



Trends

September/October 2008

Top IT Security threats of 2008

The SysAdmin, Audit, Networking and Security (SANS) Institute has released its list of the top 10 cyber security threats for 2008. The list includes:

- new developments of evergreen security risks,
- new exploitations of browser vulnerabilities,
- worms with advanced peer-to-peer technologies,
- insider attacks by rogue employees, consultants or contractors, and
- mobile phone technologies and voice over internet protocols (VoIP).

As a manager, you should be asking what are the greatest security threats facing your company's business network? And, what can be done to keep it secure?

Social Threats

Does your company use a standard instant messaging or IM client to keep in touch desk-to-desk such as AOL Instant Messenger, Yahoo or Internet Relay Chat? Do employees access social networking sites at work like MySpace.com or Facebook? Do you use Google Talk, Skype or other voice-over-Internet technologies to connect with customers? What was once considered to be relatively secure technologies on personal computers, can pose significant security risks to a secure business network.

In 2007, more than 1,000 malware attacks were reported coming from IM and chat clients alone, according to FaceTime Communications Inc., an IM security and compliance firm. Social networking sites were besieged by social engineering which tricked visitors into clicking links that activated malicious code spreading viruses such as the Skype worm and advancing phishing and identity theft. The introduction of Apple's new iPhone has been labeled as a "security nightmare" for the potential to expose business data to outsiders.

Espionage

In January 2008, the US Central Intelligence Agency admitted that cyber attacks had caused multicity blackouts and the loss of critical national data. Such attacks were traced back to IP addresses in China, where the People's Liberation Army has created an "elite Chinese unit" trained for "information warfare" and capable of carrying out "sophisticated attacks on high-risk targets." Not surprisingly, the threat of cyber espionage ranks as number three on the SANS Institute's list.

How Secure Do You Feel Now?

View the complete SANS Institute list of security threats that follows and share it with your IT department to gain an understanding of your company's risk exposure.

1. Sophisticated Web Site Attacks That Exploit Browser Vulnerabilities - Especially On Trusted Web Sites

Website attacks on browsers are increasingly targeting components, such as Flash and QuickTime, that are not automatically patched when the browser is patched. Website attacks have migrated from simple, based on one or two exploits posted on a website, to sophisticated, based on scripts that cycle through multiple exploits or packaged modules that effectively disguise their payloads. One of the latest such modules – mpack – claims a 10-25% success rate in exploiting browsers that visit infected sites.

2. Increasing Sophistication and Effectiveness In Botnets

The Storm worm started spreading in January 2007, with an email saying, "230 dead as storm batters Europe". Within a week, it accounted for one out of every twelve infections on the Internet, installing rootkits and making each infected system a member of a new type of botnet. Previous botnets used centralized command and control; the Storm worm used peer-to-peer control, so there was no central controller to take down. Additional variants have used messages with different subjects and improved the capabilities of rootkits. In 2008, additional variants and increased sophistication will keep this worm and others near the top of the list of security threats.

3. Cyber Espionage Efforts by Well Resourced Organizations Looking to Extract Large Amounts of Data - Particularly Using Targeted Phishing

One of the biggest security stories of 2007 was disclosure in Congressional hearings and by senior US Department of Defense officials of massive penetration of federal agencies and defense contractors and theft of terabytes of data by the Chinese and other nation states. Despite intense scrutiny, these nation-state attacks will expand; more targets and increased sophistication will mean many successes for attackers. Economic espionage will be increasingly common as nation-states use cyber theft of data to gain economic advantage in multi-national deals. The attack of choice involves targeted spear phishing with attachments. It uses social engineering to make victims believe an attachment comes from a trusted source, and then takes advantage of Microsoft Office vulnerabilities and hiding techniques to circumvent virus checking.

4. Mobile Phone Threats, Especially Against iPhones and Androids Plus VoIP

Mobile phones are general purpose computers, so worms, viruses, and other malware increasingly target them. Google's announcement of "android" and the formation of the "open handset alliance" is a watershed moment for the mobile phone industry. A truly open mobile platform will usher in unforeseen security nightmares. Developer toolkits provide easy access for hackers who are taking note. Attacks on VoIP systems are on the horizon as VoIP phones and IP PBXs have numerous published vulnerabilities. Attack tools exploiting these vulnerabilities are currently available on the Internet.

5. Insider Attacks

Insider attacks are initiated by an organization's rogue employees, consultants and/or contractors. Insider risk has long been exacerbated by the fact that insiders usually have some degree of access to systems, databases, and networks. Recently, however, there are cases where security has broken down, allowing insiders to attack from both inside and outside an organization's network boundaries. One defense against this type of risk is limiting employee access to IT systems based on job requirements.

6. Advanced Identity Theft from Persistent Bots

A new generation of identity theft is being powered by bots that stay on computers for three to five months collecting passwords, bank account information, surfing history, frequently used email addresses, and more. They gather enough data to pass basic security checks, enabling extortion and identify theft.

7. Increasingly Malicious Spyware

Attackers continue to refine the capabilities of malicious code, expanding on flux techniques to obscure their infrastructure and making it harder to locate their servers. Additionally, the ability of attackers to detect investigator activity and respond with an attack will become more mainstream and powerful. Tools will increasingly target and dodge anti-virus, anti-spyware, and anti-rootkit software to preserve the attacker's control of a computer for as long as possible. In short, malware will become stickier on target machines and more difficult to shut down.

8. Web Application Security Exploits

Large percentages of web sites have cross site scripting, SQL injection, and other vulnerabilities resulting from programming errors which can be exploited by criminals looking for financial gain. Web 2.0 applications are vulnerable because user-supplied data cannot be trusted; the script running in the users' browser still constitutes "user supplied data." In 2008, web 2.0 vulnerabilities will be added to more traditional programming flaws and web application attacks will grow substantially.

9. Increasingly Sophisticated Social Engineering Including Blending Phishing with VoIP and Event Phishing

Blended approaches will amplify the impact of more common attacks. For example, the success of phishing is being radically increased by stealing IDs of users of other technologies. Salesforce.com users were targeted for an "FTC complaint" phishing email. Monster.com users were targeted for a job offer phishing email. Even if it is non-targeted, event phishing is gaining in sophistication. Tax filing and US presidential election scams will be widely used in 2008, and many of them will succeed. An email with the subject "Obama drops out of presidential race" could generate huge new botnets of people who are interested in politics, but may not have patched their systems fully. Add to those opportunities potential bogus fund raising sites and political dirty tricks going digital, and you'll have an explosive junction of hacking and politics.

A second area of blended phishing combines email and VoIP. An inbound email being sent by a credit card company asks recipients to "re-authorize" their credit cards by calling a 1-800 number. The number leads them (via VoIP) to an automated system in a foreign country that convincingly asks the caller to key in their credit card number and expiration date.

10. Supply Chain Attacks Infecting Consumer Devices (USB Thumb Drives, GPS Systems, Photo Frames, etc.) Distributed by Trusted Organizations

Retail outlets are increasingly becoming unwitting distributors of malware. Devices with USB connections and CDs packaged with those devices sometimes contain malware that infect computers and connect them to botnets. This has been seen among conference attendees who are given USB thumb drives and CDs that supposedly contain conference papers, but also contain malicious software.

Excerpts by Jim Higdon, January 23, 2008, [IT Security](#) and [The SANS Institute website](#).