



October 2010

Get security advice online at: <http://www.sans.org/newsletters/ouch/updates/>

In This Issue:

- **Dirty Tricks and Larceny**
- **More Information**
- **Securing the Human Blog**
- **Patches and Updates Roundup**

[Editor's Note: (Wyman) This month we present an overview of why and how the Bad Guys do it, what it's called, and what you can do to protect your computer.]

Dirty Tricks and Larceny

Blackhats

Hackers who use their skills for explicitly criminal or other malicious ends, such as writing malware (malicious software) to steal credit card numbers and banking data or by phishing; a.k.a. the Bad Guys.

Phishing

The practice of sending out fake email messages that look as if they come from a trusted person or institution—usually a bank—in order to trick people into handing over confidential information. The emails often direct you to a website that looks like that of the real financial institution. But it is a fake and has been rigged to collect your personal information, such as passwords, credit card numbers and bank account numbers, and transmit them to the Bad Guys.

Man-in-the-middle

An attack in which a criminal hacker intercepts information sent between your computer and the website of your financial institution and then uses that information to impersonate you in cyberspace. The hacker is able to defeat even very sophisticated security measures and gain access to your account.

Botnet

Botnets consist of large numbers of hijacked computers that are under the remote control of a criminal or a criminal organization. The hijacked computers—a.k.a. “zombies” or “bots” (short for “robots”)—are recruited using viruses spread by email or drive-by downloads. Worms are used to find and recruit additional computers. The biggest botnets consist of thousands and even millions of computers, most often unprotected home computers.

Virus

A malicious program that usually requires some action on the part of a user in order to infect a computer; for example, opening an infected attachment or clicking on a link in a rigged email may trigger a virus to infect your computer.

Drive-by Download

A kind of malware that installs itself automatically when you visit a booby-trapped website. Symptoms of a drive-by download include: your homepage has been changed, unwanted toolbars have been added, and unfamiliar bookmarks appear in your browser.

Worm

Self-replicating malware that, for instance, hunts down unprotected computers and recruits them for criminal or other malicious purposes. Unlike a virus, worms do not require any action on your part in order to infect your computer.

Fake Anti-Virus

Fake anti-virus software purports to be a helpful program that can find and remove malware, but in fact it is malware--the very thing that it's supposed to eliminate. After taking over your computer, it pretends to do security scans, tells you it has found malware, and then asks you to pay to have the non-existent malware removed. Whether or not you pay, fake anti-virus is likely to install more malware.

Whitehats

Hackers who use their skills for positive ends, and often for thwarting blackhats. Many whitehats are security professionals who spend their time identifying and fixing vulnerabilities in software that blackhats seek to exploit for criminal or other malicious purposes.

Security suite

A set of software applications designed to protect your computer that consists of anti-virus, anti-malware and a personal firewall.

Anti-virus and anti-malware.

Helpful software applications that scan your computer for certain patterns of infection. The patterns they scan for are the signatures, or definitions, of known forms of malware. Since Bad Guys are creating new forms of malware continuously, it is important that you keep your anti-virus and anti-malware definitions updated. See the "Patches and Updates" section below.

Personal firewall

Software that monitors incoming and outgoing traffic on your computer and checks for suspicious patterns indicating the presence of malware or other malicious activity. A personal firewall alerts you to these threats and attempts to block them. Like anti-virus and anti-malware software, personal firewalls require frequent updates to provide effective protection.

Updates

Security software relies on frequent updates in order to be able to counteract previously undetected forms of malware. Consequently, your computer may suffer a "window of vulnerability" between the time a new form of malware is identified and the time when your security software can block it or remove the infection. Set your security software to update automatically.

Patches

Operating systems, like Windows and OS X, and software applications, such as Internet Explorer and Firefox, may be found to contain security flaws or holes that make your computer vulnerable to attack. Their makers release patches to plug the holes. The fastest and surest way to get these installed quickly is to use auto-updating via the Internet. Some software applications require manual updating. See the “Patches and Updates” section below.

Black Tuesday a.k.a. Patch Tuesday

On the second Tuesday of each month Microsoft releases security patches for Windows, Internet Explorer, Office and its other software products. You can have these installed automatically using Microsoft Update. See the “Patches and Updates” section below.

Auto-updating

A software tool built into Windows (“Microsoft Update”) and OS X (“Auto Update”) and many other applications which can download and install important security updates and patches for software installed on your computer automatically. See the “Patches and Updates” section below.

More Information:

<http://www.binaryfarm.com/jargon.html>

<http://besafe.more.net/sam/resources/jargon.pdf>

http://ittraining.iu.edu/workshops/win_security/terminology.html

Heads Up!

IS YOUR ORGANIZATION CONSIDERING STARTING AN AWARENESS PROGRAM or looking for ways to improve an existing one? SANS “Securing the Human” blog provides the latest updates, resources, and best practices to help you plan, implement, and maintain effective security awareness programs. <http://www.securingthehuman.org/blog>

Patches and Updates Roundup

Operating Systems/Applications

Windows & PC Office: <http://update.microsoft.com> &
<http://www.microsoft.com/security/updates/bulletins/201009.aspx>

Mac Office:

<http://www.microsoft.com/mac/help.mspx?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033>

OS X: <http://support.apple.com/kb/HT1338>

iPad: http://www.ehow.com/how_6256127_update-restore-apple-ipad.html

iPhone, iPod & iPod touch: <http://support.apple.com/kb/HT1414>

iPod: <http://support.apple.com/kb/HT1483>

Windows Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows>

OS X Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh>

Flash Player: <http://get.adobe.com/flashplayer/>

Firefox: <http://www.mozilla.com/en-US/firefox/update/>

Safari: http://www.ehow.com/how_2033324_update-safari.html

Opera: <http://www.opera.com/>

Chrome: <http://www.google.com/support/chrome/bin/answer.py?hl=en&answer=95414>

Java: <http://www.java.com/en/download/manual.jsp>

Windows iTunes: http://www.ehow.com/how_2016273_update-itunes-pc.html

OSX iTunes: http://www.ehow.com/how_2016270_update-itunesmac.html

Security Suites

Symantec: <http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713>

Norton:

http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95

McAfee: http://www.mcafee.com/apps/downloads/security_updates/dat.asp

Kaspersky: <http://www.kaspersky.com/avupdates>

AVG: <http://free.avg.com/us-en/download-update>

Panda: <http://www.pandasecurity.com/homeusers/downloads/clients/>

PC Tools: <http://www.downloadatoz.com/pc-tools-internet-security/smart-update.html>

BitDefender: <http://www.bitdefender.com/site/view/Desktop-Products-Updates.html>

Avast: <http://www.avast.com/download-update>

Webroot: <http://support.webroot.com>

Trend Micro: <http://esupport.trendmicro.com/Pages/How-to-update-Trend-Micro-Internet-Security-Pro-2010.aspx>

Microsoft Security Essentials:
<http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx>

Copyright 2010, SANS Institute (<http://www.sans.org>)

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Alicia Beard, Alan Paller.

OUCH! Security Information Service: <http://www.sans.org/newsletters/ouch/updates/>

Email: OUCH@sans.org

Download the formatted version of the OUCH!: <https://www.sans.org/newsletters/ouch>

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. We request that redistributions include attribution for the source of the material.