



MEDIA CONTACT:

Jennifer Culter
Websense, Inc.
858 320 9511
jculter@websense.com

NEWS RELEASE

Websense Web@Work Survey: Nearly One in Five Organizations Hit by Keyloggers in 2006

IT Decision-Maker survey results reveal how IT security landscape has changed in past 12 months

SAN DIEGO, May 15, 2006—Websense, Inc. (NASDAQ:WBSN), a global leader in web security and web filtering productivity software, today announced the IT Decision-Maker results of the company's seventh annual Web@Work study, conducted by Harris Interactive[®]. From March 15 to March 24, 2006, 351 U.S. IT decision-makers who work for organizations with at least 100 employees, at least 1 percent of whom have internet access, were interviewed online, and from March 16 to April 4, 2006, 500 U.S. employees ages 18 and older who have internet access at work and who work for organizations with at least 100 employees were surveyed over the telephone on web and software application usage in their workplace.

According to the Web@Work survey, directionally, more organizations were hit by a hacking tool or a keylogger in 2006, as almost one in five (17 percent) of organizations have had employees launch a hacking tool or a keylogger within their network. This number has increased from 2005 in which 12 percent were impacted¹. A keylogger can be defined as one of the most dangerous types of spyware, which has the ability to record keystrokes and screen shots and can be replayed later to reconstruct a user session. These applications can be utilized by hackers to steal passwords and confidential information, which can then be used to provide full access to corporate systems and files.

The 2006 Web@Work survey also highlighted a new threat on the horizon—bots. A bot (short for robot) is software that can be unknowingly installed on an end-user's PC that communicates with a command and control center. The command and control center has unauthorized control of many bot-infested PCs from a single point, and can be used for launching

¹ Last year's IT decision-maker survey was conducted online within the United States between February 21 and February 28, 2005 among a nationwide cross sample of 354 IT decision-makers in companies with more than 100 employees, at least 1% of whom have internet access. Sampling error is +/- 5.2 percentage points.

distributed Denial of Service attacks, acting as a spam proxy, and hosting malicious content and phishing exploits.

Only 34 percent of IT decision-makers said they are very or extremely confident that they can prevent bots from infecting employees' PCs when not connected to the corporate network. Furthermore, 19 percent of IT decision-makers indicated that they have had employees' work-owned computers or laptops infected with a bot. As bots are a relatively new threat to many IT decision-makers, there is still some discrepancy on whether or not to filter bot traffic—the survey found that 62 percent of IT decision-makers reported that their companies filter bot traffic in their network; 14 percent do not; 24 percent were unsure.

Upon evaluating how the IT security landscape has changed in the past 12 months, spyware within the enterprise continues to be a problem—92 percent of IT decision-makers surveyed estimated that their organization has been infected by spyware at some point, compared to 93 percent in 2005.

The threat of phishing has stayed relatively constant in the past 12 months, as hackers utilize new deception techniques to lure in internet users. Four in five IT decision-makers (81 percent) report that their employees have received a phishing attack via email or instant messaging (IM), versus 82 percent in 2005. Of those, nearly half (47 percent) of IT decision-makers said their employees have clicked through the URL, compared to 45 percent 12 months ago. Perhaps due to increasing media coverage and nationwide attention, more employees are aware of phishing—about half (49 percent) of employees have heard of phishing, compared to only 33 percent last year. Similarly, 44 percent of IT decision-makers believe that employees in their company *cannot* accurately identify phishing sites—this is slightly improved from the past year in which 50 percent of IT decision-makers believed their employees could not accurately identify phishing sites.

“Although employee awareness of web-based threats such as phishing attacks and keyloggers is improving, the vast majority of employees still do not know that they could fall prey to these types of social engineering tactics in the workplace,” said Dan Hubbard, senior director of security and technology research, Websense, Inc. “Organizations need to implement a proactive approach to web security which includes both technology to block access to these types of infected websites and applications, as well as rigorous employee internet security education programs.”

IT Decision-Maker Web@Work Survey Results:

- **HACKING TOOLS AND KEYLOGGERS**—17 percent of IT decision-makers have had employees launch a hacking tool or a keylogger within their network, versus 12 percent in 2005.

- **BOTS**—only 34 percent of IT decision-makers said they are very or extremely confident that they can prevent bots from infecting employees' PCs when not connected to the corporate network. Furthermore, 19 percent of IT decision-makers indicated that they have had employees' work-owned computers or laptops infected with a bot. Sixty-two percent of IT decision-makers report their companies filter bot traffic in their network; 14 percent do not; 24 percent were unsure.
- **SPYWARE**—ninety-two percent of IT decision-makers said their organization has been infected by spyware at some point, compared to 93 percent in 2005.
- **PHISHING**—four in five IT decision-makers (81 percent) report that their employees have received a phishing attack via email or IM, versus 82 percent in 2005. Of those, nearly half (47 percent) of IT decision-makers said their employees have clicked through the URL, compared to 45 percent 12 months ago. Forty-nine percent of employees have heard of phishing, compared to only 33 percent last year. Forty-four percent believe that employees in their company cannot accurately identify phishing sites, versus 50 percent in 2005.
- **VIRUSES**—according to the 2006 results, 97 percent of IT decision-makers said that they were at least somewhat confident that their antivirus software is able to stop viruses from attacking their network, yet almost half (46 percent) of companies have been infected by a web-based virus, such as the Toopher, Scob, Sober, and/or Netsky worm.
- **INTERNET THREATS AND JOB RISK**—when asked which security breaches could potentially put their job at risk, the top three responses were system downtime due to viruses (50 percent), lost or stolen intellectual property (44 percent), and internet security breaches (38 percent). In comparison, in 2005, lost or stolen intellectual property (45 percent) was the number one concern over system downtime caused by viruses (41 percent).
- **INTELLECTUAL PROPERTY**—there is much concern among IT decision-makers regarding the loss of intellectual property. For example, 40 percent said they are very or extremely concerned; 35 percent are somewhat concerned; and only 25 percent are not very (21 percent) or not at all (5 percent) concerned about the loss of intellectual property. Almost half (48 percent) of companies have software in place to combat the loss of corporate intellectual property. (30 percent do not have any software in place, and 22 percent were not sure).

- **TARGETED ATTACKS**—regarding the possibility of targeted web-based security attacks against their company (i.e. being hacked or being hit by a phishing scam), 76 percent of IT decision-makers said they are at least somewhat concerned.
- **USB DRIVES**—USB drive usage is also on the rise. Almost three-quarters (73 percent) of IT decision-makers have had employees use a portable hard drive, such as a USB device, to download company information. This is compared to 65 percent in 2005.
- **WHAT IT DECISION-MAKERS BLOCK**—to mitigate web-based attacks such as phishing or malicious spyware, 63 percent of IT decision-makers surveyed reported they block executable programs (attachments) transmitted through email, compared to 2005, when 60 percent blocked executables via email. However, only 15 percent said they block HTML within emails, as compared to 14 percent 12 months ago. Also, 52 percent of IT decision-makers surveyed said they block executables transmitted through IM, compared to last year in which only 47 percent blocked executables through IM.

However, only 26 percent indicated they block HTML within IM, as compared to 24 percent in 2005, suggesting that IM will continue to be a back door for hackers to hit up unsuspecting employees. New questions this year on that subject include whether or not IT decision-makers block RSS feeds and zip files—only 14 percent reported they block RSS and 2 percent block zip files.

About the Web@Work Survey

Web@Work is a comprehensive annual survey of internet and application usage in the workplace. By surveying both employees and IT management, the study reveals unique insights on employees' surfing habits as well as IT decision-makers' perspective on the top network problems facing today's organizations. Web@Work is commissioned by Websense, Inc. and conducted by Harris Interactive®. This is the seventh annual Web@Work survey.

Survey Methodology

Data for these surveys were collected by Harris Interactive® on behalf of Websense. Harris Interactive is solely responsible for the online and telephone data collected and Websense is responsible for the data analysis and reporting. Both parties collaborated on the survey questionnaire.

The employee survey was conducted by telephone within the United States between March 16 and April 4, 2006 among a nationwide cross sample of 500 employees aged 18+ who have Internet access at work and work at a company with at least 100 employees. The IT decision-makers survey was conducted online within the United States between March 15 and March 24,

2006, among a nationwide cross section of 351 IT decision-makers in companies with more than 100 employees. Data were not weighted and are therefore only representative of those employees and IT decision-makers surveyed.

In theory, with probability samples of this size, one can say with 95 percent certainty that the overall employee results have a sampling error of plus or minus 4.4 percentage points and the overall IT decision-maker results have a sampling error of plus or minus 5.2 percentage points. Sampling error for various sub-samples is higher and varies. The online sample is not a probability sample.

About Harris Interactive®

Harris Interactive Inc. (www.harrisinteractive.com), based in Rochester, New York, is the 13th largest and the fastest-growing market research firm in the world, most widely known for *The Harris Poll*® and for its pioneering leadership in the online market research industry. Long recognized by its clients for delivering insights that enable confident business decisions, the Company blends the science of innovative research with the art of strategic consulting to deliver knowledge that leads to measurable and enduring value.

Harris Interactive serves clients worldwide through its United States, Europe (www.harrisinteractive.com/europe) and Asia offices, its wholly-owned subsidiary Novatris in Paris, France (www.novatris.com), and through an independent global network of affiliate market research companies. EOE M/F/D/V

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.

###