****
*
*
OUCH!
SANS Security Newsletter for End Users
Volume 2, Number 12 December 2005
****
*
*

In This Issue
What to Watch Out for This Month - Three Things You Can Do (a really useful section) - Security Newsbytes - Arrests and Convictions - Quiz Time: Phishing, Part 1

For a formatted version of this newsletter go to:
http://www.sans.org/newsletters/ouch/issue/20051213.php

What to Watch Out for This Month

Of the 136 reported phishing alerts this month, 53 were attacks against banks and credit unions. The threat is still widespread. Information for this report was gathered from many sites including http://www.millersmiles.co.uk/archives/current http://www.antiphishing.org.

1. Phishing Scams
Subject: Royal Bank of Canada - Update Information
Bait: Fake email asking you to confirm/update/verify your account data at Royal Bank of Canada 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/1683

Subject: PayPal - Account Update [This is one of three items on PayPal this month.]
Bait: Fake email 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 your PayPal Username and Password.
Sample: http://www.millersmiles.co.uk/report/1678

Subject: eBay - Invoice for Wednesday, November 23, 2005
Bait: Fake email asking you to confirm/update/verify your account at eBay 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/1662

Subject: Colonial Bank - Online Banking
Bait: Fake email asking you to confirm/update/verify your account data at Colonial Bank by clicking on the embedded link.
Goal: To have you visit the phishing site and divulge your login information and personal information.
Sample: http://www.millersmiles.co.uk/report/1664

Subject: Armed Forces Bank - Afbank.com Security Check
Bait: Fake email asking you to confirm/update/verify your Armed Forces Bank account by visiting the embedded link.
Goal: To capture as much account information as possible.
http://www.millersmiles.co.uk/report/941

2. Hoaxes and Scams
#90 Hoax: This email warning claims a scammer can take over your mobile phone if you key in #90. The email message also claims that a phone virus is circulating that can erase the SIM card of the infected mobile.
http://www.hoax-slayer.com/xalan-hoax.html

Australian Terrorist Attack Hoax: A number of emails and text messages warning about impending terrorist attacks are currently circulating in Australia. None of the messages are from a credible source, or backed up by police warnings or mainstream media reports.
http://www.hoax-slayer.com/terror-warning-hoaxes.html

3. Virus Alerts
SDBot variants spreading: Several new variants of the SDBot virus are spreading through Instant Messenger programs, especially AIM (AOL's Instant Messenger). Computers become infected only if users click on the link that accompanies the IM message. Once a computer is infected, it becomes part of a "bot army" that receives instructions from an IRC controller. It spreads by sending copies of itself to people in the AOL Buddy list.

New Sober Variant Spreading Quickly: The FBI and the CIA have posted warnings on their web sites about new variants of the Sober worm that pose as messages from the agencies. The phony email messages state that the government has found that the recipient has been visiting illegal web sites and asks the person to click on an attachment and answer some questions.
http://www.hoax-slayer.com/fbi-virus-emails.html

Phishing Attack Targets PayPal Users: A new phishing attack is now targeting people who use PayPal. You receive an email message that says someone has been trying to access your account from a foreign country.
You are advised to click on a link that purports to be a PayPal Security Tool, but is really a Trojan horse program that changes your computer's DNS (Domain Name Service) settings and then deletes itself. When you try to visit the PayPal web site in the future, you are directed to a fraudulently crafted site where the thieves solicit your personal data including your name, Social Security number, bank account and bank routing numbers.
http://www.vnunet.com/vnunet/news/2145545/phishing-attack-paypal

PayPal Billing Center - Your Account Limited: This one has not made it to the phishing and virus sites. It was submitted by an OUCH reader and is reproduced below in its entirety for your information. It claims to be an email from PayPal Billing Center.

<Start of phishing email>

Dear PayPal user,

We are currently performing regular maintenance of our security measures.
Your account has been randomly selected for this maintenance, and you will now be taken through a series of identity verification pages. Protecting the security of your PayPal account is our primary concern, and we apologize for any inconvenience this may cause.

We recently received a report of unauthorized credit card use associated with this account. As a precaution, we have limited access to your PayPal account in order to protect against future unauthorized transactions. You can check your transaction details in attachment.

Case ID Number: PE-901-449-020

Please understand that this is a security measure intended to help protect you and your account.
Thank you,

PayPal Billing Center

<End of phishing email>

There's a catch. The culprits want you to download a file called, PE-901-449-040.jpg.exe in order to view the "transaction details."
But notice the .exe file name at the end of the .jpg file name.
This is a tip that the file is an executable, and that means it can be dangerous. Testing in a secure environment revealed that the file contained a virus named "Download.Trojan."
If you receive this email, play it safe by deleting it immediately.
Do not open the attachment.

****

Three Things You Can Do to Make Your Computer and Information More Secure

1. Keep your operating system and software applications up to date and patched.

Microsoft now offers "Microsoft Update" which provides many patches for Microsoft Windows and other Microsoft programs, such as Microsoft Office, Visio, Project, Publisher, Microsoft Exchange Server, and Microsoft SQL Server, at one convenient location. This service from Microsoft includes all the updating and patching features of Windows Update and Office Update, plus downloads for other Microsoft products-- -even those still in Beta--as well as updates for software drivers. Go to the Windows Update page, click on the "News" item "Upgrade to Microsoft Update" in the lower right hand corner, and follow the instructions. Remember: Making the patching process automatic will help minimize the risk of your computer being infected or getting hacked.

Windows:
http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=en-us
Mac OSX: http://www.apple.com/support/downloads/ and
http://www.apple.com/macosx/features/security/

More info: http://www.its.monash.edu.au/security/home/patching.html and http://www.softwarepatch.com/

2. Making your own backups
Q: Is there a simple way I can back up my important files?
A: Yes. Purchase a memory stick (a.k.a. thumb drive or flash drive). Prices start at about $30.00 for 128 MB. That's the equivalent of about 75 floppy disks worth of storage space. After closing any running applications, copy your new files or files you have changed to your memory stick at the end of the day, at the end of the week, and when you have finished working on a project. Store your memory stick in a safe place, like a locked desk drawer, or tuck it in your pocket and take it home with you.
Tip: You can buy a memory stick that comes on a lariat or a chain; it's easier to keep track of and it's right there when you need it.
Tip 2: Encrypt data if it is sensitive, these thumb drives are easy to lose.

Q: How about putting backups on floppy disks?
A: A thing of the past. Floppies used to be an inexpensive way to store files, but they were never very reliable, and most files today will be too big to fit on them. It's time to trade in those floppies for a better technology, like a memory stick.
Tip: It's a good idea to back up your files before you have your computer serviced (even if the technicians assure you that they will make a backup or that your files will be safe), and before you install any new software or software upgrades.

More backup tips for Windows users:
http://www.microsoft.com/athome/moredone/backupfiles.mspx
<Note: The "Related Links" on the right side of the page at this url provide actual procedures for users to follow, e.g. how to use the windows backup utility, and how to specifically backup Outlook Express data.

Here is a URL pointing to several backup software packages.
http://www.pcmag.com/category2/0,1738,4798,00.asp

3. Avoid phishing scams and protect your identity.
Beware of fraudulent emails and web sites that masquerade as messages from familiar institutions. By tricking you into disclosing your Social Security Number, PIN number, a password, or an account number, identity thieves can drain your bank account or run up bills on your credit card.

The best ways to avoid becoming a victim are:
* Never disclose personal information in response to an unsolicited email
* Never click on the link in the email
* Always access the web site by manually typing in the Web address in a browser

You can report suspected phishing scams by sending an email to reportphishing@antiphishing.com or spam@uce.gov, or by visiting these Web sites http://www.ifccfbi.gov or http://www.consumer.gov/idtheft.

More info: http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

and http://www.atg.wa.gov/consumer/idprivacy/phishing.shtml

****
Security Newsbytes

Verizon Files Lawsuit Against Florida Company for Allegedly Spamming: Verizon has filed a lawsuit in US District Court in New Jersey asking for an injunction to keep Passport Holidays from sending any further spam messages to Verizon mobile phone customers. Verizon is also seeking financial damages from the Florida-based company. The lawsuit alleges that the messages were sent to sequential mobile phone numbers within certain area codes and were sent at rates of up to 200 a minute. The "From" field in the messages was blank; customers called requesting refunds for receiving the spam messages. Verizon says they had US$150,000 in related expenses. Passport Holidays claims that everyone who received a message had "opted-in" to receive such messages.
http://www.msnbc.msn.com/id/10166148/

Apple Update Patches 13 Flaws: Apple has issued a bundle of security fixes to mend 13 separate security flaws in several versions of its Mac OS X operating system. These include security holes that attackers could use to seize control of vulnerable machines. The vulnerabilities are present in products ranging from Apache Web Services to Safari.
https://enterprisesecurity.symantec.com/content.cfm?articleid=6266&EID=0

FTC Cracks Down on Spyware Site: A U.S. District Court has ordered a Web business that offers free music files, browser upgrades and ring-tones to halt downloads of alleged spyware and adware at the behest of the Federal Trade Commission. According to the FTC instead of free files or patches, the downloads contained spyware.
http://ses.symantec.com/jp/symes1173.cfm?JID=5&PID=182998

****
Arrests and Convictions

Spammer Sentenced to One Year in Prison: Peter Moshou, sometimes known as the "Timeshare Spammer," was sentenced to one year in Federal prison and ordered to pay US$120,000 in restitution for sending millions of spam messages in 2004 and 2005. Mr. Moshou was convicted in June of violating the CAN-SPAM Act. He had been named in the lawsuit, filed by EarthLink.
http://news.com.com/2102-7348_3-5959367.html?tag=st.util.print

"Vindictive" Spammer Receives Six-Year Sentence: British police have sentenced Peter Francis-Macrae to six years in jail. Francis-Macrae sent spam offering to sell .eu domain names even though he had no authority to do so; his efforts earned him GBP 1.6 million (US$2.75 million).
When law enforcement officials began to close in on him, Francis-Macrae started making violent threats against people. Francis-Macrae has so far refused to disclose to police the location of more than GBP 400,000 (US$688,000) in proceeds from his activities.
http://www.sophos.com/pressoffice/news/articles/2005/11/weasel.html

FBI Arrests 20-year-old Suspected Zombie King: US Attorney spokesman Thom Mrozek said this prosecution was unusual because Jeanson James

Ancheta, who lives in the Los Angeles suburb of Downey, was accused of profiting from his attacks by installing adware on a network of innocent, compromised computers. According to prosecutors, among the computers attacked were four located at the Weapons Division of the US Naval Air Warfare Center in China Lake, California, as well as an undisclosed number of systems at the US Department of Defense. Ancheta is said to have made nearly $60,000 from installing adware on the zombie computers. He used the profits allegedly to pay for computer servers to carry out additional attacks and a luxury BMW car.
http://www.sophos.com/pressoffice/news/articles/2005/11/ancheta.html

British eBay phishing mastermind sentenced: David Levi, 29, of Lytham near Blackpool, will serve a three-year jail sentence for fraud after being found guilty of stealing identities and bank account information from more than 160 users of the eBay auction website. Other members of his gang received jail sentences ranging from six months to two years.
http://www.sophos.com/pressoffice/news/articles/2005/11/sa_ebayphish.html

****

Quiz Time: Phishing Part 1
Take the quiz, not the bait! Do you know the basic steps to help protect your computer from spyware, worms, and other harmful programs? Discover how you can help avoid being lured into giving away your personal information. Look for Phishing, Part 2 coming in the January edition of OUCH.
http://www.microsoft.com/athome/security/quiz/pypcbasics1.mspx

==end==

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.1 (Darwin)

iD8DBQFDnvhu+LUG5KFpTkYRAi9IAJ4nB+r7YE7AThL3ikyi3mBNfXj6RgCdGCkO
6Anhf76G5DgdK+6KP4JgKjA=
=U5n6
-----END PGP SIGNATURE-----