



For Immediate Release –

Blue Coat Publishes Annual Web Security Report

Report Examines Evolving Malware Attack Strategies That Exploit Online User Behavior

MUMBAI, March 31, 2010 – Blue Coat Systems, Inc. (Nasdaq: BCSI), the technology leader in Application Delivery Networking, today published its annual Blue Coat Web Security Report for 2009, which provides a comprehensive analysis of user behavior in relation to Web-based threats and specifically examines where users encountered malware on the Internet. Based on data collected from the Blue Coat® WebPulse™ service, the report concludes that the overwhelming popularity of social networking services and changes in online user behavior are driving broader attack strategies, including complex blended threats, faster malware lifecycles and search engine manipulation.

Key Findings:

- **Malware adapts with rapid lifecycles:** The average lifespan of malware dropped to two hours in 2009, from as many as seven hours in 2007, as cybercriminals responded to the increasing use and effectiveness of URL filtering at blocking malware sources. As a result of this faster malware lifecycle, defenses that require patches and downloads are unable to keep pace.
- **Social networking leads Internet access activity:** Social networking sites led Internet access activity in 2009 and accounted for 25 percent of activity among the top 10 URL categories for 2009. Increased reliance on social networking for communication also meant less reliance on Web-based email, which dropped in popularity from fifth place in 2008 to ninth place in 2009.
- **Exploiting user trust drives most common threats:** The two most common Web-based threats in 2009 – the fake antivirus software and the fake video codec – both exploited user trust in the Internet, search engines and social networks. These were not the “drive-by” attacks of recent years, nor did they require a vulnerability to exploit other than human behavior.
- **Malware lurks on unexpected sites:** Online storage and software download sites were the most frequent hiding places for Web-based malware in 2009. The number of online storage sites grew 200 percent over the prior year, and this growth, coupled with the nature of the service, makes them an ideal and easily accessible malware storage location.
- **Advanced spyware drives increase in malware and phone-home sites:** The number of malware sites (sites that store malware for download on victims’ computers) nearly doubled in 2009, but more surprising is the 500 percent increase in the number of malware effects sites (phone-home sites that collect data from an infected computer). This is largely attributable to the emergence of advanced spyware that generates multiple URLs for possible activity, increasing the likelihood that one or more of the URLs will remain undiscovered long enough for cybercriminals to retrieve stolen information.
- **Real-time analysis needed:** The changing threat landscape is driving the evolution to a hybrid defense that unites traditional Web gateways with cloud-based intelligence that can provide real-time analysis and ratings and be extended to remote users.

The information in the report is based on an analysis of data collected from the Blue Coat WebPulse service, a cloud-based collaborative defense that unites 62 million users to provide on-demand security intelligence and real-time ratings for 17 languages. WebPulse complements BlueCoat WebFilter and Blue Coat ProxySG® appliances in a hybrid design to provide a first line of defense against malicious attacks for any user, on any network, in any location.

Blue Coat Web Security Report for 2009

<http://dc.bluecoat.com/content/SecurityReport2010>

Supporting Quotes

Chris Larsen, senior malware researcher at Blue Coat Systems

"The increasing use of link farms to manipulate search engine results and prey on the trust users have in their Internet experience drove many of the malware exploits we saw in 2009 and are continuing to see in 2010. To provide comprehensive protection in the face of these threats, enterprises need not only a layered defense but also better user education."

"The Web is growing too fast in all directions for human raters or even Web crawlers to manage. It is turning into a war of machines, and the best defenses are able to leverage the strength-in-numbers principle to protect users."

Bob Hansmann, senior product marketing manager at Blue Coat Systems

"The social engineering techniques that cybercriminals are using today make it difficult for enterprises to protect their users with traditional desktop defenses alone. Enterprises need to go one step further to mitigate exposure to these new Web threats and add defenses that can dynamically analyze and rate new Web content to provide continuous protection and on-demand security intelligence."

Andreas Antonopoulos, senior vice president and founding partner of Nemertes Research

"The battlefield for information security against identity theft and cybercrime is the Web. The Web, and especially social media, is where the apps are, where the eyeballs are and, therefore, where the attacks are. As today's threats move too fast for "patch and distribute" strategies, enterprises must adapt and deploy defenses that are scalable, real time and community intelligence-based to protect employees regardless of location."

Video

Anatomy of a Fake Anti-Virus Scanner Attack

<http://www.youtube.com/watch?v=dofgiRkzQXg>

Images

Blended Web-based Threats

<http://www.flickr.com/photos/bluecoatsystems/4471945112/>

WebPulse Collaborative Cloud Defense

<http://www.flickr.com/photos/bluecoatsystems/4463550488/in/set-72157623562484791/>

Additional Resources

Blue Coat Security Lab

<http://www.bluecoat.com/security>

Blue Coat Security Blog

<http://www.bluecoat.com/security/blog>

Blue Coat WebFilter

<http://www.bluecoat.com/products/webfilter>

About Blue Coat Systems

Blue Coat Systems is the technology leader in Application Delivery Networking. Blue Coat offers an Application Delivery Network Infrastructure that provides the visibility, acceleration and security required to optimize and secure the flow of information to any user, on any network, anywhere. This application intelligence enables enterprises to tightly align network investments with business requirements, speed decision making and secure business applications for long-term competitive advantage. For additional information, please visit www.bluecoat.com

###

FORWARD LOOKING STATEMENTS: The statements contained in this press release that are not purely historical are forward-looking statements, including statements regarding Blue Coat Systems' expectations, beliefs, intentions or strategies regarding the future, and including statements regarding the capabilities and expected performance of Blue Coat Systems' products. All forward-looking statements included in this press release are based upon information available to Blue Coat Systems as of the date hereof, and Blue Coat Systems assumes no obligation to update any such forward-looking statements. Forward-looking statements involve risks and uncertainties, which could cause actual results to differ materially from those projected. These and other risks relating to Blue Coat Systems' business are set forth in the Securities and Exchange Commission reports filed by Blue Coat Systems, including but not limited to the risks described in the most recent reports on Form 10-K and Form 10-Q, particularly under the heading "Risk Factors."

Blue Coat, ProxySG, WebPulse and the Blue Coat logo are registered trademarks or trademarks of Blue Coat Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document are the property of their respective owners.