****
OUCH!
SANS Institute Security Newsletter for Computer Users
Volume 3, Number 2 February 2006
****

In This Issue

What to Watch Out for This Month – Microsoft January Security Updates - Security Newsbytes - Arrests and Convictions -

****

What to Watch Out for This Month

There were 152 reported Phishing alerts this month, of which 29 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. Below are banks and credit unions whose account holders were the object of the most phishing scams last month. Information for this report was gathered from various sites including http://www.millersmiles.co.uk/archives/current & http://www.antiphishing.org.

Credit Union of Texas	HSBC Bank	UK Banks Association
Halifax Bank	Chase Bank	JPMorgan Chase & Co
Bank of America	Armed Forces Bank	MBNA
Barclays	North Fork Bank	Flagstar Bank

1. Phishing Scams

- Subject: UK Banks Association – Protect Your Bank Account
Bait: Fake email asking you to confirm/update/verify your account data by clicking on the embedded link.
Goal: To have you visit the Phishing site and divulge your logon information.
Sample: http://www.millersmiles.co.uk/report/2004

- Subject: Credit Union of Texas – Message from Fraud Department
Bait: Fake e-mail asking you to confirm/update/verify your account by clicking on the embedded link.
Goal: To have you visit the Phishing site and divulge your logon and PIN information
Sample: http://www.millersmiles.co.uk/report/2008

- Subject: PayPal – Account Compromised: Billing Information Moved or Changed
Bait: Fake e-mail asking you to confirm/update/verify your account at PayPal by clicking on the embedded link
Goal: To have you visit the Phishing site and divulge information about your PayPal account.
Sample: http://www.millersmiles.co.uk/report/1996

- Subject: eBay – Question About Item – Respond Now
Bait: Fake e-mail asking you to respond to eBay user by clicking on the embedded link.
Goal: To have you visit the Phishing site and divulge your login information.
Sample: http://www.millersmiles.co.uk/report/1984

2. Hoaxes and Scams
- Use Left Ear for Mobile Phone Hoax: Playing on oft-repeated but as yet unsubstantiated concerns about cell phone radiation damage, a message has been showing up in e-mails, on blogs, and in online forums claiming that cell phone users should always use the left ear for calls because using the right ear will directly affect the brain. It includes a nostalgic endorsement by the "Apollo medical team."
More information: http://www.hoax-slayer.com/use-left-ear-mobile.html

- Lead in Lipstick Alert Hoax: This email claims certain brands of lipstick contain dangerous amounts of lead and can cause cancer. The message includes a list of lipstick brands and instructions for testing lipsticks for lead content.
More information: http://www.hoax-slayer.com/lead-lipstick.html

- Spirit Airlines Flight Giveaway Hoax: Would you believe that Spirit Airlines is giving away free flights based on how many times the message is forwarded to others? Don't!
More information: http://www.hoax-slayer.com/spirit-airlines-hoax.html

3. Virus Alerts
- Symantec has updated its Norton SystemWorks to address a flaw that could be used by attackers to hide malicious code on vulnerable computers. The flaw lies in the Norton Protected Recycle Bin feature that creates a hidden directory on Windows systems and is designed to allow restoration of deleted or modified files. The flaw affects Norton SystemWorks 2005 and 2006 and Norton SystemWorks Premier 2005 and 2006. Meanwhile, Symantec is disputing allegations that this feature constitutes a rootkit.
More information: http://www.techweb.com/wire/175804046

- W32.Sygyp.A@mm is a mass-mailing worm that spreads through file-sharing networks and lowers security settings on the compromised computer. An example of the email that carries the worm is shown below. The email arrives with an attachment called "GoogleEarthSetup.exe."

----------Sample ----------

Subject:
Google Earth - Explore, Search and Discover

Message body:
Want to know more about a specific location? Dive right in -- Google Earth combines satellite imagery, maps and the power of Google Search to put the world's geographic information at your fingertips.

** Fly from space to your neighborhood. Type in an address and zoom right in.*
** Search for schools, parks, restaurants, and hotels. Get driving directions.*
** Tilt and rotate the view to see 3D terrain and buildings.*
** Save and share your searches and favorites. Even add your own annotations.*

----------Sample ----------

- New Trojan Horses Threaten Cell Phones

Three new Trojan Horse programs are hitting certain cell phones and combination cell phone/PDA devices. The Trojan horses--programs that are disguised as legitimate applications--spread via Bluetooth or multimedia messages and can affect phones running the Symbian operating system. The Trojans are Bootton.E, Pbstealer.D, and Sendtool.A. The infection rate so far from the new malware is low, but could escalate rapidly. More at: http://enterprisesecurity.symantec.com/content.cfm?articleid=6369

****

Microsoft January Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of each month and sends a bulletin announcing the update. There were three "critical" updates released in January: MS06-001, MS06-002, and MS06-003. These patch a vulnerability in the Graphics Rendering Engine, one in Embedded Web Fonts, and one in Transport Neutral Encapsulation Format (TNEF) Decoding in Microsoft Outlook and Microsoft Exchange. Windows users should use Windows Update to ensure safety of their computers. More information: http://www.microsoft.com/technet/security/bulletin/ms06-jan.mspx

****

Security Newsbytes

- At the recent Cyber Crime Conference sponsored by the US Department of Defense, intensive courses offered on Mac OS X, Linux and iPods indicate a growing concern with malicious code running on the operating systems and, in particular, the threats posed by iPods and similar devices. As these platforms become more widely used, implanting malicious code in them is emerging as a new kind of threat.
More information: http://www.eweek.com/print_article2/0,1217,a=169104,00.asp

- FBI: Damaging Cyber Attack on US Critical Infrastructure Unlikely. The FBI said that while terrorists may not be capable of damaging the nation's critical infrastructure via the Internet, it is likely that foreign governments are backing cyber attempts to obtain sensitive military and technological data. There is, however, no conclusive proof that such intrusion attempts are state-sponsored.
More information: http://news.zdnet.com/2102-1009_22-5986099.html?tag=printthis

- Apple Releases a Cumulative Update for the Mac OS X Operating System. The update addresses 13 flaws that could be exploited to allow remote code execution as well as cross-site scripting and spoofing. The most serious flaws are the remote code execution vulnerabilities in the software applications CoreFoundation, Curl, and Safari.
More information: http://isc.sans.org/diary.php?storyid=905

- The SANS Internet Storm Center has found that more than 500,000 personal computers have been infected by the 'Grew' worm, which goes by a number of different names including Nyxem. On February 3rd, it will delete Word, Excel and a number of other kinds of other documents. Make sure you tell your Mom and your kids (and anyone else who may call you when they lose data) to update their anti-virus software manually and then run a full manual scan. "Update now or all your files may be lost." A special Storm Center web page on the worm can be found at: http://isc.sans.org/blackworm

****

Arrests & Convictions

- Alleged spammer Daniel Lin was expected to enter a guilty plea in court on January 17, 2006 after he admitted using corporate and government computer networks to send unsolicited commercial email. Lin's deal with prosecutors will send him to jail where he will serve between two years and 57 months. One of four people charged in April 2005 with using compromised computers to send spam, the group allegedly sent spam through proxies with phony return-path addresses in violation of the CAN-SPAM Act.
News report: http://www.theregister.co.uk/2006/01/13/detroit_spam_case/print.html

- Robert Kramer, the owner of an Iowa-based Internet services company, has been awarded a US$11.2 billion judgment against spammer James McCalla. McCalla has also been prohibited from accessing the Internet for three years. Kramer won a US$1 billion judgment against other spammers in December 2004 which, at that time, was the largest judgment against spammers ever recorded.
News report: http://www.wired.com/news/politics/1,69966-0.html

- Sean Galvez of Boston, Massachusetts has been indicted on one count of larceny and 10 counts of unauthorized access to a computer and identity fraud for breaking into more than 40 eBay accounts and accumulating charges totaling US$32,000. The Massachusetts Attorney General's office is still trying to determine how Galvez obtained access to the accounts. Galvez allegedly changed passwords and gathered credit card information. Galvez faces up to five years in state prison if convicted.
News report: http://www.eweek.com/print_article2/0,1217,a=168683,00.asp

- An Australian court has ordered two men to pay AU$2.3 million (US$1.72 million) in damages and legal fees for running a domain registration scam that targeted as many as 50,000 UK website owners.
News report: http://www.theregister.co.uk/2006/01/03/domain_scam/print.html

---

From one of our Readers: Commercial grade of "Rainbow Table" is available now (http://www.rainbowcrack-online.com/?x=home). The objective of "Rainbow Table" is to pre-compute all possible password hash's for a given length on a specific encryption for instant password decryption. While this requires significant resources (time to compute, storage and RAM) to derive and hold the Rainbow Tables, its use is not infeasible. According to the web site, the current password length that could be decrypted is at most 7 characters, with a success rate approaching 100%. This provides a rationale for why it is important to choose upper/lower case letters, as well as numbers and symbols and to make your passwords at least 8 characters long.
