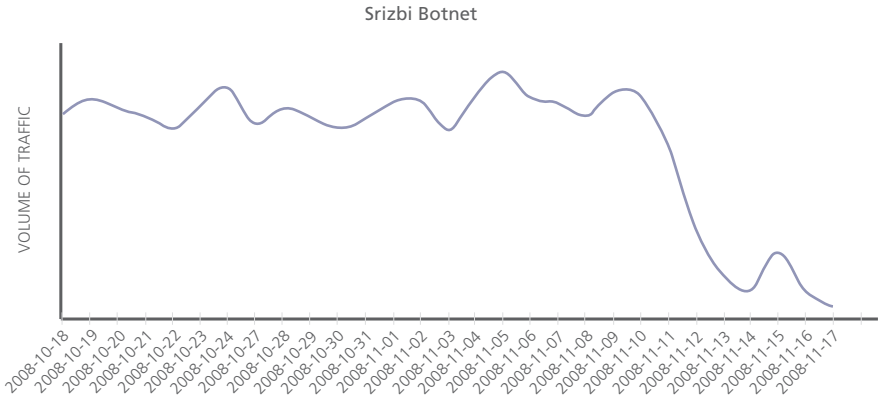


Figure 4: Traffic from botnet Srizbi also fell rapidly after the McColo shutdown.

Spammers learn their lessons

In Figures 3 and 4, we can see where the volumes of two leading botnets stood and how they dropped off after McColo was axed. The shutdown's effect was dramatic, yet ultimately brief. We have seen dramatic increases since November 2008 due to the relaunching of Rustock as well as the birth of botnets such as Bredo (which primarily sends fake nondelivery notifications spoofing package-delivery services such as FedEx, DHL, and UPS) and Waledac (a new version of the Storm botnet). Spam volumes have more than doubled since February 2009, dwarfing several times over the decreases due to McColo's demise.

The McColo closure as a single event remains significant, but when we compare it with the huge increases in volumes that followed, the decrease now represents only a momentary dip. An increase in spoofs, such as the Koobface virus, against social networking sites and spam from botnets Rustock and Cutwail have provided plenty of success for spammers.

We're confident, however, that we'll see more of these takedowns, as security researchers and research organizations continue to get involved; but we must expect the overall effect of shutdowns to be temporary. McColo has taught botnet owners a lesson. As a result, botnet control centers have become more distributed, spanning many networks in many countries. The loss of a big hosting provider today would prove only a minor inconvenience—as opposed to a major defeat—for spammers.

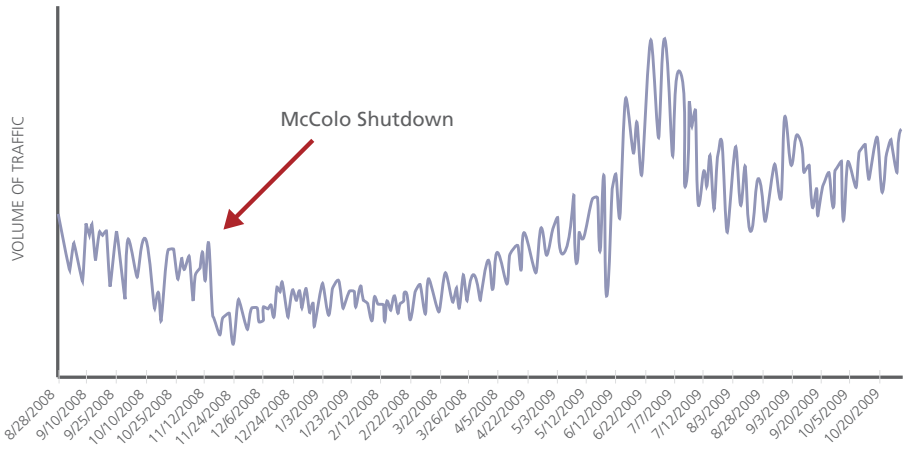


Figure 5: The shutdown caused a precipitous drop in traffic, but spammers quickly recovered and reached new heights.

'Tis the Season for Christmas Spam

It didn't take long for spammers to change from Halloween lures to holiday messages to promote their spam and malware. After all, the economy is down and they know that people won't be spending as much on holiday gifts this year. So spammers are trying to beat retailers to the advertising punch. We have already seen emails from the Cutwail botnet that use a Christmas theme to trick users into visiting malicious websites.

One campaign we are monitoring uses subject lines that try to get users to visit websites selling fake jewelry and Rolexes. These spammers aren't offering cheap merchandise, either. Only the best will do for their customers: Brands such as Cartier, Gucci, and Tag Heuer are "on sale" to all who would be fooled.

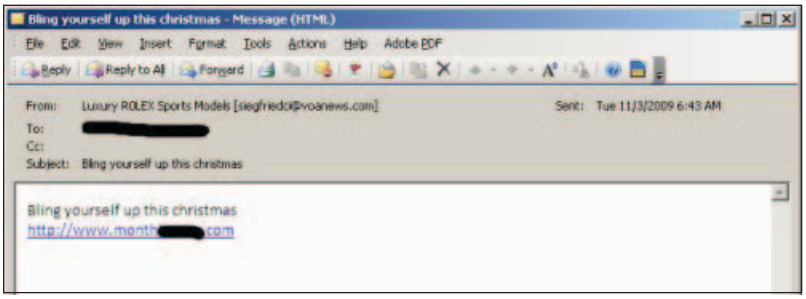


Figure 6: A Rolex spam message.

The spammers even include a Better Business Bureau logo and a Hacker Safe icon on their site. Makes you feel secure, doesn't it?

This page and similar sites are part of a campaign to steal your credit card information and identity. With the holiday shopping season rushing toward us, be sure to exercise extreme diligence regarding businesses with which you share your sensitive information. Many of the tricks that criminals use during the holiday season will be difficult to discern from legitimate marketing.

Figure 7: A fraudulent Rolex web page.

Safe online purchases

How can you stay safe? Never click links in emails. If you want to visit your favorite retail site, type the address directly into the address bar. Most legitimate sites will not force you to click a link within an email to take advantage of their latest deals.

Adam Wosotowsky is the anti-spam technology lead for McAfee Labs. During his twelve-year career in the computer security industry he has covered the gamut of corporate job responsibilities in network intrusion prevention, with a current focus on email trends and stopping spam. Wosotowsky enjoys riding his motorcycle like he stole it and going on long rants with his friends. He favors twistor theory over string theory and thinks you should, too.

Elan Winkler is a director of product marketing at McAfee, responsible for the company's web and mail portfolio. Her 20 years of security experience spans networking, desktops, messaging, encryption, and authentication. When not battling cybercriminals, Winkler and her border collie, Rain, conduct therapy visits with children and seniors at hospitals, hospices, and convalescent homes.

About McAfee Labs

McAfee Labs is the global research team of McAfee, Inc. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based reputation technologies such as Artemis and TrustedSource. McAfee Labs' 350 multidisciplinary researchers in 30 countries follow the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

7736rpt_spam_1209_ETMG