

Top Ten Security Trends for 2009

1 Cybercriminals will increasingly use SQL injection attacks and IFRAME injections.

There will be growing use of SQL injection and IFRAME attacks against primarily legitimate Web sites during 2009. Victims of such attacks during 2008 included BusinessWeek, USA Today, Wal-Mart, Sears and The Miami Herald, among many others. These attacks will increase for two simple reasons: a) they work and b) most users are completely or inadequately protected against them. As testament to the efficacy of these types of attacks, Sophos found that one new Web page was infected every 4.5 seconds during 2008.

2 Web sites will continue to remain vulnerable to attack until security training and testing become the norm for Web developers.

Web developers—unsurprisingly—focus on the development of new and better Web sites and applications. They do not focus nearly as heavily on security, leaving their applications vulnerable to a host of ever-more virulent and more sophisticated attacks. Until security becomes a sufficiently high priority, Web sites and related applications will continue to be ripe for attack by cyber criminals.

3 Malware infections will spread through fake software updates.

Fake software updates for Adobe Flash Player, Microsoft elements, or anti-malware will leverage users trust to download malware. Users may desire to see an online video and they are presented with a flash player update first, blindly they say “Yes” to the fake update and the malware downloads, then the video starts. Cyber criminals will increasingly fake software updates to spread malware and gain access to sensitive information.

4 Thieves and other criminals will continue to target laptops and mobile devices that hold valuable, identity-based information.

Mobile devices, including laptops, are becoming the primary work platform for a growing number of users – 2008 saw the first year in which laptop sales outpaced sales of desktop computers. Cybercriminals, recognizing this trend, will increasingly focus on mobile platforms in an attempt to access the sensitive corporate information stored on them. Mobile platforms are more vulnerable to attack, in part because many users access unsecured networks at hotels, airports, coffee shops and other public places. This, among many factors, has allowed cybercrime to become a larger “industry” than illegal drug trafficking.

5 The allure of online video sources, such as YouTube, will spread malware in a more serious way during 2009.

Sources of video content are rapidly becoming more popular among corporate and personal users, and are increasingly used to distribute business content. Venues for video content, such as YouTube, will become a favorite lure of cyber criminals as users flock to these sources for entertainment and, sometimes, valid business purposes.

6 A variety of common devices—some of which might be in your family room—are now vulnerable to attack.

Electronic items from digital picture frames to memory sticks to Xboxes to other video games are open to cyber criminal attack. The problem has become so serious, in fact, that the US Army recently issued an order banning the use of USB thumb drives in an effort to stop the spread of malware.

7 Botnets will continue to become a more serious problem.

More than 80% of spam today comes from botnets—networks of compromised home and corporate computers that have been infected with malware and are used to send a variety of threats. Botnets have the dual advantage (to cyber criminals) of allowing malicious content to be sent in a highly distributed manner and they offer a highly lucrative source of income through their rental to those who manage spam and malware campaigns.

8 Social networking sites will become a more dangerous source of malware.

Social networking sites allow you to find old friends and new malware. The popularity of these tools is being exploited by cyber criminals to spread malware using social engineering techniques akin to those exploited by criminals who distribute their attacks through instant messaging systems. Facebook has been a key victim of these attacks, but expect business-oriented social networking tools to become victims of these attacks, as well.

9 Biometrics will become more important as a tool in protecting identity.

The use of biometric technology, such as the technology used to scan fingerprints, will permit users to gain greater control over the use of their identity. Biometrics will be useful in slowing the growth of identity theft and raising the bar for cybercriminals.

10 Community-based cloud services will become increasingly important as a means of protecting individuals and networks.

One against the Web simply doesn't cut it anymore, nor do "brick-and-mortar" gateways to protect against the growing number of malware attacks. Instead, the most effective protection will increasingly come from community-based, cloud-based services that provide protection via the participation of a growing number of users.

About Blue Coat Systems

Blue Coat Systems is the technical leader in application delivery networking. Blue Coat offers an application delivery network infrastructure that optimizes and secures the flow of information to any user, on any network, anywhere which fuels a sustainable competitive advantage for distributed enterprises. Over 15,000 of the most demanding organizations, including 81% of the Fortune Global 500®, trust Blue Coat with their mission-critical applications. Additional information is available at www.bluecoat.com.