Volume 3, Number 4 April 2006

SANS OUCH! SANS Institute Security Newsletter for Computer Users

In This Issue

Late-Breaking News --What to Watch Out for This Month -- Microsoft March Security Updates --Security Newsbytes -- Arrests and Convictions

Late-Breaking News

The editors of the OUCH newsletter suggest you check the security of your Windows computer using Microsoft Baseline Security Analyzer 2.0 (MBSA). MBSA, a free tool, compares the state of your computer to Microsoft's current security standards and offers specific information about remediation and guidance. Please note that some information provided by MBSA may be technically complex. MBSA works with the following operating systems: Windows 2000 SP3 and XP, Office XP and 2003, and also evaluates the security of Exchange 2000 and 2003, and SQL Server 2000 SP4 and 2005.
More information: http://www.microsoft.com/technet/security/tools/mbsahome.mspx.

What to Watch Out for This Month

There were 144 reported Phishing alerts during the month of March, of which 20 involved banks and credit unions. Don't take the bait! Before you respond to any e-mail requests for personal information, call the bank, credit union or other institution. 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.

Bank of America
BancorpSouth Bank
Bank of Hawaii
Bank of Southern Utah
Barclays Bank
Chase Bank
CitiBank
Federal Credit Union
Florida Credit Union
JP Morgan Bank
JPMorgan Chase & Co
Halifax Bank
HSBC Bank
St. Francis Bank
San Diego County Credit Union
TD Canada Trust
WAMU Bank
Wells Fargo
Zions Bank

1. Phishing Scams
Subject: **St. Francis Bank – Internet Banking**
Bait: The verification Web page prompts the user for information such as a full name, email address, ATM/debit card number, CVV2 and ATM PIN code. You'll notice that the site does **not** have a security lock displayed in your browser. This indicates the site is **not** secure, and its absence is a telltale sign that the site may be bogus.
Sample: http://www.trendmicro.com/en/security/phishing/overview/phish060310a.htm

Subject: **Florida Credit Union – Verify your Data**
Bait: The verification Web page prompts the user for information such as a full name, email address, zip code, credit card number, card expiration date, CVV2, and ATM PIN code. You'll notice that the site does **not** have a security lock displayed in your browser.

This indicates the site is **not** secure, and its absence is a telltale sign that the site may be bogus.
Sample: http://www.trendmicro.com/en/security/phishing/overview/phish060305a.htm

Subject: Citibank – **Reactivate Your Account**
Bait: The email threatens that you may be denied access to your account unless you verify your personal information. When you visit the site, it gathers your personal account information such as registration number and password by means of a spoofed Web page.
Sample: http://www.trendmicro.com/en/security/phishing/overview/phish060316a.htm

Subject: PayPal – **Critical Information Regarding your Account**
Bait: Email asks you to confirm/update/verify your account data at PayPal by visiting the embedded link. You will be taken to a spoofed website where your personal information will be captured for use by the phishers. Keep in mind that PayPal never sends their users emails requesting personal details in this manner.
Sample: http://www.millersmiles.co.uk/report/2338

2. Hoaxes and Scams

Olympic Torch Invitation Virus Hoax. A "warning" message claims that an email with an attached file named "Invitation" contains a virus that will infect your computer with an "Olympic Torch, which 'burns' the whole hard disc C of your computer." But there's no smoke--much less fire--in this tale.
More information: http://www.hoax-slayer.com/olympic-torch-virus-hoax.html

Formosan termites in *my* garden? A forwarded email warns recipients that cheap mulch currently being distributed and sold across the United States originated from debris left by the New Orleans hurricanes and may contain Formosan termites. Don't let it bug you.
More Information: http://www.hoax-slayer.com/formosan-termites-mulch.html

3. Virus Alerts

WORM_CXOVER.A: A proof-of-concept cross-platform worm that affects desktop computers and mobile devices running the .NET Framework software commonly installed on computers running Windows XP, Windows Server 2003 as well as mobile devices running Windows CE or Mobile Edition. More information: http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FCXOVER%2EA

Trojan.Cryzip.A: This is a Trojan horse that creates password-protected ZIP files on the compromised computer and issues a ransom demand for the affected files.

More information: http://www.symantec.com/avcenter/venc/data/trojan.cryzip.html

Microsoft March Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of each month and sends a bulletin announcing the update. There was one "critical" update released in March: MS06-012. This patches vulnerabilities in Microsoft Office for

several operating systems. There was also one “important” update released as well: MS06-011. This patch addresses the privilege elevation vulnerability that could allow a user with valid logon credentials to take complete control of the system.
More information: http://www.microsoft.com/technet/security/bulletin/ms06-mar.mspx

The next set of Microsoft Security updates is scheduled to be released on April 11th.

Security Newsbytes

Apple has released another patch for Macintosh OS X, the third in the last month. The patch is believed to address problems with an earlier patch which itself was issued in part to address problems with a previous security update. Version 1.1 of the 2006-002 patch was released on March 17th; the original version was released on March 13th. **The SANS Internet Storm center urges users to apply the patch immediately.**
More information: http://isc.sans.org/diary.php?storyid=1196 &
http://www.techworld.com/security/news/index.cfm?NewsID=5590

Adobe has issued fixes for flaws in Flash Player version 8.0.22 and earlier, Breeze Meeting version 5.1 and earlier, and Shockwave player version 10.1.0.11 and earlier. Adobe encourages users to upgrade to Flash version 8.0.24.0. The vulnerabilities are serious enough to warrant a warning from Microsoft, which distributes Flash software with Windows.
More information: http://www.macromedia.com/devnet/security/security_zone/apsb06-03.html

Citibank acknowledged last week that attackers had infiltrated its ATM network in Canada, Russia and the United Kingdom, and stolen a block of PIN’s (personal identification numbers). Sophisticated hackers use stolen PIN’s to create counterfeit bankcards and steal money.
More information:
http://www.silicon.com/financialservices/0,3800010322,39157105,00.htm

Phishers have begun using a new technique to ensure that more victims will be lured to fraudulent Web sites. Because anti-phishing vendors are taking more aggressive steps to close Phishing sites, some Phishing emails now direct recipients to an IP address that hosts a “smart redirector”. The redirector checks to see which bogus Web sites are still live before deciding where to send the intended victim. Smart redirector attacks have been detected by two banks.
More information:
http://www.theregister.co.uk/2006/03/08/smart_redirect_phish_attack/print.html

Scam messages are circulating that tell the recipient they are due a tax refund from the IRS and then direct the reader to a Web site that appears to be a genuine IRS site. The bogus sites contain forms or interactive Web pages similar to IRS forms or Web pages, but they have been modified to request detailed personal and financial information. The Internal Revenue Service has set up an e-mail address for taxpayers to forward suspicious e-mail messages that claim to come from the IRS. The address is phishing@irs.gov.
More information: http://www.fcw.com/article92749-03-27-06-Web
and http://www.fcw.com/article92433-02-24-06-Web

Arrests & Convictions

Microsoft is launching legal action against 100 Phishing gangs based in Europe, the Middle East, and Africa. By the end of March, 53 cases will have begun, said Microsoft. All 100 will be filed by the end of June. Seven of the criminal groups behind fake websites that trick people into handing over confidential information are known to be located in the United Kingdom. The legal cases follow investigative work undertaken by Microsoft, national police forces and Interpol.
More information:
http://www.atomicpark.com/newsletter/articles/art_mar21_europhish.aspx

Ali Shekafroush of Corona, 20, a student at Riverside Community College, California, has been arrested for allegedly trying to steal the personal information of about 30,000 people through phishing spam.
More information:
http://www.spamdailynews.com/publish/printer_College_student_arrested_for_phishing.asp

============================