

Spammers attack Sourceforge Wiki revealing vulnerabilities faced by User generated content, says Cyberoam Threat Report

Cyberoam, a division of Elitecore Technologies and the innovator of identity-based Unified Threat Management (UTM) solutions, today announced the Q3 2009 Internet threats trend report, prepared in collaboration with its partner, Commtouch. Among the ...

Ahmedabad, Gujarat, November 1, 2009 /[India PRwire](#)/ -- Cyberoam, a division of Elitecore Technologies and the innovator of identity-based Unified Threat Management (UTM) solutions, today announced the Q3 2009 Internet threats trend report, prepared in collaboration with its partner, Commtouch. Among the top stories, Sourceforge.net, a popular download site for open source software, saw a search engine spam attack in its wiki subdomain, with keywords and inbound links leading to a specific pornography site. The above incident could have as easily involved a malware hosting site, which puts the consumers of user generated content such as wikis at huge risk from threats where spammers hide inappropriate content deep inside the site URL while simultaneously using reputable domains/subdomains for getting a higher page rank.

Says Abhilash Sonwane, VP, Product Management, Cyberoam, "The proliferation of open source user generated content such as wikis has created new opportunities for spammers. Since, these projects run on collaboration and trust among a community, search engine bombers can misuse the open environment to fill up wiki-like pages with their own marketing promotional links and use reputed domains/subdomains to rank their page higher. The presence of malware hosting sites only aggravates the problem."

Also, in the report, the current financial crisis and the debate around health care reform in the US have made Americans an easier target for 419 scammers. One of the more creative examples seen by Cyberoam was in an ironical message that appeared to be from the "F.B.I." explaining to the recipient that he or she has been targeted for a 419 scam and they have recourse to quick retrieval of funds. Another email touted bogus low-cost health insurance coverage for recipients with a working unsubscribe link for deception.

Another major highlight of the report was regarding higher-than-average spam levels which shot up to an astonishingly high 97% in July. Pharmacy spam continues to be at top spot where spammers are using innovative ways to bypass content and human filters, such as masquerading their spam through Facebook messages. There was also an outbreak of Google Spreadsheet spam, where a pharmaceutical spammer used Google Spreadsheets for URL redirection, seeing that such applications are typically trusted by anti-spam filters.

For the 2nd quarter in a row, Cyberoam saw spikes in email-borne viruses not caught by major anti-virus engines. Out of these, two particular viruses Mal-Bredo A and Mal-Behav 340 saw distribution of over 10,000 distinct variants. Sites in the "Health and Medicine" and "Sex Education" category topped the list of sites manipulated by phishing schemes. Brazil continues to remain the zombie hotspot accounting for nearly 19.7% of global zombie activity.

Cyberoam uses the Commtouch RPDTM technology to analyze large volumes of Internet traffic in real-time. Unlike traditional spam filters, it does not rely on email content, so it is able to detect spam in any language and in every message format (including images, HTML, etc.), non-English characters, single and double byte, etc. Its language and content agnostic nature enables it to provide effective spam blocking capabilities. Cyberoam incorporates this technology within its unique identity-based UTM appliances, which deploy user identity-based functionality across all of its features. A departure from traditional IP address-dependent solutions, Cyberoam determines precisely who is doing what in the network, providing IT managers with stronger policy control and clearer visibility of activity.

[For the full Q3 2009 threat report click here](#)

Notes to Editor

About Cyberoam

Cyberoam Identity-based UTM appliances offer comprehensive protection against existing and emerging Internet

threats, including viruses, worms, Trojans, spyware, phishing, pharming and more. Cyberoam delivers the complete range of security features such as stateful inspection firewall, VPN, gateway anti-virus, gateway anti-malware, gateway anti-spam, intrusion prevention system, content filtering in addition to bandwidth management and multiple link management over a single platform. Cyberoam is certified by the West Coast Labs with CheckMark UTM Level 5 Certification, ICSA Lab, an independent division of Verizon Business, and the Virtual Private Network Consortium. Cyberoam has received the 2008 Emerging Vendor of the Year award by Frost & Sullivan, 2007 Global Excellence Awards for Integrated Security Appliance, Security Solution for Education and Unified Security, the 2007 Tomorrow's Technology Today Award for Unified Security was rated Positive by Gartner in its Marketscope for SMB multi-function firewalls. Cyberoam has offices in the Woburn, MA, USA and India. For more information, please visit www.cyberoam.com

About Elitecore Technologies Limited

Elitecore Technologies Limited is the global provider of Cyberoam UTM appliances. Elitecore's other divisions include CRESTEL Convergent Billing Solution that meets the voice, data, video billing and customer care requirements of Tier-1 service providers and 24online Billing and Bandwidth Management Solution for hotels, hotspots and Internet service providers. Elitecore has a strong R&D base and support center in India; it has sustained a healthy growth rate of over 75 % since inception. For more information, please visit www.elitecore.com

For more information, please contact:

L K Pathak

Chief Manager, Corporate Communications
(L) +91-79-66065606, (M) +91 9925012059

© copyright 2012 India PRwire (<http://www.indiaprwire.com>)

India PRwire disclaims any content contained in press release. Use of our service is governed by our privacy policy and terms of service.