Websense Offers Industry's Most Advanced Protection From Cybercriminals Taking Advantage of Shortened URL Services

Secure Web Gateway Classifies Specific Content on Web Pages in Real-Time, Enabling Organizations to Take Advantage of Benefits of Web 2.0, With Up-to-the-Second Protection From Threats and Inappropriate Content

SAN DIEGO, CA, Aug 25, 2009 (MARKETWIRE via COMTEX News Network) -- Websense, Inc. (NASDAQ: WBSN) today affirmed its advanced content security solutions provide protection from the growing number of shortened URLs used and shared on social networking sites such as Facebook and Twitter and in blog comments.

Unlike other Web security solutions that rely primarily on antivirus signatures to detect malware -- unique to Websense and only available with the Websense® Web Security Gateway -- if the shortened URL leads the user to a Web 2.0 Web site with dynamic content, the Websense secure Web gateway in real-time classifies the content on that page and will either allow the user to go to the site if its deemed safe and appropriate or prevent the user from visiting the page. Websense Web Security Gateway is the only secure Web gateway that can scan Web 2.0 properties in real time for content across more than 90 categories.

"For years, Websense Web Security solutions have protected customers from URLs that attempt to redirect users to malicious Web sites," said Sr. Director of Technical Marketing Bill Gardner, Websense. "Many of today's Web 2.0 sites used for business purposes are 'mashups' of different applications. Additionally, Web 2.0 sites allow third party applications and user-generated content that can change from minute-to-minute. With Websense Web Security Gateway, customers are protected from the latest threats, such as malicious shortened URLs."

View Slideshare presentation on the dangers of shortened URLs

Additional Facts

-- Use of URL shortening services like TinyURL, Snipurl, Bit.ly and Cligs is exploding due to the growing popularity of Twitter, blogs, social networking sites and other Web 2.0 sites that allow user-generated content and where users often share links with their friends, business associates and followers.

-- In June 2009, hackers were able to exploit a flaw in the Cligs' URL editing software, allowing them to hijack 2.2 million Cligs links.

-- In May 2009, Websense Security Labs alerted that "Koobface" malware, which has plagued social networking sites like Facebook, MySpace and Hi5, was spread among friend networks through the use of TinyURLs and other shortened links.

-- Taking advantage of the convenience of these services, business use of shortened URLs is growing rapidly. Most shortened URL providers now offer free analytics that enable organizations to track important data such as the number of people that have clicked on the links, where they are located and more.

-- Shortened URL service providers are reporting massive growth. According to media reports, Bit.ly is used to create 5 million to 7 million shortened URLs each day, and Snipurl has delivered 53 billion since its inception.

-- Despite the risks, organizations are continuing to adopt Web 2.0 for the many benefits it can provide. In fact, a recent Websense survey of 1,300 IT managers worldwide called Web 2.0 @ Work found that 95 percent of respondents currently allow employee access to some Web 2.0 sites and applications and 62 percent of IT managers believe that Web 2.0 is necessary to their business.

"The volume of shortened URLs and the increased use by businesses have encouraged the attention of criminals because they are a perfect way to get an unsuspecting user to click on a spam or malicious link -- the URL identity is masked to the user and they are used so commonly on sites like Twitter, social networking sites and blogs that people don't hesitate to click on them," added Gardner. "Without Web 2.0 content security that understands where the link is trying to direct the user and what type of content is on that page, in real time, malicious shortened URLs will continue to plague both businesses and consumers."

With Websense Web Security solutions, including the latest Websense Web Security and Web Filter version 7, customers are protected from shortened URLs. When a user clicks on a shortened URL, Websense technology knows if the destination Web site is serving up spam, malicious or in violation of the organization's Web use policies and protects the organization from those threats.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection™ for approximately 44 million product seats under subscription. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies. For more information, visit www.websense.com.

Image Available: http://www2.marketwire.com/mw/frame_mw?attachid=1050427

Media Contact:
Sarah Thornton
sthornton@websense.com
858.320.9500

SOURCE: Websense, Inc.

mailto:sthornton@websense.com