



WebSense® Security Labs™ Issues Second Half 2005 Semi-Annual Security Trends Report

WebSense Security Labs reports on high-level security events; first to discover Microsoft WMF vulnerability and websites attacking Sony copy protection uninstall program

San Diego March 1, 2006 -- Websense, Inc. (NASDAQ: WBSN), a global leader in web security and web filtering productivity software, today announced the release of the 2005 Semi-Annual Web Security Trends Report issued by Websense® Security Labs™. The new report summarizes findings for the second half of 2005 and presents projections for the upcoming year. In the second half of 2005, Websense Security Labs was successful in identifying and mitigating several new high-profile exploits, including being the first to discover the Microsoft Windows Metafile (WMF) vulnerability being exploited in the wild and also uncovering websites hosting code attacking the vulnerability within the Sony BMG Music Entertainment copy protection uninstall program.

Websense Security Labs was introduced in August 2004 with the primary objective of discovering and investigating today's advanced internet threats, and then publishing those findings to the security community and customers. Websense Security Labs research delivers precise depictions of current web outbreaks as well as insight into new malicious threats before attacks are launched. Utilizing a worldwide network of computers, data mining processes, customer feedback loops, and malicious code categorization expertise, Websense Security Labs proactively discovers and immediately defends customers against web-based threats. As new threats are discovered, Websense web security software quickly protects an organization's network infrastructure and employees via real-time security updates of malicious URLs and applications.

According to the report, the web continued to evolve and grow as an attack vector in the second half of 2005. The report found that the trend of bot-led denial-of-service attacks increased at an alarming rate. In these attacks, hundreds of thousands of computers infected with an unauthorized software agent are directed by a centralized control channel to carry out attacks. In addition, cyber-extortion attacks, in which money is requested from users to fix a problem created by the cyber-criminal, continue to rise.

"Websense Security Labs utilizes a unique and sophisticated process to scan over 75 million websites per day, looking for malicious attacks against the end-user and enterprise. With our extensive malicious code detection and classification expertise, we continue to be on the forefront of discovering advanced attacks and techniques," said Dan Hubbard, senior director of security and technology research for Websense, Inc. "As Websense Security Labs discovers new high-level security threats, we utilize these findings to provide rapid web security protection to our customers by eliminating the threat entirely."

Major Discoveries by Websense Security Labs during the second half of 2005

November 16, 2005 - Websense Security Labs was the first to discover websites hosting code attacking the vulnerability in the Sony BMG Music Entertainment copy protection uninstall program. The code on these websites allowed hackers to obtain remote access into users' machines simply by visiting a website.

December 2, 2005 - Websense Security Labs was the first to discover exploits that were using a zero-day Internet Explorer vulnerability. The Windows object exploit allowed successful downloading and launching of malicious code without user-intervention.

December 14, 2005 - Websense Security Labs was the first to discover the Microsoft Windows Metafile (WMF) vulnerability and an associated active exploit. The exploit enabled attackers to download and launch additional software on vulnerable Windows clients, including keyloggers, crimeware, bots, and Trojan horse malicious code.

Additional Highlights from the Second Half 2005 Security Trends Report

The motives for creating malicious websites continued to trend away from annoyances, such as changing default homepages, to increasingly malicious purposes, such as changing browser address bars to redirect users to fake banking, commerce and other sites.

Browser and operating system vulnerabilities were exploited more frequently by spyware, crimeware, phishing, and keylogger installations.

There was a shift towards profiting from current events, in particular, donation scams for natural disasters. Prime examples were sites purporting to collect donations for tsunami or Hurricane Katrina victims.

Phishing attacks continued to target and exploit non-financial organizations as well as banks.

Spear phishing, attacks that use stolen inside information to convince victims that the approach is legitimate, was on the rise as a technique used to dupe increasingly sophisticated consumers into taking the lure.

To view the report in its entirety please visit: http://www.websensesecuritylabs.com/docs/WebSenseSecurityLabs20052H_Report.pdf.

Websense software is available for organizations who wish to protect themselves from internet and application security threats. For a free 30-day evaluation of Websense software or for more information on protecting your organization from a wide range of threats including spyware, peer-to-peer, virus outbreaks and internal hacking exploits, please visit www.websense.com. Websense Security Labs offers free email security updates as new internet threats are discovered and is available at www.websensesecuritylabs.com.

About Websense, Inc.

Websense, Inc. (NASDAQ:WBSN), a global leader in web security and web filtering software, is trusted to protect 24 million employees worldwide. Websense proactively discovers and immediately protects customers against web-based threats such as spyware, phishing attacks, viruses and crimeware with maximum protection and minimal effort. With diverse partnerships and integrations, Websense enhances our customers' network and security environments. For more information, visit www.websense.com.

© 2006, Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

MEDIA CONTACT

Cas Purdy

Senior Manager, Public Relations

Websense, Inc.

Phone: 858.320.9493

cpurdy@websense.com

This press release contains forward-looking statements that involve risks, uncertainties, assumptions and other factors which, if they do not materialize or prove correct, could cause Websense's results to differ materially from historical results or those expressed or implied by such forward-looking statements. All statements, other than statements of historical fact, are statements that could be deemed forward-looking statements, including statements containing the words "planned," "expects," "believes," "strategy," "opportunity," "anticipates" and similar words. These statements may include, among others, plans, strategies and objectives of management for future operations; any statements regarding proposed new products, services or developments; any statements regarding future economic conditions or financial or operating performance, including estimates of billings and revenue; statements of belief and any statements of assumptions underlying any of the foregoing. The potential risks and uncertainties which contribute to the uncertain nature of these statements include, among others, customer acceptance of the company's services, products and fee structures; the success of Websense's brand development efforts; the volatile and competitive nature of the Internet industry; changes in domestic and international market conditions and the entry into and development of international markets for the company's products; risks relating to intellectual property ownership; changes in estimated amounts based on the review and audit of Websense's financial statements by its independent auditors; and the other risks and uncertainties described in Websense's public filings with the Securities and Exchange Commission, available at <http://www.sec.gov>. Websense assumes no obligation to update any forward-looking statement to reflect events or circumstances arising after the date on which it was made.

© 2008 Websense, Inc. All Rights Reserved.