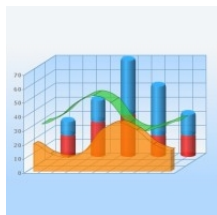


12 November 2008

By: Lucian Constantin, Web News Editor



Spam activity decreases because McColo was depeered ObjectPlanet, Inc.

[Severe Decrease in Spam Activity](#)

As ISPs pull the plug on major spam and phishing hosting services

Security researchers, anti-spam groups and the whole security community in general were taken by surprise yesterday when reports of a sudden drop in junk mail activity started flowing in. This was the result of ISPs depeering McColo Corp., a U.S. based company offering web hosting services to many international cybercrime organizations.

McColo Corp. is based in San Jose, California and offers web hosting solutions. Nothing bad so far, but according to many reports and an important amount of evidence, a large number of their clients are shady at best. Security experts estimate that the spam generated by the illegal activities hosted by McColo amounts for a whopping 75% of the junk mail sent everyday on a global level.

Brian Krebs, reputable journalist at The Washington Post, informed on the [Security Fix blog](#) that he was involved with forwarding evidence of the criminal activity to Global Crossing and Hurricane Electric, McColo's two major Internet service providers. "For the past four months, Security Fix has been gathering data from the security industry about McColo Corp. [...] On Monday, Security Fix contacted the Internet providers that manage more than 90 percent of the company's connection to the larger Internet, sending them information about badness at McColo as documented by the security industry," he writes.

According to Krebs, while the response from Global Crossing was rather evasive, Hurricane Electric was a lot more responsive to the abuse report and even quick to act about it. "We looked into it a bit, saw the size and scope of the problem you were reporting and said 'Holy cow! Within the hour we had terminated all of our connections to them,'" Benny Ng, the Fremont-based ISP's Director of Marketing, told Krebs.

As a result, McColo's website went offline and the global spam activity registered a sudden drop. Based on the statistics graph generated by the SpamCop service, the decrease in junk mail activity occurred a bit after 16:20 EST on Tuesday and continues to remain at low levels at the time of writing this article. "I admit, I was very surprised when I checked my email today after being offline for 7 or so hours, and discovered that there had only been a dozen or so pieces of spam in my inbox, when I normally receive hundreds (after filtering) over the same period of time," writes [Sandi Hardmeier](#), long time Microsoft MVP, on her spyware tracking blog.

As the Washington Post journalist points out, illegal activity originating from McColo's IP block was not limited to spam and also consisted of phishing campaigns, malware distribution and even the hosting of illegal content involving minors. This makes McColo's banishment from the Internet an important win over international cybercrime and comes after another recent major criminal activity hub in the US, the infamous [Intercage](#) (Atrivo) hosting company, suffered a [similar fate](#).

Also recently, the authorities shut down the funding source and arrested the owners of what was considered the [biggest spam network](#) in the world, HerbalKing and in addition, the number one domain registrar used by spammers and other criminals is also currently having [accreditation problems](#). All of this raises our hopes that change might be coming.