

In This Issue

1. *Security Myths* – 2. *Scams and Hoaxes* – 3. *Malware* – 4. *Microsoft and Apple Security Updates* – 5. *Security Screw-Up of the Month* – 6. *Security Newsbytes*

1. Security Myths

Firewall Foibles

Myth: I've heard that hardware firewalls are better than software firewalls.

Fact: Hardware and software firewalls provide different protections for your computer, which make it a good idea to have both. If you have DSL (digital subscriber line), for example, chances are good that your DSL modem also acts as a basic hardware firewall; it makes your system invisible to the Bad Guys out there prowling around on the Internet. "Security by obscurity" is an important primary defense, but many kinds of viruses, worms, and spyware can get past this kind of protection. A software firewall, your best secondary defense, should be ready and waiting to stop the malware before it gets loose in your computer where it can both compromise your personal information and begin attacking other networked computers.

Myth: I know that my DSL modem is also a hardware firewall, and I have the Windows firewall turned on, so I don't need a separate software firewall.

Fact: With a basic hardware firewall in place and the Windows firewall turned on, *your* system is protected against hacking attempts from the Internet and the ill effects of many varieties of malware. But the Windows firewall is one-directional; it only defends your computer against incoming attacks. Your computer can still get infected via other means such as infected e-mail attachments. If it does, your computer may start acting out and attacking other networked computers, also without your knowledge. A two-directional firewall will help quash outgoing attacks directed at other computers as well incoming ones directed at your computer, and serves to alert you that your computer has become infected so you can take the steps to correct the problem.

2. Scams and Hoaxes

-- Bank, Credit Union, Pay-Pal, and eBay Phishing Scams

Bait: As we approach the end of summer 2007, these email phishing scams are fewer in number, but are still going strong. Remember that banks, credit unions, Pay-Pal, and eBay never send out emails asking account holders and members to provide or verify personal information. If you do get one about an institution you belong to, you should call them.

More information: <http://www.millersmiles.co.uk/>

--Fake E-card Emails Beget Fake Membership Emails

Bait: Emails claiming that you have received a free, temporary membership in a website providing resume listings or cellphone ringtones.

The criminals responsible for the fake e-Card messages changed tactics and began distributing these bogus membership confirmation emails in August. The login link in the

email actually points to a dirty website that attempts to install yet another Trojan. It may also attempt to trick you into manually installing malware components. The bogus web page may contain a message similar to the following: *If you do not see the Secure Login Window please install our **Secure Login Applet**.* Don't fall for any of it.

More information: <http://www.hoax-slayer.com/login-trojan-emails.shtml>
<http://www.hoax-slayer.com/postcard-from-family-member.shtml>

- Bum_tnoo7 Hacker Warning Hoax

Bait: Emails claiming that "bum_tnoo7@hotmail.com" is the address of a hacker and simply by accepting the address into your instant messaging contact list, you will allow the hacker access to your computer. The warning has been rapidly circulating around social networking communities such as Facebook and MySpace and is also travelling via instant messages and email. This warning is bogus and should not be taken seriously. The message is, in fact, nothing more than a spin-off of the long running MSN contact list virus hoax.

More information: <http://www.hoax-slayer.com/bumtnoo7-hacker-hoax.shtml>
<http://www.hoax-slayer.com/msn-contact-virus-hoax.html>

3. Malware

Infostealer.Monstres, a Trojan that installed itself on many users' computers, has stolen over 1 million records from the Monster.com job search website's database, including the name, email address, home address and phone numbers of several hundred thousand job-seekers, based mostly in the United States.

More information:

<http://www.techworld.com/security/features/index.cfm?featureid=3626&pagtype=all>
http://news.com.com/Monster.com+waited+5+days+to+disclose+data+theft/2100-7349_3-6204261.html?tag=cd.lede

Editor's Note (Reichert): If you didn't read Section One of this issue on Firewall Foibles, go back and read through it. This is an excellent example of why you want a two-directional firewall on your machine.

Storm Worm, a worm that spreads by infected email attachments, began spreading and creating botnets in January. Many variants that have appeared since then make it a tough security opponent. The latest targets have been colleges and universities. The malware's latest trick is to strike back at the computers pressed into service to scan networks and remove the worm. (See also Security Newsbytes below.)

More information: http://www.infoworld.com/article/07/08/14/Record-breaking-Storm-Trojan_1.html

VirusProtectPro, a Trojan masquerading as an anti-virus and anti-spyware product installs itself on your computer without your permission and creates a series of pop-ups suggesting that you need to purchase more products like it.

More information: <http://www.pcindanger.com/virusprotectpro-removal.html>

Editor's Note (Rietveld): This imaginative malware has all the elements of well done IT parody – no exotic name, no unexpected attachment, no bogus claim on how to make money, just a “straightforward” offer to protect yourself from Bad Guys, expressed in language that ordinary computer users understand and are accustomed to: “Virus”, to get your attention; “Protect” to reassure you; and “Pro” to suggest that it is the Real Thing.

4. Microsoft and Apple Security Updates

Microsoft provides free security updates for Windows, as does Apple for Mac OSX and the iPhone.

Windows: Microsoft issues patches for all Microsoft products on the second Tuesday of each month as well as out-of-cycle patches on any day of the month. The next scheduled release date is September 11th. Check manually too, once every two weeks, to make sure all of the updates have been installed.

More information: <http://www.microsoft.com/athome/security/default.mspx>

OS X: Updates are issued frequently, and their contents may differ depending on which processor is in your Mac (PPC or Intel).

More information: <http://www.apple.com/support/downloads/>

iPhones: Must be updated manually:

<http://docs.info.apple.com/article.html?artnum=305744>

Security Tips: Be sure your operating system is set to retrieve and install updates automatically.

Windows:

<http://www.microsoft.com/athome/security/update/bulletins/automaticupdates.mspx>

OSX: <http://docs.info.apple.com/article.html?artnum=106704> &

<http://docs.info.apple.com/article.html?artnum=301191>

5. Security Screw-Up of the Month

IRS Gives Away Security Information and Wireless Network Access

IRS employees ignored security rules and turned over sensitive computer information to a caller posing as a technical support person, according to a government study. Sixty-one of the 102 people who got the test calls, including managers and a contractor, complied with a request that the employee provide his or her username and temporarily change his or her password to one the caller suggested, according to the Treasury Inspector General for Tax Administration, an office that oversees the Internal Revenue Service. The caller asked for assistance to correct a "computer problem."

The IRS has a history of responding slowly to calls for improving security and providing security training for its 100,000 employees. A 2003 study by the Treasury Inspector General for Tax Administration found unauthorized wireless devices directly connected to an IRS-wide network. They recommended that the agency issue policies and procedures for the use of wireless technology and scan for unauthorized networks and devices. But an inspection of 20 IRS buildings in 10 cities in 2006 found at least one unauthorized wireless network and strong indications of three others. In addition, an improperly configured agency computer connected to the wireless network could give a hacker access to the agency-wide network, the report stated.

More information: <http://www.epic.org/privacy/surveillance/spotlight/0306/>

6. Security Newsbytes

YouTube and You Lose

A hacker group known as "Storm Botnet" began flooding the Internet over the weekend with emails, inviting Web users to watch a salacious video starring them on YouTube, the video-sharing site owned by Google. However, links in the emails actually point to attacker-operated sites that try to download several malicious programs onto vulnerable personal computers. Once infected, victimized PC's become spam machines, "zombies"

that Storm Botnet can use to attack other computers. The attackers also plant a rootkit in victim PCs that tries to hide the malicious programs so antivirus software can't remove them. (See also Malware above)

More information:

http://blog.washingtonpost.com/securityfix/2007/08/storm_worm_authors_turn_to_you.html

Insecure Security Products

Several anti-malware vendors have issued security updates for their products recently. The highest-profile fix was by Trend Micro, which patched numerous flaws in its ServerProtect, Anti-Spyware, and PC-cillin products. CheckPoint Labs also fixed a serious vulnerability in their ZoneAlarm products—a privilege-escalation error could allow attackers to disable the software or gain unauthorized access to the system. Finally, ClamAV, the open-source security software recently acquired by SourceFire, recently added fixes for denial of service and other bugs.

More information:

http://blogs.pcmag.com/securitywatch/2007/08/insecure_security_products.php

More Bad News for Yahoo Messenger

According to McAfee Avert Labs, there is a zero-day vulnerability* in Yahoo Messenger. The discovery marks the second time in a month that security researchers have disclosed vulnerabilities in the instant-messaging client. McAfee researchers first learned about the bug on a Chinese-language security forum, then dug into the report and were able to reproduce the vulnerability on Yahoo Messenger. Yahoo has released a patched version of its Messenger.

More information: http://www.newsfactor.com/story.xhtml?story_id=54669

<http://messenger.yahoo.com/download.php>

*Definition: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci955554,00.html

Skype Says Crash Was Not Their Fault (Sort of)

The widespread failure of Skype's Internet telephony service in mid-August happened when millions of Windows users tried to log in to the system at the same time, after downloading a software update from Microsoft and rebooting their machines. Users encountered problems logging on to Skype's VoIP (Voice over Internet Protocol) service, leaving them unable to connect for up to a week. Skype said that the load placed on its system as computers rebooted after receiving a routine set of patches from Microsoft's Windows Update service revealed a previously unknown bug in the Skype software.

More information: <http://www.pcworld.com/article/id,136149-c,webtelephonyconferencing/article.html>

Copyright 2007, SANS Institute (www.sans.org).

Editorial Board: Bill Wyman, Alan Reichert, Barbara Rietveld, Alan Paller. Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>.