Cyber Crime Protection

A Midwestern company's computer system became infected with a virus that tracked keystrokes. The hacker was able to decipher the log-on keystrokes to the company's bank, logged on, and sent $160,000 in ACH credits to various bank accounts. The money was sent overseas to bank accounts controlled by the thief. The company was shocked when its bank denied liability for the loss because the log-on was authentic. A bank is not responsible for the integrity of a customer's computer.

Of the companies responding to the 2008 CSI Computer Crime and Security Survey, the overall average annual loss due to computer security incidents was almost $300,000 per company. At the end of 2007, Symantec had detected 499,811 new malicious code threats, a 571% increase over the second half of 2006.

Computer crime is becoming "professionalized" and criminals have adopted stealthier attack techniques. They now target end users on individual computers through the Web, rather than attempting widespread broadcast attacks to infiltrate networks. The Web is now the primary avenue for attacks, as demonstrated by the 11,253 site-specific vulnerabilities versus the 2,134 traditional vulnerabilities verified by Symantec in 2007. Social networks like Facebook and MySpace are prime targets for cyber crime activities.

Bots are programs secretly installed on a computer, allowing a malicious user to control it remotely. Attackers scan the Internet to find computers that are unprotected, and then install software through "open doors." For example, attachments, links or images in spam email, if opened, can install hidden "bot" software. Sometimes visiting a website or downloading files may cause a "drive-by download," which installs malicious software, turning your computer into a "bot." An attacker controls a large number of "bot" computers in a botnet, which can then be used to launch coordinated attacks. If you find unknown messages in your out box, or if messages bounce back that you did not send, it's a sign that your computer may be part of a botnet.

The Verizon 2008 Data Breach Investigations Report found that of the 500 data breaches that were investigated, more than half only required minimal skills to commit. Basic security protections and procedures would have thwarted them. Here are some of the ways individuals and companies can protect themselves. For more details, see **"Resources"** below.

For Individuals

- Use anti-virus and anti-spyware software that removes or quarantines viruses, and set it to perform daily automatic updates. Consider Norton Internet Security 2009 (no longer a resource hog), AVG, Kaspersky, McAfee, etc.
- Use a properly-configured firewall, which helps make you invisible on the Internet and blocks incoming communications from unauthorized sources.
- Do not follow links found in emails messages from untrusted sources, as these may be links to spoofed Web sites. Manually type the URL into your browser bar.
- Unplug your Internet connection when you're away.
- Never reply to an email, text, or pop-up message that asks for personal or financial information

- Never open an email attachment unless you are expecting it or know what it contains
- Download software only from trusted sites.
- Restrict which applications you install on social networks, and never install a codec from a random Web site.
- Don't send sensitive files over a Wi-Fi network unless it is secure. Most public "hot spots" are not secure.
- When you're not using Wi-Fi, turn off the wireless connection to your laptop.
- Don't respond to a message asking you to call a phone number to update your account or give your personal information. If you need to reach an organization, look the number up yourself.
- You can track your child's keystrokes, emails, IM, MySpace, Facebook and websites visited with **Spector Pro** (spectorsoft.com). You can also have their emails forwarded to you by including eBlaster. Never divulge the source of your "parent's intuition."

For Companies and Organizations

- The recommendations for individuals (above) also apply to companies and organizations.
- Implement security policies to restrict unauthorized access to sensitive data.
- Require that all sensitive data be encrypted or password protected before transmission. Adobe Acrobat 7 and higher does this easily. Other programs may, as well.
- Regularly review updated patches for your operating system software, and install those that tighten your security.
- Develop written policies for using flash drives, etc. Some companies fill in the flash drive port with epoxy to stop data theft.
- Install software to limit the sites users may access; be cautious about visiting unknown or untrusted Web sites
- Use a network-based Intrusion Prevention System (IPS)
- Maintain a whitelist of trusted Web sites, and disable individual plug-ins and scripting capabilities for other sites.
- Educate in-house developers about secure development practices, such as the Security Development Lifecycle.
- When employees leaves the company, immediately disconnect their access to the company's network and building, shut down remote connections, and collect their cell phones, iPDAs, smartphones, etc.
- Consider using a Virtual Private Network (VPN), an advanced networking feature for Wi-Fi transmissions.

Resources

2008 CSI Computer Crime and Security Survey
Symantec Global Internet Security Threat Report (2006, 2007)
Verizon 2008 Data Breach Investigations Report
OnGuardOnline.gov
fbi.gov/cyberinvest/protect_online.htm (several articles on website)
getnetwise.org
pcisecuritystandards.org
PC Magazine (pcmag.com)
CNET Networks (cnet.com)
"Small Business Security, New Entrepreneurial Solutions" Brigham Young University, Marriott School of Management Alumni Magazine, Fall 2008