

In This Issue

1. Scams and Hoaxes - 2. Malware - 3. Microsoft and Apple Security Updates - 4. Security Screw-up of the Month - 5. Security Newsbytes

A formatted version of the OUCH newsletter can be found at <https://www.sans.org/newsletters/ouch>. You can subscribe to OUCH on the same site.

1. Scams and Hoaxes

--Skype Phishing Scam

Bait: An email, purporting to be from Skype, claims that the customer's account has been suspended until he or she agrees to a changed Terms of Use statement. The message instructs users to click on an embedded link and logon to the Skype website in order to agree to the new terms so that the account can be re-activated. However, the message is not from Skype and the link actually leads to a bogus web page that resembles the real website. If a victim logs on to the bogus page, the username and password, and any other personal information submitted, can be collected by the scammers who will then have access to the victim's Skype account.

More information: <http://www.hoax-slayer.com/skype-phishing-scam.shtml>

--Abnormal Activity From Your IP Alert Email

Bait: An email, claiming that a scanning robot has detected "abnormal activity" from the (IP) Internet Protocol address used by the recipient's computer and suggesting that the activity is related to a recent email worm "epidemic." The message instructs recipients to click on an embedded link to install a patch that will supposedly remove worm files. It warns that the recipient's account may be blocked if the patch is not installed. However, clicking on the link will lead to a malicious website that will download and install a Trojan to the user's computer. Once installed, the Trojan may try to connect to the Internet and download other malware components. The link to the supposed patch is disguised as a weblink so that it forms a clickable part of the message.

More information: <http://www.hoax-slayer.com/robot-abnormal-activity.shtml>

--Fake Online iPhone Store

Bait: Aided by a new customized Trojan, scammers, feeding on the excitement surrounding the iPhone, are trying to steal money from unwitting customers looking to get their hands on the new Apple cellphone/PDA. Once your computer is infected, if you attempt to browse to <http://www.apple.com/iphone/>, you will be redirected to a bogus iPhone shopping site. The malware can also produce a phony pop-up offer to buy an iPhone, triggered by going to yahoo.com or google.com. (See also 2. Malware)

More information: <http://sunbeltblog.blogspot.com/2007/06/iphone-madness-this-hot-phone-now-sold.html>

--Email Domain Name Renewal Scam

Bait: An email from a company named Domain Renewal, offering to renew the name of your Internet domain (a name that identifies a computer or group of computers on the Internet, like www.sans.org, or which follows the @ sign in an email address, like webmaster@sans.org.) However, Domain Renewal is not the Registrar and, despite their claims to the contrary, cannot renew your domain on your behalf. In all likelihood, they are just taking your money. Scams preying on domain owners are an old story, with many of them relying on direct paper mail. The Domain Renewals' contact comes by email. Don't assume, just because they seem to know so much about you and your domain, that they have any official status. Information about Internet domains is a matter of public record.

More information:

http://blogs.pcmag.com/securitywatch/2007/07/beware_fake_domain_renewal_not.php

2. Malware

Gpcode-AI (aka Sinowal-FY), a “ransomware” Trojan that encrypts data on compromised machines before demanding \$300 from users to decrypt it. The malware includes backdoor key-logging* features designed to capture confidential information from compromised PC's, and warns the victim: “If you will not contact us . . . , your private information will be shared and you will lost all your data.” This threat is, however, false because the malware lacks any routine to delete encrypted data, as is the claim that private user files might be sent to a malicious user. These tactics are a ruse designed to speed up payment from victims.

More information: * <http://www.kaspersky.com/crimeware>
http://www.theregister.com/2007/07/19/ransomware_trojan/

Phish-BuyPhony, a Trojan which spreads by email, chat sessions, peer-to-peer networks, and newsgroup postings, implants an Internet Explorer Browser Helper Object (BHO), maliciously designed to hijack your browser by masquerading as Apple's iPhone on-line shop. When successful, the victim is brought to a fake site where payment is made to the crooks via Western Union or MoneyGram. (See also 1. Scams and Hoaxes)

More information: http://vil.nai.com/vil/Content/v_142599.htm

3. 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 August 14th. 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.msp>

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.msp>

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

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

4. Security Screw-Up of the Month

-- Data breach exposed 900,000 soldier and government employee health records.

In yet another case of seriously flawed security precautions, the personal health care records of nearly 900,000 troops, family members and other government employees stored on an a Department of Defense contractor's non-secure computer server were exposed to compromise. The contractor, SAIC, said the information included combinations of names, addresses, Social Security numbers, birth dates and/or "limited health information in the form of codes." The information was stored on a single, SAIC-owned, non-secure server in Shalimar, Fla., and was in some cases transmitted over the Internet in unencrypted form. The information was exposed while being processed, the company said. According to an *Army Times* report, SAIC said a forensic analysis by top computer security experts "has not yielded any information that any personal information was actually compromised," but added that "the possibility cannot be ruled out." Although SAIC did not announce the data breach until July 20th, the company acknowledged it had known about it since May 29.

More information: <http://www.networkworld.com/community/node/17717>

5. Security Newsbytes

--Apple Patches iPhone Flaws

Apple has released the first patch for the iPhone. iPhone Software Version 1.0.1 fixes a series of flaws that could allow Bad Guys to take control of any iPhone either through a Wi-Fi connection or by tricking users into going to a website that contains malicious code, and gain access to the wealth of information stored on your iPhone.

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

*<http://www.nytimes.com/2007/07/23/technology/23iphone.html?ex=1186545600&en=3fce8c7c68eb9ef9&ei=5070>

* Note: Access to *The New York Times* on-line requires registration (an NYT username and password). Registration is free.

--VA's Total for Missing IT Equipment Reaches \$19.6 Million

An audit of three medical centers operated by the U.S. Department of Veterans Affairs and of the VA's headquarters found that a total of \$6.4 million worth of IT equipment went missing from those facilities or was misplaced during the federal government's past two fiscal years. About 2,400 IT devices couldn't be accounted for during inventory counts done by officials at the four facilities in fiscal 2005 and 2006, according to a report released Tuesday by the Government Accountability Office. Among the missing items were dozens of computers that could have stored personal data about VA clients, the GAO said in its report. The four-site audit was a follow-up to an earlier one at five other VA facilities. Based on updated information obtained from those facilities earlier this year, they couldn't account for more than 8,600 pieces of IT equipment with a combined original cost of \$13.2 million, the GAO said. Across the nine audited facilities, the total value of the missing equipment was \$19.6 million.

More information:

http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=13&articleId=9027940&intsrc=hm_topic

--Loose Lips Sink Ships, and Flying Fingers Scuttle Computers

Malicious code attacks over instant messaging networks are up almost 80 percent over last year, according to a new study from vendor Akonix. The company, which develops IM hygiene and compliance appliances and services, said it uncovered 20 malicious code attacks over IM in July. The total number of threats for 2007 so far is 226, the company said--a 78 percent increase over the last year. The company also said attacks on peer-to-peer networks, such as Kazaa and eDonkey, in July 2007 were of 32 varieties—an increase of 357 percent over July 2006. The report comes on the heels of revelations by peer-to-peer network monitoring vendor Tiversa that contractors and U.S. government employees are sharing hundreds of secret documents on peer-to-peer networks--even when doing so requires users to override the default security settings on their peer-to-peer network software.

More information:

<http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9028279>

--Password vulnerability in Firefox 2.0.0.5

Only days after Mozilla released an update for Firefox, designed to combat security issues that arise when Internet Explorer is installed on the same computer, another flaw has surfaced. The newly-discovered--but likely not new--flaw could potentially result in having a password stolen. The latest version of Firefox, 2.0.0.5, contains a password management vulnerability that can allow malicious websites to steal user passwords. If you have JavaScript enabled and allow Firefox to remember your passwords, you are at risk from this flaw. In addition to Firefox, it seems that Safari is vulnerable in the same way.

More information: <http://www.pro-networks.org/forum/story96102.html>

--Pump-and-dump Scammers Turn to Excel Spreadsheets

First, it was the onslaught of spam with pdf attachments. Now the pump-and-dump stock scammers have begun using Microsoft Excel spreadsheet attachments, with names like "invoice20202.xls" and "stock information-3572.xls," to slip past anti-spam filters. Attachments contain an unsolicited message, which, as in all classic pump-and-dump scams, touts shares of one or more lightly-traded companies as hot and ready to climb. The fraudsters, however, have already bought shares and only spam their unwilling potential investors to get others to buy in. If enough do, the price goes up, and the scammers sell their holdings. The duped recipients of the spam are left holding the bag when the price later plunges.

More information: <http://www.networkworld.com/news/2007/072307-pump-and-dump-scammers-turn-to.html>

Copyright 2006, SANS Institute (<http://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>.