January 2010 Spam Report

McAfee Labs™ Discovers and Discusses Key Spam Trends

By Adam Wosotowsky and Elan Winkler

Key Findings

Spam volume shot up again in mid-December, primarily with subject lines claiming to offer cheap Pfizer pharmaceuticals. However, tougher Chinese domain registration laws might soon make it harder for spammers to get in business.

Spammers happily take advantage of "free-hosting" websites, temporarily benefiting from a host's legitimate reputation.

Who are your favorite celebrities? Angelina Jolie and Barack Obama appeared in more spam subject lines than any other individual in 2009.

Table of Contents

Spam Advertising Pfizer Takes Off Like a Rocket

Spam volumes have been steadily trending downward since the beginning of October 2009, but on December 14 they skyrocketed up. This boost in spam came primarily in the form of Chinese pharmaceutical spam with message subjects advertising discounts on Pfizer drugs.

The Chinese pharmaceutical spams, though they use the Pfizer corporate name, are actually illegally selling cheap generic drugs that have not been through any sort of safety verification. (Some of these sites exist only to take payments, and ship no products at all.) This spam abuses the Pfizer brand name to sell these drugs. Pfizer is not the actual source of these pharmaceuticals.

Early in December we saw positive signs that efforts were succeeding to curb the pharmaceutical spam scourge that draws registration and hosting from Chinese sources. Not only was spam volume diminishing, but the domain names used to forward targets to the websites seemed to be expiring quickly. On December 11, the China Internet Network Information Center, the state body, released an update regarding its auditing of domain name registrations.[1] As of today, domain name applicants must submit a formal paper-based application when making an online application to the registrar. This includes the original application form with business seal, company business license, and a photocopy of the ID. This occurred as China was taking steps to improve the connotation of the "made in China" label. (The observation that pharmaceutical spam domains were expiring rapidly was made in late 2008 as well, perhaps as a reaction to the shutdown of spam host ISP McColo.)

These registration changes will make the .cn domain very unattractive for criminals and fraudsters who are looking for domains that they can register anonymously, preferably paying with stolen credit cards. This appears to be a great step in making the domain name space of .cn a safer place. If these measures are implemented as announced, China would become a leading example in the fight against fraud on the Internet.

This effort will require constant pressure, however. It seems that spammers have already had to change the sources of their hosting and DNS infrastructure. This has caused spam volumes to decline, but the volumes will recover as new sources appear for hosting spam domains. As we have seen throughout 2009, spam hosting and registration are still located primarily in China, and to a lesser degree Russia, but the companies providing the hosting have changed, suggesting that the pressure on spammers may be building. Offsetting this downward trend, however, we've recorded a marked increase in spam from social networking sites such as live.com (Microsoft), blogspot (Google), and livejournal.com. (See Figure 1.)

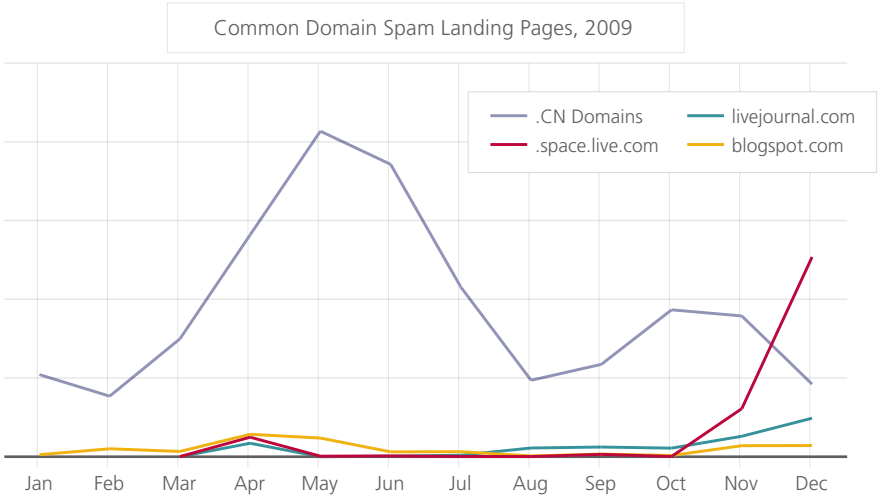

Figure 1: Although Chinese domains (.cn) hosted less spam at the end of 2009 than earlier in the year, other sites have made up for the loss.

1. "The Notification about further enhancement of auditing domain name registration information," China Internet Network Information Center. http://www.cnnic.cn/html/Dir/2009/12/12/5750.htm#_blank

The mid-December skyrocket, clogging spam filters everywhere, carried the subject "Pfizer 80% OFF." Although variations on this theme exist, the presence of the word *Pfizer* in the subject line has leaped through the first few weeks of December. (See Figure 2.)

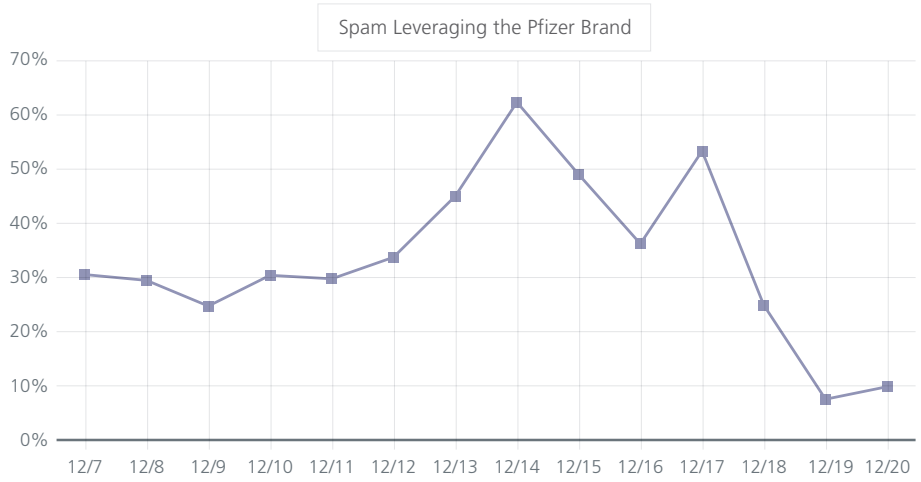

Figure 2: Spam with "Pfizer" in the subject line saw a rapid rise in December 2009 as a percentage of all spam.

The messages themselves are the same picture of Viagra pills and a Chinese URL that have formed the bulk of the global spam problem all year. (See Figure 3.)

Figure 3: Most types of "Pfizer" spam showed the same message, referencing Viagra and a Chinese URL.

The steep drop-off starting on December 17 was not due to a decrease in spam, but was rather a result of a changing subject line, with most spams using the form "daily dose XX% off" or "personal XX% off." (See Figure 4.)

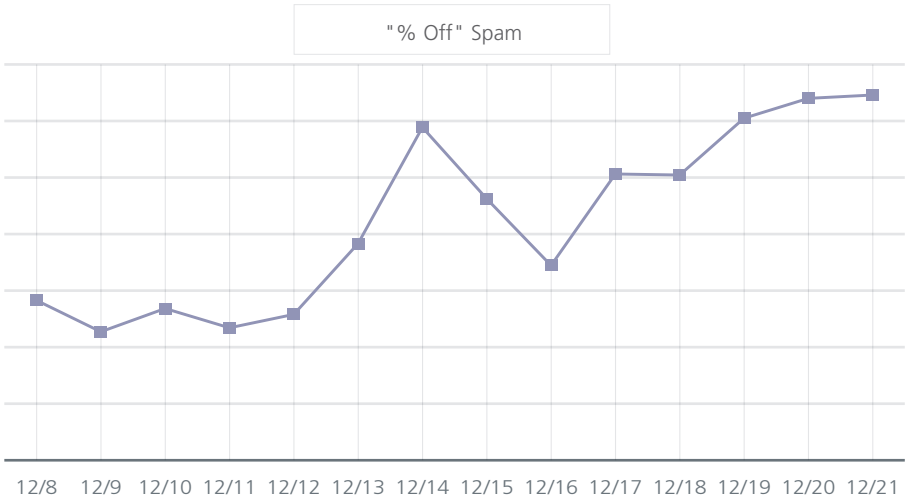

Figure 4: In the third week of the month, spammers changed the subject lines to attract new customers. December 14 showed a spike in this campaign as a percentage of all spam.

If Chinese registrars really are taking steps to clean up their act, they must be prepared—because success will not come easily. China's Internet presence is large and powerful, making the country a very attractive home for spammers who have taken the time to entrench themselves into the system. Working against spammers in a quickly growing economy will be a formidable challenge, so let us hope that the global environment continues to become a less accepting place for systemic abuse.

Spammers Seek "Free-Hosting" Websites to Provide Spam URLs

We've observed a growing trend of spammers signing up for free subdomains and complimentary hosting through the online hosting companies that allow it. For example, if a hosting company's URL is freehost.com, then a spammer could request "blah" and would be provided with the website blah.freehost.com.

This trend has turned into an all-out gold rush. Dozens of these "free-hosting" websites have sprung up to provide free web space to anyone who requests it, and spammers have requested a lot of it.

Figure 5: Free website hosting is immensely popular with spammers.

Coincidentally most of these free-hosting websites have almost the exact same appearance. In one recent round of abuse, most of the hosting sites differ only by the icon in the upper-left corner. All of the sites most heavily abused by spammers seem to be related to 0catch.com, which serves up a number of free-hosting sites to anonymous persons, and apparently does nothing to prevent spammers and botmasters from hosting malware.

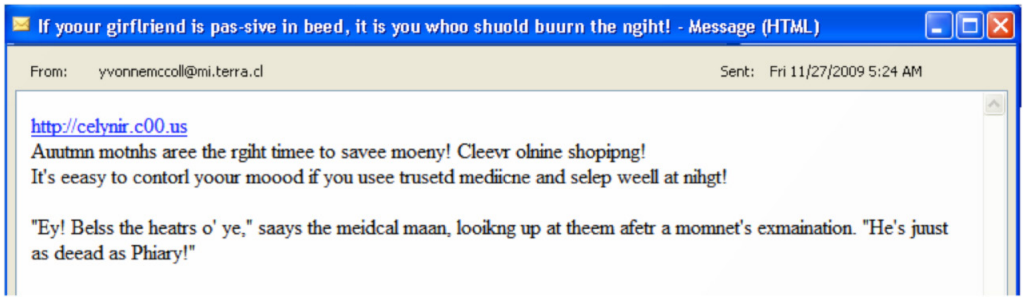

Figure 6: This comically bad message is typical of spam that abuses free-hosting sites.

Using a free hosting service is a good tactic for spammers because it is easier to automatically block a new infected website than to block a site that has been around for a longer period and has possibly had legitimate traffic associated with it. This edge can provide spammers a few precious additional hours before the spam-blocking services of the world blacklist that host. In the course of a few hours a botnet can generate billions of messages.

Although there is nothing to indicate active collusion between the free-hosting websites and the spammers that use them, this should be a lesson to legitimate businesses looking for free hosting. You get what you pay for, and using free-hosting sites that entertain spammers is likely to affect the perceived legitimacy of any honest client of one of these hosting sites.

The Year's Top 25 Men and Women in Spam

Spammers are fond of using celebrities in their mails to attract our attention. They know we'll frequently take the bait. These celebrities are often treated in a less than dignified manner, so rather than discuss the spam itself we'll just have a look at the top male and female celebrities who appeared in spam subjects this year.

To draw comparisons, we'll create an index that expresses the volumes in terms of Angelina Jolie's volume, as she was the most popular female subject. We'll call Jolie's volume 1.0, with the others' relative to that figure. (See Figure 7.)

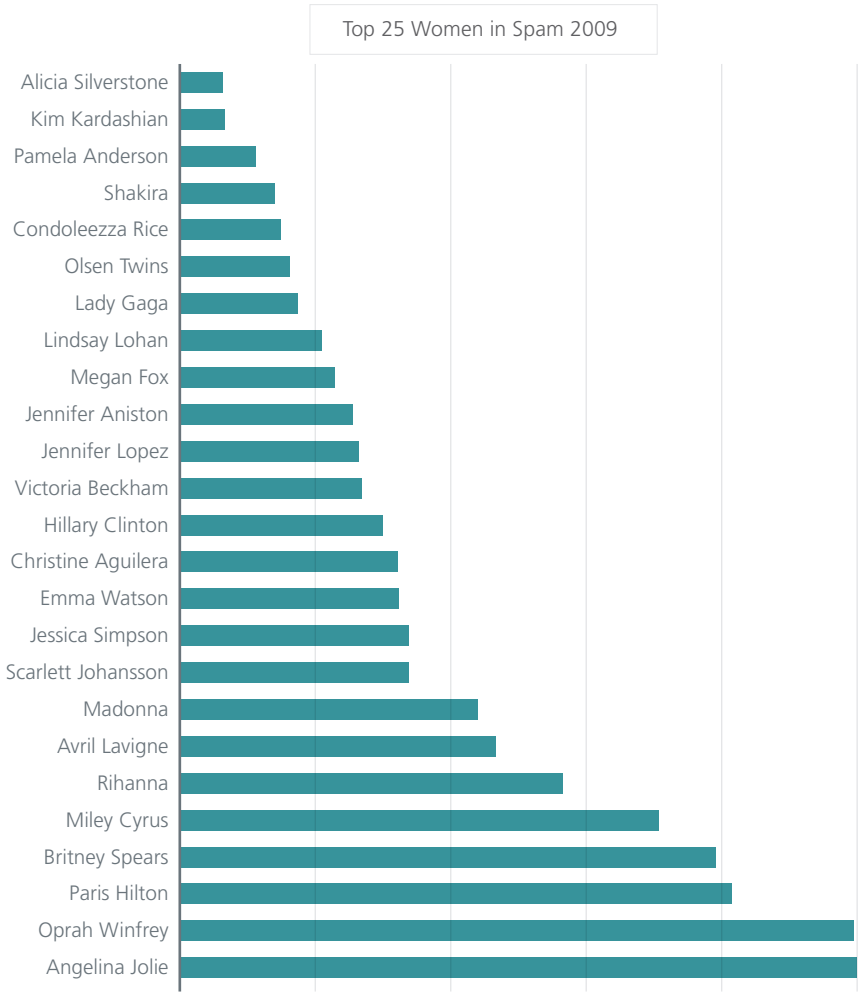

Figure 7: With Angelina Jolie as our baseline, we can see that only Oprah Winfrey came close to her popularity in spam subject lines in 2009.

Let's see how celebrity men did when compared with Jolie.

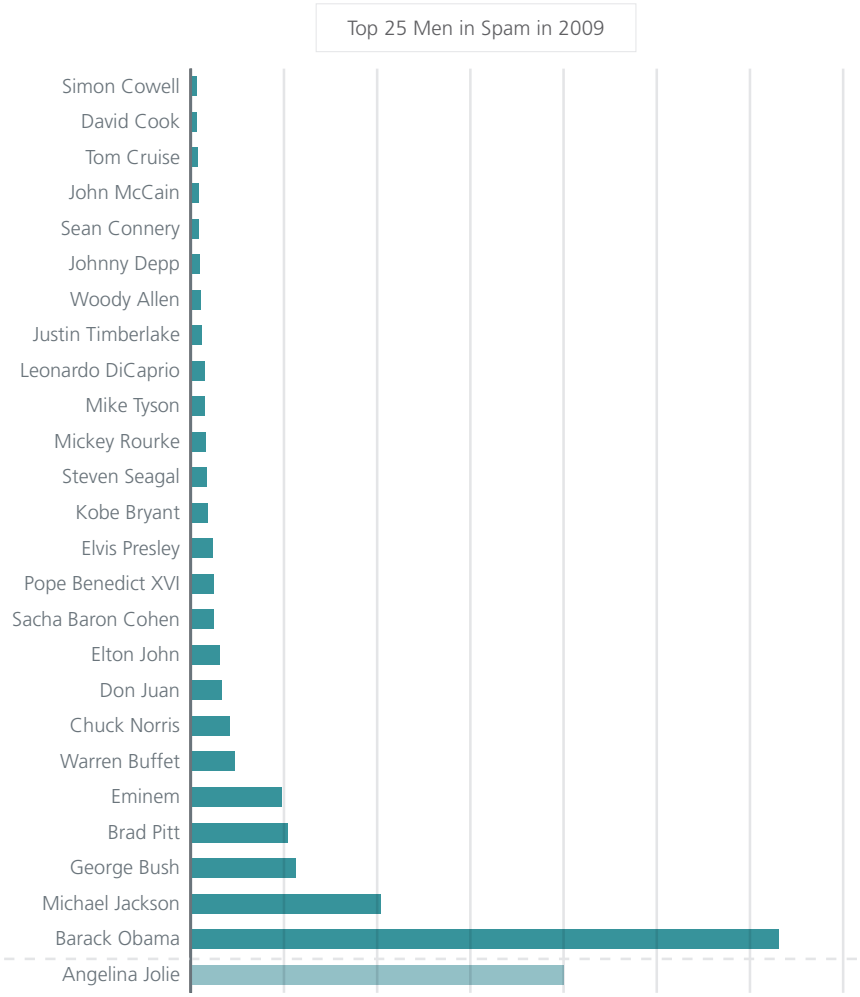

Figure 8: In spam subjects Angelina Jolie was more popular than any other male celebrity last year, with one exception.

Bottom line, it looks like you have to president to be a more popular spam target than Angelina. Sorry, guys!

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. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows 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

8216rpt_spam_0110_ETMG