Volume 3, Number 12 **December 2006**

SANS OUCH! SANS Institute Security Newsletter for Computer Users

In This Issue

1. What to Watch Out for This Month – 2. More Phishing – 3. Hoaxes – 4. Malware – 5. Have You Updated this Month? – 6. Security Newsbytes

1. What to Watch Out for This Month

As of this writing, there were over 180 reported phishing alerts during the month of November, of which 122 involved banks and credit unions. Don't take the bait! Before you respond to any email requests for personal information, call your bank, credit union or other institution. In general, reputable financial institutions do not request personal information via email. Listed below are banks and credit unions whose account holders were the object of phishing scams last month. Information for this report was gathered from various sites including:
http://www.trendmicro.com/en/security/phishing/overview.htm &
http://www.millersmiles.co.uk

AmSouth Bank
Bangkok Bank
Bank of America
Bank of Cascades
Bank of Scotland
Barclays Bank
Bendigo Bank
BOA Military Bank
Brattleboro S&L
Chase
Chemical Bank
Citibank
Commerce Bank
Community America CU
Co-operative Bank
Credit Union of Texas
Egg Bank
Empire FCU
Fairwinds CU
Fibre FCU
Fifth Third Bank
Flagstar Bank
Franklin Mint FCU
Greater Atlantic Bank
Halifax Bank
HFC Bank
Honolulu City & County Employees FCU
HSBC Bank
ICICI Bank
Interchange bank
Iowa Corporate Central Credit
LaSalle Bank
Lloyds TSB Bank
Marine CU
Michigan Schools & Government CU
Mid America Bank
NatWest Bank
Numerica CU
Pearl Harbor FCU
PNC Bank
Santa Barbara Bank & Trust
Sears National Bank
Service CU
Talbot Bank
Teachers CU
USF FCU
Wachovia Bank
Warren FCU
Wells Fargo
West Bend Savings Bank

2. More Phishing

Subject: Social Security Administration
Bait: A phony email attempting to convince recipients to reveal their name, address, date of birth, Social Security number, credit card information, and bank account numbers or risk having their Social Security "account" suspended indefinitely. Recipients are then directed to click on an embedded link that takes them to a website designed to look like that of the Social Security Administration.
More information:
http://money.cnn.com/2006/11/07/pf/Social_Security_email/index.htm?section=money_latest

Subject: Sears – "Security Notification about Your Sears Card Account"
Bait: A phony email, allegedly sent from alertingservice@searscard.com stating that due to several failed logon attempts, your Sears card Account features have been restricted, and demanding that you click on the embedded link and sign on to your online account. The link leads to a phishing site in Korea.
Security Tip: Sears never sends their users emails requesting personal details in this way.
Sample: http://www.millersmiles.co.uk/report/3828

Subject: PayPal – "You have added samantha_millercarter@charter.net as a new email address to your PayPal account"
Bait: A phony email, allegedly sent from service@paypal.com, stating that you have added an email address to your PayPal account, and requesting that you click on a link if you don't agree with the addition. The link takes you to a fake, phishing website.
Security Tips: PayPal never sends emails requesting personal information in this way. The spoofed website looks nothing like an actual PayPal webpage.
Sample: http://www.millersmiles.co.uk/report/3869

Subject: eBay – "Question from t-rexcomputing"
Bait: A phony email, allegedly sent from eBay Member t-rexcomputing < support@eBay.com > letting you know that "t-rexcomputing" is interested in buying your XPS 2010 computer. The embedded "Respond Now" button is nothing more than a diversionary graphic device, which leads to a fake web site.
Security Tip: eBay never sends their users emails requesting personal details in this way. The spoofed website looks nothing like an actual eBay webpage.
Sample: http://www.millersmiles.co.uk/report/3857

Subject: PhishingSpace on MySpace website
Bait: A spoofed login form, apparently inserted by phishers, on the MySpace main website. This bit of fakery is difficult to detect because it has been smuggled onto the actual MySpace website. The modified login form is designed to submit the victim's username and password to a remote server hosted in France.
More information:
http://news.netcraft.com/archives/2006/10/27/myspace_accounts_compromised_by_phishers.html

3. Hoaxes

Fake Mail Server Report Message Carries W32.Stration Worm
An email is circulating that attempts to trick the recipient into opening an attachment by claiming that "e-mails containing worm copies" have been sent from his or her computer. The message, labeled "Mail server report," instructs the recipient to install updates to remove the worm infection. The update, supposedly included in an attachment that comes with the email, actually carries a variant of the W32.Stration worm.
More information: http://www.hoax-slayer.com/fake-update-worm.shtml

Editor's Note: (Wyman): The W32.Stration worm has been with us since September, and every self-respecting anti-virus product has already been updated to detect it. What's new this month is the ruse of using a bogus, official-looking report to trick users into opening an attachment and exposing their systems to the worm.

4. Malware

W32.Spybot.ACYR – Worm
University security experts warned administrators on November 27th that a bot program has started to spread by exploiting five previously patched Microsoft vulnerabilities and a 6-month-old flaw in Symantec's anti-virus software. Dubbed W32.Spybot.ACYR by Symantec, the bot has compromised a relatively small number of systems at various universities, but very quickly compromised about 30 systems at the University of Arkansas and another 150 systems at the University of New South Wales in Australia
More information:
http://www.theregister.co.uk/2006/11/29/bot_antivirus_windows_flaws/ &
http://www.symantec.com/enterprise/security_response/weblog/2006/11/spybot_attempts_to_exploit_old.html

Mac OSX Spyware – iAdware
The first spyware program for Mac OS X has been detected. The proof-of-concept code could potentially be installed without users' knowledge. The program, known as iAdware, installs itself as a System Library. It does not exploit a flaw, but takes advantage of a feature in Mac OS X to launch Safari each time an application is opened.
More information: http://www.eweek.com/print_article2/0,1217,a=194912,00.asp
http://www.theregister.co.uk/2006/11/24/mac_os_x_adware/print.html

5. Have You Updated This Month?

Microsoft and Apple provide free security updates for the Windows and Mac OS X operating systems.
Windows:
http://www.microsoft.com/athome/security/update/bulletins/automaticupdates.mspx
OS X: http://docs.info.apple.com/article.html?artnum=106704
Check manually, too, once every two weeks to make sure all updates have been installed.

6. Security Newsbytes

Remembering the VA Laptop SNAFU
One of the biggest data breaches yet may have cost the General Counsel of the Department of Veterans Affairs his job. In May a laptop and external hard drive containing 26.5 million personal records was stolen from the home of a VA data analyst. According to his congressional critics, two old memos by McClain prevented the VA's chief information officer from keeping a closer rein on the department's equipment. In July the VA announced that McClain was stepping down to "return to the private sector."
More information: http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1164189920380

Feet to the Fire at Ohio University
An Ohio University official has upheld the firing of two school administrators over computer breaches discovered on campus in April. Tom Reid, former director of communication network services, and Todd Acheson, former UNIX systems manager, were fired in July, two months after the university discovered breaches that exposed 173,000 files containing Social Security numbers, names, medical records and home addresses. University Provost Kathy Krendl said in letters sent to Reid and Acheson on November 28th that their dismissal "does not indicate that you intended to put our data at

risk, but in fact, that was the result of failing to take the necessary proactive steps to protect confidential information."
More information:
http://news.enquirer.com/apps/pbcs.dll/article?AID=/20061117/NEWS0102/611170370/1058/NEWS01

VoIP - Open Season for Crackers
Sensitive data sent using Voice over Internet Protocol (VoIP), or routing conversations over the Internet, is vulnerable to attack because call centers fail to secure their networks robustly enough. Customers' private information could be stolen using the wiretapping method. The security company Scanit concluded that as many as 7 out of 10 calls are open to attack after auditing data transfer at various busy call centers and service providers. Many consumers are familiar with the VoIP technology called Skype.
More information: http://www.theregister.co.uk/2006/11/29/voip_hack_calls/

Still Feeling "Safe" on Your Mac?
Apple has issued software updates to fix 31 security holes in various versions of its OSX operating system. The Mac maker sent the free updates to its users via its online software update service on November 29th. Consumers can also download the patches directly from Apple's Web site. The patches address critical vulnerabilities, including a Wi-Fi flaw affecting eMac, iBook, iMac, PowerBook G3, PowerBook G4 and Power Mac G4 systems. So far Apple has released patches for 185 vulnerabilities in 2006.
More information: http://www.technewsworld.com/story/54479.html
Security tip: If you missed it, a link to instructions for updating your Mac is listed under item 5 above. Don't wait!

Another Worm in the Apple?
The US Computer Emergency Readiness Team (US Cert) issued an alert after security researchers produced code that could exploit the DMG (Disk Image) bug. The flaw involves the way OSX handles disk images and could be used to crash or take over a vulnerable machine. So far the DMG bug, which came to light during a month-long project run by the Info-Pull research group that aimed to find one "kernel" bug a day, has only been shown to work under laboratory conditions.
More information: http://news.bbc.co.uk/1/hi/technology/6187302.stm

Reverse Cross-Site Request Flaw Tarnishes Firefox 2.0 and IE7 Security
The latest versions of both Firefox and Internet Explorer are vulnerable to an unpatched flaw that allows hackers to harvest users' login credentials through automated phishing attacks. This flaw could affect anyone visiting a weblog or forum website that allows user-contributed HTML codes to be added.
More information: http://www.info-svc.com/news/11-21-2006/

Zombie Armies Batter Windows
Malicious remote control software continues to be one of the biggest threats to Windows PCs. More than 43,000 new variants of bot-making software were found in the first half of 2006, which makes them the most active category of malicious software, according to a Microsoft Security Intelligence Report. Of the 4 million Windows PC's found to be infected with some kind of malicious software in the first half of 2006, about 2 million were running malicious remote control software.

More information: http://software.silicon.com/malware/0,3800003100,39163520,00.htm

Wikipedia Hijacked to Spread Malware

Hackers took advantage of the popular Wikipedia encyclopedia in an attempt to spread malicious code. An article in the German edition of Wikipedia, de.wikipedia.org, was created by hackers and claimed to include a link to a fix for a supposedly new version of the Blaster worm. However, the fix was actually a piece of malicious code designed to infect visitors' PCs. Hackers then spammed out an email to German computer users, claiming to come from Wikipedia, and directing them to more information about the "new worm."

More information: http://www.sophos.com/pressoffice/news/articles/2006/11/wikipedia-malware.html

****