

Top 10 Computer Security Threats for 2008

1. Malicious spam invades blogs, search engines, forums and Web sites

Websense predicts that hackers will increasingly use Web spam to post URLs to malicious sites within forums, blogs, in the commentary or 'talk-back' sections of news sites and on compromised Web sites. This activity not only drives traffic to the infected Web sites but also assists in the purveyor's site sitting higher on search engine rankings, increasing the risk that users will visit the site.

2. Attackers use Web's 'weakest links' to launch attacks

The Web is an entanglement of links and content. The advent of Web 2.0 additions such as Google AdSense, mash-ups, widgets, and social networks along with the massive amounts of Web advertisements linked to Web pages have increased the likelihood of 'weak links' -- or Web sites and content that are vulnerable to compromises.

Websense predicts that attackers will increasingly exploit the weakest links within the Web infrastructure in order to target the greatest number of Internet users. Most vulnerable to these attacks are search engines and large user networks such as MySpace, Facebook or other social networking sites.

3. Number of compromised Web sites will surpass number of created malicious sites

The Web as an attack vector has been steadily increasing for the last five years and now attackers are using compromised sites as their launching platforms -- even more than their own created sites. Compromising sites -- particularly, sites well-visited by end-users, such as the Dolphin Stadium attack that occurred a few days prior to the 2007 Super Bowl XLI in Miami, provides attackers with built-in Web traffic and minimizes the need for lures through email, instant messaging or Web posts.

4. Cross-platform Web attacks: Mac, iPhone popularity spurs increase

With the brand popularity and growing use of iPhones and Macintosh computers, Websense researchers predict attackers will increasingly launch cross-platform Web attacks that detect the operating system in use and serve up code specifically targeting that operating system instead of attacks based on just the Web browser. Operating systems that are targeted now include Mac OSX, iPhone, and Windows.

5. Rise in targeted Web 2.0 special interest attacks: Hackers targeting specific groups of people based on interests and profile

Web 2.0 has spawned a proliferation of Web users that visit chat rooms, social networking sites, and special interest Web sites such as travel sites, automotive, and more. These sites provide attackers with potential victims that fall within a certain age group, wealth bracket, or people with particular purchasing habits. In 2008, Websense

researchers predict targeted attacks will rise toward specific social networking or special interest sites that have a higher probability of delivering a payoff.

6. Morphing JavaScript to evade anti-virus scanners

Hackers are upping the ante with evasion techniques that use poly-morphic JavaScript (Polyscript) -- which means that a uniquely-coded Web page is served up for each visit by a user to a malicious Web site. By changing the code every visit, signature-based security scanning technologies have difficulty detecting Web pages as malicious and hackers can extend the length of time their malicious site evades detection.

7. New cyber attacks, phishing and fraud

Event-based attacks and scams are popular, and with the whole world watching, the 2008 Olympics may fuel a surge in cyberattacks, says Websense. As the Olympic torch burns, Websense researchers predict the possibility of large scale denial-of-service attacks on Beijing Olympic-related sites as political statements and fraud attempts through email and the Web surrounding the Olympics. Additionally, Websense predicts compromises of popular Olympic news or other sports sites -- attacks designed to install malicious code on end-users' machines and steal personal or confidential business information.

8. Data concealment methods increase in sophistication

Websense predicts an increased use of crypto-virology and sophistication in data concealment including the use of stenography, embedding data within standard protocols, and potentially within media files. Toolkits widely available on the Web will be used to embed proprietary information and steal data.

9. Global law enforcement will crack down on key hacker groups and individuals

In 2007, large-scale Internet-based attacks garnered the attention of law enforcement officials around the world. Websense anticipates that through the global cooperation of enforcement agencies, in 2008 the biggest crackdown and arrests of key members of a hacker group will occur.

10. Vishing and voice spam will combine and increase

The vast cell phone user population has grown into a lucrative market to exploit with spamming and 'vishing' for financial gain. To date, researchers have seen an increased number of vishing attacks but not a lot of spam -- or pro-active automated calling. In 2008 Websense predicts that 'vishing' or the practice of using social engineering and Voice over IP (VoIP) to gain personal and financial information, and voice spam will combine and increase -- users will receive automated voice calls on LAN lines with voice spam to lure them to input their credentials through the telephone.