

Press Release

Contact

John Murden
VP Marketing
Mail-Filters.com, Inc.
(650) 655-7759
jmurden@mail-filters.com

For immediate release

Spammers Redirecting Links in Spam Messages to Avoid Detection

Redirect Tactics Embarrassing to Unsuspecting Websites and Creates Increased Traffic Loads

Redwood City, Calif. October 23, 2007. Mail-Filters.com, Inc., the global leader in OEM anti-spam solutions, providing technology for its OEM partners filtering billions of messages a day in more than 100 countries and over 30 languages, reported today that spammers have escalated their use of redirection techniques to try to get around many anti-spam filters. The latest flurry started about 10:00 AM PDT and by 11:00 AM represented an estimated 4.3% of the spam on the Internet. The technique, most commonly found with pharmaceutical spam in this latest flurry, sends a user to a webpage and the user is then automatically redirected to another webpage. This technique is specifically designed to get around databases of destination URLs that many anti-spam technologies rely upon. Mail-Filters anti-spam/anti-phishing technology is successfully detecting these spam messages.

“Spammers are constantly looking for solutions to avoid detection by anti-spam technologies so that they can reach more eyeballs. We have seen a substantial increase in spam messages being sent where the hyperlinks contained in the messages are actually links to legitimate sites that are then redirected to the spammer sites,” explained Ben Westbrook, CTO of Mail-Filters. Mr. Westbrook continued by explaining, “Because the hyperlink appears to be to a legitimate site, most anti-spam technologies will determine it is a legitimate message or create false-positives by misidentifying legitimate email messages that contain links to these same sites. Mail-Filters technology is correctly blocking the spam messages without causing false-positives. This latest technique is coming in a flurry of messages that sometimes has breaks in the sending – implying the spammer is evaluating techniques to see what message receives the highest response rate.”

Another byproduct of this new spammer technique is that legitimate websites are seeing increased traffic to their websites during the redirect process. This increased traffic could create significant load problems for the sites, potentially even temporarily crashing a site from the increased traffic. In addition, unassuming websites that are being

targeted by the spammers find themselves in the embarrassing situation of being associated with spammers.

Mail-Filters combines three proprietary weapons to catch both spam and phishing messages: the Bullet Signature Database created and maintained by both technology and human editors, the STAR Engine that detects spammer tricks, and the RETIRE System designed for detecting image-based spam as well as email-borne malware. Because the Bullet Signature Database is updated by the minute this approach allows the filter to catch new types of spam, including MP3 attachment spam, phishing, embedded content, HTML, and foreign language spam. The result is a consistent catch rate of more than 95% with less than 1 in 1,000,000 false positives.

ABOUT MAIL-FILTERS™

Founded in 2001, Mail-Filters™ focuses on providing its technology through OEM partners. Recognized as the global leader in the OEM anti-spam market, the Mail-Filters™ technology is currently deployed with over 40,000 enterprise customers, filtering millions of mailboxes, in over 100 countries and supporting over 30 languages. Mail-Filters™ processes billions of messages every day and is one of the only anti-spam companies to offer a guarantee on performance.

Mail-Filters.com, Inc.™ is located in Redwood City, California. The company can be found on the Internet at www.Mail-Filters.com or reached in the USA at (650) 655-7700 and in the UK at +44 20 70234965.

Trademarked company and product names are the property of their respective owners.

Mail-Filters.com, Inc.™
505 Seaport Court, Suite 102
Redwood City, CA 94063
(650) 655-7700