

Websense, Inc. (NASDAQ: WBSN) today revealed the findings from its bi-annual research report Websense Security Labs, State of Internet Security, Q1-Q2 2009. The full report can be downloaded at <http://www.websense.com/threatreport>. Major findings from the report include:

Websense Security Labs identified a 233 percent growth in the number of malicious sites in the last six months and 671 percent growth in the number of malicious sites during the last year.

In the first half of 2009, 77 percent of Web sites with malicious code are legitimate sites that have been compromised. This high percentage was maintained over the past six months due in part to widespread attacks including Gumblar, Beladen and Nine Ball which aimed to compromise trusted and known Web properties with massive injection campaigns.

Web 2.0 sites allowing user-generated content are a top target for cybercriminals and spammers. Websense Defensio technology enabled Websense Security Labs to identify that 95 percent of user-generated comments to blogs, chat rooms and message boards are spam or malicious.

Efforts to self police Web 2.0 properties have been largely ineffective. Websense research shows that community-driven security tools used on sites like YouTube and BlogSpot are 65 percent to 75 percent ineffective in protecting Web users from objectionable content and security risks.

The dirty Web is getting dirtier: 69 percent of all Web pages with content classified as objectionable (e.g. Sex, Adult Content, Gambling, Drugs) also had at least one malicious link. This is becoming even more pervasive, as 78 percent of new Web pages discovered in the first half of 2009 with objectionable content had at least one malicious link.

Websense Security Labs found

that 37 percent of malicious Web attacks included data-stealing code, demonstrating that attackers are after essential information and data.

The Web continues to be the most popular vector for data-stealing attacks. In the first half of 2009 the Websense Security Labs found that 57 percent of data-stealing attacks are conducted over the Web.

The convergence of blended Web and email threats continues to increase. Websense Security Labs reports that 85.6 percent of all unwanted emails in circulation during this period contained links to spam sites and/or malicious Web sites.

In June alone, the

total number of emails detected as containing viruses increased 600 percent over the previous month.

Every hour, Websense Security Labs

ThreatSeeker Network scans more than 40 million Web sites and ten million emails for unwanted content and malicious code. Using more than 50 million real-time data collecting systems, ThreatSeeker Network monitors and classifies Web, email and data content providing Websense with unparalleled visibility into the state of content on the Internet and in email.

Quote:

Websense

Chief Technology Officer Dan Hubbard -- The last six months have shown that malicious hackers and fraudsters go where the people are on the Web - and have heightened their attacks on popular Web 2.0 sites and continued to compromise established, trusted Web sites in the hope of infecting unsuspecting users. From malicious Twitter spam campaigns and blog comment spam to the massive injection attacks, those perpetrating fraud are exploiting the inherent trust users have of known Web properties and other users.

Links:

Full

Report: <http://www.websense.com/threatreport> Webinar: <http://connect.websense.com/f41597193/Archived>  
Webinars: <http://www.websense.com/content/ProductResources.aspx>

Video:

State of the

Internet video recap: <http://www.youtube.com/watch?v=BNu1TXNYArI> Websense  
Security Labs on YouTube: <http://www.youtube.com/user/wslabsutube> Websense  
YouTube Channel: <http://www.youtube.com/user/WBSNMKTG>

Other Resources:

The Websense ThreatSeeker

Network: Leveraging Websense

HoneyGrid Computing [http://securitylabs.websense.com/content/Assets/ThreatSeeker\\_whitepaperFNL.pdf](http://securitylabs.websense.com/content/Assets/ThreatSeeker_whitepaperFNL.pdf)

Security Labs Security Effectiveness Center: <http://securitylabs.websense.com/content/ThreatUpdateCenter.aspx>

Security Labs Attack Information Center: <http://securitylabs.websense.com/content/threatResource.aspx>

Join Websense on Facebook: <http://www.facebook.com/websense>

Follow Websense Security Labs on

Twitter: <http://twitter.com/websenselabs>

Follow Websense Security Labs on

Twitter:

Websense Blog RSS feed: All Websense News RSS Feed

Websense Security Labs Alerts RSS

feed: <http://securitylabs.websense.com/content/alertsRSS.xml>

Websense Security Labs Blog RSS feed: <http://securitylabs.websense.com/content/blogsRSS.xml>

About Websense, Inc.

Websense,

Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection(TM) 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](http://www.websense.com).