

Symantec White Paper: Cybercrime Trends in 2008

Every year, Symantec's Internet security experts look ahead to new trends in the threat landscape. "Forewarned is forearmed," says Kevin Haley, Director of Product Management for Symantec Security Response. "We make these predictions to help raise awareness, and to help guide Symantec product development."

Here is a look at anticipated threats for 2008.

BOT Evolution

Bots are programs that secretly download and install themselves on a victim's computer. Cybercrooks can then remotely control the machine, using it for such criminal activities as sending spam or launching denial-of-service attacks.

BOT networks will continue to diversify and evolve. For example, criminals may use infected machines to host phishing sites.

Political Campaigns

The increasing reliance of political campaigns on Web sites for fundraising and organizing opens the door to serious security risks, including:

- Diversion of online campaign donations or donor information
- Web site hacking to present misinformation about candidates' positions and conduct
- Crashing of the Web site at a crucial time

Advanced Web Threats

Java-based Web applications—small programs, such as video players or interactive maps, that launch themselves from a Web page—are proliferating, which will provide a growing opportunity for cyberthieves to spread bots, keyloggers, and other malicious software.

Spam Evolution

Spammers will find new ways to evade traditional blocking systems and to trick users into reading their messages. For example, spammers are now using pictures of their text, rather than actual text, to evade content filtering. Moreover, in November 2007, Symantec observed spam in the form of an MP3 file: People who clicked a link expecting to hear a song instead heard a stock tip.

Mobile Platforms

As mobile phones support a greater range of applications, hackers will move in and find vulnerabilities to exploit.

Virtual Worlds

Cybercriminals will focus on communities of persistent virtual worlds and multiplayer online games. Stolen passwords and game resources are a growing segment of the underground economy.

Conclusion

Cyberthreats will continue to evolve, finding vulnerabilities in new software, applications, and devices. Consumers can protect themselves by using reasonable precautions online, keeping their security software current, and updating all their applications with the latest security patches.