Top 10 Security Trends for 2008

❶ The Hack is back! Actually ill-intentioned hackers (who were never really gone) will continue to inject Mobile Malicious Code (MMC) into otherwise reputable sites.

Using SQL and iframe injections, plus other attacks, hackers go on infecting popular, legitimate Web sites with malicious code. Typically, the infections are timed for peak traffic at the site. The worst part is that visitors don't have to explicitly download any content to have their own machines infected. Simply browsing or "driving by" sections of these infected sites allows evil scripts to embed themselves in customer PCs and do tremendous damage. Because these are well-known, reputable sites—some of the most trusted names in online news and commerce—URL-filtering and reputation tools won't block users from visiting them.

❷ Web sites will remain vulnerable to attack until security training and testing become mandatory for Web developers.

Web site developers are busy learning about new technologies such as Adobe Flex and Microsoft Silverlight. Security remains an afterthought. As well, evil-doers continue to develop new programs for breaking through firewalls and infiltrating HTTP applications and SSL communications continues. To stay safe requires vigilance and reliable security solutions.

❸ Malware infections will spread through widgets in Web sites and dashboards.

Even hailing from such leading developers as Microsoft and Yahoo!, widgets have been found to have insufficient security features, leaving them vulnerable to infection. Because widgets often have access to the host operating system, they pose major risks to users.

❹ Thieves and "ne'er-do-wells" will continue to target laptops harboring valuable identity-based information.

The black market for personal records (about $14/name) makes laptops attractive targets for thieves. A laptop with records for 10,000 employees, for example, is worth about $140,000 on the black market. Not bad for a dishonest day's work!

❺ Online videos will become a channel for attacks.

Cisco has already had to patch its VOIP protocol to close a security loophole. Vulnerabilities surely exist in video formats, as well. The ever-growing popularity of videos and video sites such as YouTube ensures that hackers will not neglect this format for long.

❻ Infected devices might even be sitting on your living room mantel! Digital picture frames and memory sticks are now vulnerable to attack

In February, a major electronics retailer warned customers that a popular model of digital picture frame, which connects to a computer over a USB port to display images, had become infected with the Mocmex Trojan Horse. The popularity of digital photography and music downloads is leading users to connect a wide variety of devices to their computers. Unfortunately, not all these devices are safe.

❼ Storm warning! Botnets, like the Storm botnet, will be responsible for the bulk of spam and malware infections this year.

Major botnets (networks of infected computers) are now for rent to spammers and criminals. The Storm botnet, comprising over 85,000 machines infected by a Trojan , sent about 20% of the world's spam in 2007. Researchers have recently discovered new, even more insidious botnets, such as MayDay.

8 Through social network sites, we'll find old friends—and new malware.

Facebook and MySpace continue to add users at an impressive clip, but these sites and their myriad applications are vulnerable to attack. For example, security researchers recently identified Facebook's image uploader as a significant threat to end user security.

9 In response to identity thefts, companies will begin using custom identity numbers rather than Social Security numbers to identify individuals.

New identity standards such as Open ID will gain popularity as organizations try to minimize exposure to identity theft.

10 Web security will continue to be thwarted by the performance and scalability limitation of most Web gateway products.

A "dirty little secret" of the IT security industry is that most Web security gateway products are architecturally incapable of scaling to meet enterprise needs. Enterprises will continue to find themselves short-changed by products that promise comprehensive network protection but don't deliver on performance.

Conclusion

Security threats still abound and some can be disastrous to company IT infrastructure and corporate data. To better protect your organization, we suggest:

-> Be aware and keep current of these threats

-> Learn how to recognize their format and pattern and watch for them

-> Educate all members of the IT Dept and Senior Managers

-> Deploy tools to help you protect your data

Do research and look for vendor tools that provide you with not just desktop anti virus protection, but also:

-> Distributed application threat monitoring

-> Information on employee web browsing activity

-> Prevention from virus injected reputable web sites

-> Filtering to block malicious URLs and code

-> Laptop lock down and recovery processes

About Blue Coat Systems

Blue Coat WAN Application Delivery solutions "stop the bad and accelerate the good," optimizing application performance and security for any user, anywhere, across a distributed enterprise. Blue Coat's proxy architecture completely understands users and applications on the network, affords granular control over security, and permits fast, secure delivery of all applications critical to running the business.

Blue Coat Systems is the world's largest provider of WAN Application Delivery solutions. Over 6,000 of the most demanding enterprises, including 93 from the top 100 of the Fortune Global 500®, trust Blue Coat to secure and accelerate mission-critical applications. Additional information is available at www.bluecoat.com.