Volume 3, Number 9 September 2006

SANS OUCH!

SANS Institute Security Newsletter
for Computer Users

In This Issue

What to Watch Out for This Month -- Microsoft August Security Updates –Outlook Junk Email Filter – Security Screw-Up of the Month –Security Newsbytes – Arrests and Convictions

What to Watch Out for This Month

There were more than 170 reported phishing alerts during the month of August, of which 117 involved the following 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. Reputable financial institutions do not make a practice of requesting personal information via email. Listed below are banks and credit unions whose account holders were the most frequent targets 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

Bank of America
Bank of Castile
Bank of Ireland
Barclays Bank
Central Florida Educators FCU
Central Minnesota FCU
Chase Bank
Citibank
Commonwealth Bank of Australia
Corporate America
Family CU
Egg Bank
FirstBank
First National Bank of Greencastle
Flagstar Bank
Golden 1 CU
Halifax Bank
HSBC Bank
Key Bank
Lloyds Bank
Machias Savings Bank
MBNA Bank
Nationwide
Paragon FCU
People's Trust FCU
Royal Bank of Scotland
Santa Barbara Bank & Trust
St. George Bank
Suntrust Bank
Teachers FCU
Texas DPS FCU
Town North Bank
Wachovia Bank
Warren FCU

1. Phishing Scams

Subject: VISA – Verified By Visa Activation
Bait: An email asking you to confirm/update/verify your account data at VISA by clicking on the embedded link.
Security Tip: VISA never sends their users emails requesting information in this way.
Sample: http://www.millersmiles.co.uk/report/3279

Subject: Amazon – Amazon Account Update
Bait: An email asks you to confirm/update/verify your account data at Amazon by clicking on the embedded link.
Security Tip: Amazon never sends their users emails requesting personal information in this way.
Sample: http://www.millersmiles.co.uk/report/3300

Subject: e-Gold – Suspicious attempts to log on to your account.

Bait: Similar to the "Citibank Citibusiness" phishing scam (see August 2006 OUCH). An email indicating that there has been suspicious activity on your account, including the number of "suspicious" login attempts and the IP address of the alleged suspect.
Security Tip: e-Gold never sends their users emails requesting personal information in this way.
Sample: http://www.millersmiles.co.uk/report/3150
Another variation: http://www.millersmiles.co.uk/report/3171

2. Hoaxes and Scams

Pepsi Company Lottery Promotion – scam: An email claiming that the recipient has won money in an international lottery.
More Information: http://www.hoax-slayer.com/pepsi-lottery-scam.html

Package Deposited in Your Name – scam: An email claiming that a package deposited in your name contains a large sum of money in cash and is being held for you by a group of diplomats.
More Information: http://www.hoax-slayer.com/package-deposited-scam.html

Space Shuttle Columbia Explosion Photos – hoax: Email claiming that attached photographs taken by an Israeli satellite show the explosion of the Columbia Space Shuttle.
More Information: http://www.hoax-slayer.com/columbia-explosion-photos.html

3. Virus Alerts

Mocbot – a worm that exploits a recent Windows hole and has led to a reported 23% growth in the number of hijacked or "zombie" PCs, according to messaging security company CipherTrust. Also known as Cuebot and Graweg, Mocbot exploits a Windows security flaw for which Microsoft issued a patch (MS06-040) on August 8th.
More information: http://news.zdnet.com/2100-1009_22-6108409.html

W32.bounds - This is proof-of-concept code that targets computer processors made by AMD Corporation. This worm is unusual because it targets a specific piece of hardware (the CPU chip) rather than software such as an operating system (i.e. Windows) or an application (i.e. Internet Explorer). Because it involves "proof-of-concept" code, this worm is considered a low-level threat for now, but this method may become a common way for hackers to attack a computer system.
More information: http://www.pcauthority.com.au/news.aspx?CIaNID=36347

Microsoft August Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of every month. August was busier for Microsoft than last month: there were nine "critical" updates and three "important" updates. One patch, MS06-042, was subsequently re-released on August 24th. See "Patch for the patch" in the Security Newsbytes below. The next set of Microsoft Security updates is scheduled for release on September 12th
More information: http://www.microsoft.com/technet/security/bulletin/ms06-aug.mspx

Security Tips: Be sure your operating system, Windows and Mac alike, is set to receive updates automatically and periodically check your patches manually. New vulnerabilities are being detected and exploited quickly after updates are released, and sometimes patches for newly discovered vulnerabilities can be a month or more away.

Outlook Junk Email Filter

While Outlook Junk Email Filter (OJE) does a great job of keeping spam out of your Inbox, it is also a powerful anti-phishing tool. OJE checks suspicious incoming messages for embedded links, strips away graphics designed to make the message appear genuine, and "dismembers" any embedded Web links, revealing their true destination in plain text. This reduces the chances that you might be tricked into clicking on an embedded link and lured into revealing personal information on a bogus Web site. Patches and updates are released monthly through Microsoft Update to help keep OJE attuned to the latest phishing scams and other emerging spam schemes and tricks. OJE also works with Outlook Web Access.
More information: http://office.microsoft.com/en-au/assistance/HP052429671033.aspx

Security Screw-Up of the Month

High cost of education. The U.S. Department of Education has disabled the online payment feature for its Federal Student Aid site following a security breach that could affect up to 21,000 borrowers. Federal Student Aid recipients who accessed one of six Web pages on the Department of Education site during a three-day period may have had their personal information exposed to others.
More information: http://news.zdnet.com/2100-1009_22-6109405.html

Security Newsbytes

***What* was in that spreadsheet?** Verizon Wireless has accidentally distributed a file to about 1,800 people outside the company with limited details on 5,210 Verizon Wireless customers, a screw-up that may get another rash of identity thefts off to a running start in a big way. The Microsoft Excel spreadsheet file was reported to include the names, email addresses, cellphone numbers and cellphone models of customers.
More information: http://news.zdnet.com/2100-1009_22-6109883.html

You wrote *what* on a yellow sticky note? A health care group in Michigan disclosed last week that a laptop PC containing personal information on about 28,000 home-care patients had been stolen on August 5th in a car theft. The car theft caused concern among hospital officials because an employee's ID access code and password were written on a piece of paper that was taped to the inside of the stolen laptop. The employee, a nurse, has since been fired.
More information:
http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=12&articleId=9002765

Patch for a patch. There's more trouble with Microsoft's latest Internet Explorer 6 patch. It introduces a serious new security flaw on some Windows systems**.** The vulnerability

could allow miscreants to hijack a Windows PC running IE 6 with Service Pack 1 and the MS06-042 update installed. MS06-042 has since been re-released.
More information: http://news.zdnet.com/2100-1009_22-6108490.html &
http://news.zdnet.com/2100-1009_22-6107191.html

Arrests & Convictions

Email bomber confesses. A 19-year-old U.K. man pleaded guilty to breaking the Computer Misuse Act by sending an "email bomb" to his former employer, which caused the company's email server to collapse. David Lennon of Bedworth, Warwickshire was sentenced to a two-month curfew and must wear an electronic tag.
More information: http://www.theregister.co.uk/2006/08/23/email_bomber_guilty/

Vacation scammers charged. Two people have been charged with offenses connected to scam vacation Web sites which could have conned as many as 3,000 people. The scammers took money for vacations that didn't exist and then attempted to disappear with the cash.
More information: http://www.theregister.co.uk/2006/08/21/fake_holiday_websites/

MySpace hackers arrested. The operators of a Web site that allowed MySpace.com users to track their visitors have been charged with trying to extort US$150,000 from the popular social networking site. Shaun Harrison, 18, and Saverio Mondelli, 19, both of Suffolk County, New York, were arrested by undercover agents posing as MySpace employees in Los Angeles.
More information: http://www.pcwelt.de/news/englishnews/Security/138744/

****