Volume 3, Number 6 **June 2006**

SANS OUCH!

SANS Institute Security Newsletter
for Computer Users

In This Issue

What to Watch Out for This Month -- Microsoft May Security Updates – Security Screw-Up of the Month -- Security Newsbytes -- Arrests and Convictions

What to Watch Out for This Month

There were 132 reported Phishing alerts during the month of which 91 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. 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

Abbey Online Bank
America's Credit Unions
American National Bank of Texas
Bank of America
Bancorp South Bank
Barclays Bank
BB&T
Central Bank
Chase Bank
CitiBank
Commonwealth Bank
First City Credit Union
Flagstar Bank
JPMorgan Chase & Co
Halifax Bank
HSBC Bank
Lloyds TSB Bank
MBNA America Bank
Nationwide Online Banking
NatWest Bank
Ohio Savings Bank
South Trust Bank
St. George Bank
U.S. Bank
UW Credit Union
WAMU Bank

1. Phishing Scams

Subject: AOL - **Last Notice**
Bait: An email asking you to confirm your account, then your billing information, and then provides a link for you to click on if you did not authorize the change. The link directs you to a site that is unsecured. The Web site is fake.
Security Tip: AOL never sends their users emails requesting personal details in this way.
Sample: http://www.millersmiles.co.uk/report/2697

Subject: PayPal – Your payment has been sent
Bait: An email asking you to confirm that you have paid "PLASMATVS $495.85 USD" using PayPal. You'll notice that the site does not have a security lock. This indicates the site is not secure, and its absence is a telltale sign that the site may be bogus.
Security Tip: PayPal never sends their users emails requesting personal details in this way. The REAL URL of the spoof Web site looks nothing like the actual PayPal URL.
Sample: http://www.millersmiles.co.uk/report/2660

Subject: **VISA – Attention! Several VISA Credit Card Bases have been LOST!**
Bait: An email asking you to confirm/update/verify your account data at VISA by visiting the embedded link.
Security Tip: VISA never sends their users emails requesting personal details in this way. The REAL URL of the spoof Web site has been chosen to look very similar to the actual VISA URL. Do not be fooled!
Sample: http://www.millersmiles.co.uk/report/2605

Subject: PayPal – Receipt for Your Payment to AT&T Wireless
Bait: An email asking you to confirm/update/verify your account data at PayPal by visiting the embedded link. When you visit the site, it gathers your personal account information such as Logon ID and password by means of a spoofed Web page.
Security Tip: PayPal never sends their users emails requesting personal details in this way. The REAL URL of the spoof website looks nothing like the actual PayPal URL.
Sample: http://www.millersmiles.co.uk/report/2621

Subject: eBay - Re: Question about payment Item #4634543874 Ford-Mustang
Bait: An email asking you to confirm/update/verify your account data at eBay by visiting the embedded link. You will be taken to a spoofed Web site where your personal information will be captured for use by phishers.
Security Tip: eBay never sends their users email requesting personal details in this manner. The REAL URL of the spoof website has been chosen to look very similar to the actual eBay URL. Do not be fooled!
Sample: http://www.millersmiles.co.uk/report/2646

2. Virus Alerts

Symbos_Skulls.Z: This Symbian malware affects mobile phones running on Series 60 Symbian operating systems. It arrives as a desktop theme installer with the file name *JUGGLERR THEME.SIS*. The malware attempts to overwrite files in the affected phone's flash memory (usually designated as C:\) by dropping corrupted copies of the following files:

C:\ETel.dll
C:\etelmm.dll
C:\etelpckt.dll
C:\etelsat.dl

More Information:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=SYMBOS%5FSKULLS%2EZ

Worm_Hoots.A: Upon execution, this worm drops copies of itself in the root folder using the following file names:

O.RLY
CHECK.EXE
NOT RLY.BAT
YA RLY.BAT

It also drops a copy of itself in the startup folder as *O RLY.EXE*. This worm propagates by dropping copies of itself in several hardcoded network shared folders.

More Information:
http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FHOOTS%2EA&VSect=P

Microsoft May Security Updates

As necessary, Microsoft provides new security updates on the second Tuesday of each month and sends a bulletin announcing the updates. There were two "critical" updates released in May: MS06-019 (Vulnerability in Microsoft Exchange) and MS06-020 (Vulnerabilities in Macromedia Flash Player). All of these security patches address vulnerabilities that could allow a hacker to execute code on your computer by remote control and without your knowledge. There was one "moderately critical" update released as well: MS06-018 (Vulnerability in Microsoft Distributed Transaction Coordinator).
More information:
http://www.microsoft.com/technet/security/bulletin/ms06-may.mspx

The next set of Microsoft Security updates are scheduled for release on June 13th.
Security Tip: Be sure your operating system, Windows and Mac alike, is set to receive updates automatically.

Security Screw-Up of the Month (in stereo)

What was stored on the notebook you took home? According to officials at Mercantile Bankshares Corp. on Friday, May 12th, a laptop computer containing personal information about more than 48,000 customers was stolen from an employee of its subsidiary Mercantile Potomac Bank. Mercantile Potomac Bank serves Fairfax and Loudoun counties in Northern Virginia. The bank said it is notifying customers about the incident and that the theft appears to have been a random event. The stolen computer contains confidential information about some customers, including Social Security numbers and account numbers.

Not to be outdone, VA Officials reported last week that a Veterans Affairs department employee walked out of a facility with a CD in hand and took it home. The CD contained information on 26.5 million Veterans including their names, Social Security numbers, disability ratings and dates of birth. The VA took the news calmly, suggesting blandly that veterans should keep an eye on their credit reports in the unlikely event that the thief stumbles on the idea of trying to steal a couple of thousand (or million) identities.
More Information: http://www.fcw.com/article94608-05-22-06-Web

Editor's note: Tell me this. If the computers are not supposed to be removed from the premises, then why are they using ***laptops?*** And why is such information stored on a CD rather than on a physically and electronically secure server?
More Information:
http://baltimore.bizjournals.com/baltimore/stories/2006/05/08/daily37.html?t=printable

Editor's Note: It's the type of thing that is presumably SO obvious that it doesn't need to be said. **But that's why it happens -- because it is SO obvious that companies aren't focusing on it.**

Security Newsbytes

The SANS Internet Storm Center (ISC) has released evidence showing botnets are being used to defraud advertisers using Google Adword, a pay-per-click advertising system. Advertisers pay Google for each click. Unscrupulous publishers work with the botmasters to generate high volumes of clicks and ultimately revenue. The botmasters get a share of this as well. ISC uncovered evidence of a botnet with 115 bots, each of which was clicking on sites up to 15 times a day, keeping them under the detection system's radar.
More information: http://isc.sans.org/diary.php?storyid=1334

Monday again? In which Microsoft warns about a **New Zero-Day Exploit which targets Microsoft Word.** Anti-virus vendors are advising users to take extra precautions opening e-mail messages with Microsoft Word document attachments.
More Information: http://www.symantec.com/outbreak/word_exploit.html

Arrests & Convictions

Christopher Maxwell of California has pleaded guilty to computer fraud and intentionally damaging a protected computer by launching an attack that attempted to install adware on vulnerable machines. Maxwell used powerful computers at universities in California and Michigan to launch the attack, which occurred in January 2005 and affected US Department of Defense (DoD) computers as well as the computer network of Northwest Hospital and Medical Center in Seattle. Maxwell faces a jail sentence of up to 15 years in August and has agreed to pay US $252,000 in compensation to the hospital and the DoD.
More Information: http://news.com.com/2102-7348_3-6069238.html?tag=st.util.print

Jeanson James Ancheta, a well-known member of the "Botmaster Underground" who pleaded guilty in January to federal charges of conspiracy, fraud and damaging U.S. government computers. He was given the longest sentence to date for spreading computer viruses, federal prosecutors said -- 57 months in prison and three years of supervised release
More information:
http://www.cnn.com/2006/TECH/internet/05/09/botmaster.sentence.reut/

****