

# Cybercrime

## Security Threat Trends for 2008

*"Forewarned is forearmed. We make these predictions to help raise awareness for customers and the industry. But these predictions also guide our product direction. Many of the new technologies released in Symantec's 2007 security products were put there to better protect our customers from the threats of 2008 and beyond. By continually monitoring the threat landscape, we are better able to anticipate the protection customers will need to safeguard their online interactions."*

Kevin Haley

Director, Product Management for Symantec Security Response

It's the time of year to look back and take stock of the events over the past twelve months. Newspapers and magazines have published their list of top movies, records, and books. Symantec is publishing a top 10 list, too. While not as fun, in many cases this collection of security trends confirms that the predicted evolution of cybercrime has become more professional and commercial.

### A Year in Review - A Look Back at the Security Trends of 2007

Attackers are exploiting current events and trusted brands to trick computer users in an effort to make money. And security companies like Symantec continue to block their efforts.

- **Data Breaches.** High-profile data breaches underscored the importance of data loss prevention technologies and strategies.
- **Windows Vista™ Introduction.** Windows Vista made its debut and quickly attackers found holes. Microsoft® has already released 16 security patches to address impacts on the new operating system.
- **Spam.** In 2007, spam reached new and record levels. Image spam declined while PDF spam emerged as a new annoyance. Greeting-card spam was also responsible for delivering Storm worm malware (also known as Peacomm).
- **Professional Attack Kits.** Today's attackers are increasingly sophisticated and organized and have begun to adopt methods that are similar to traditional software. MPack is just one illustration of this phenomenon.
- **Phishing.** Phishing continued to be big in 2007 with an 18 percent increase in unique phishing sites during the first half of the year. Phishing toolkits contributed to the problem. A recent Olympic phishing scheme illustrates the topical tricks phishers use as bait.
- **Exploitation of Trusted Brands.** By exploiting a trusted Web environment, attackers now prefer to lie in wait for victims to come to them.
- **Bots.** Bots and botnets continued to silently slip onto unsecured computers and perpetrate a wide variety of malicious activity. Bots knocked Estonia.com off the online map and the Storm worm employed bot technology as well.
- **Web Plug-in Vulnerabilities.** Web plug-in vulnerabilities and exploits continued to plague IT staff during 2007. ActiveX controls comprise the majority of plug-in vulnerabilities and pose various security threats that may compromise the availability, confidentiality, and integrity of a vulnerable computer.
- **Vulnerabilities for Sale.** WabiSabiLabi debuted and offered an auction-style system for selling vulnerability information to the highest bidder, sparking controversy and discussion

Symantec is the market leader in tackling tough threats; technology, expertise, and history enable us to deliver comprehensive protection against the latest breed of attacks. Symantec delivers confidence with:

- Innovative security technologies to handle the toughest threats with over 250 issued patents
- Unrivaled, worldwide security intelligence network
- Timely early warning protection via 24x7x365 coverage
- Fastest, most comprehensive analysis from a global team of security and operational specialists
- Security intelligence and protection content across Symantec's products
- Staying ahead of tomorrow's threats

between competing schools of thought on how to handle vulnerability information.

- **Virtual Machine Security Implications.** Virtualization made big headlines in 2007 with major players going public. Security researchers are actively exploring the security implications of virtual technology.

### A Look Ahead - Security Trends for 2008

There are no fortune tellers in Symantec Security Response, but with the data gathered by the Symantec Global Intelligence Network, the company's 200+ trained security analysts have enough insights to make a pretty good prediction of what will be happening in cybercrime in the New Year.

Here is the Security Response team's forecast of the most likely security challenges for 2008:

- **Bot Evolution.** Hackers infect computers and turn them into zombies or robots ("bots") that do their bidding, including denial of service attacks and sending spam. Security Response expects bots to diversify and evolve in their behavior. Bot networks will come up with new ways of hiding from the good guys, and we may even see phishing sites hosted by bot zombies.
- **Election Campaigns.** As political candidates increasingly turn to the Internet, Security Response expects to see associated security risks develop. These risks include the diversion of online campaign donations; dissemination of misinformation about candidates' positions and conduct; fraud; phishing; and invasion of privacy threats. For example, information captured by a keylogger placed on the computer of a candidate, an aide, or a family member could be used to embarrass or damage that person's political campaign.
- **Advanced Web Threats.** As the number of available Web services increases and browsers continue to converge on a uniform interpretation standard for scripting languages such as JavaScript™, Security Response expects that the number of new Web-based threats will continue to increase.
- **Mobile Platforms.** Any platform that is in widespread use draws the attention of the bad guys, so interest in mobile security has never been higher. With mobile phones becoming ever more complex and more connected, Security Response expects attackers to take advantage of them.
- **Spam Evolution.** Security Response expects to see spam continuously evolve in order to evade traditional blocking systems and trick users into reading messages. For example, in November 2007 we saw spam in the form of an mp3 file. Instead of hearing a song, people who clicked on the link heard a promotional message for a stock.
- **Virtual Worlds.** Security Response expects that as the use of persistent virtual worlds (PVWs) and massively multiplayer online games (MMOGs) expands, new threats will emerge from criminals, phishers, spammers, and others turning their attention to these

### Symantec Global Services

Deep technical knowledge, proven expertise, and global insight to help organizations identify and avert potential threats in today's security landscape

- Outsource key functions
- Augment your staff
- Gain a trusted advisor
- Implement a product or solution
- Get early warning on threats
- Evaluate support options
- Get training on products and services

new communities. Security Response researchers have already seen World of Warcraft® accounts for sale in the underground economy.

### Additional Resources

- **Internet Security Threat Report:** The Symantec Internet Security Threat Report provides a six-month update of Internet threat activity. The report covers attacks, vulnerabilities, malicious code, Phishing, spam and security risks.
- **Security Weblog:** The Security Response Weblog delivers cutting edge information on research and threats as they happen. Readers will find interesting, relevant, and edgy discussions by some of the top minds in their fields.
- **Security Updates:** Security Response provides your Enterprise with world-class analysis and protection from viruses, blended threats, security risks and vulnerabilities. Information on availability of updates, definitions and signatures are provided daily.

### Contact Us Today

Call toll-free 1 (800) 745 6054

### Visit our Web site

<http://enterprise.symantec.com>

### About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

### Symantec World Headquarters

20330 Stevens Creek Boulevard  
Cupertino, CA 95014 USA  
+1 (408) 517 8000  
1 (800) 721 3934  
[www.symantec.com](http://www.symantec.com)