

In This Issue

1. *Malware* – 2. *Scams and Hoaxes* – 3. *Security Screw-Up of the Month* – 4. *Microsoft and Apple Security Updates* – 5. *Security Newsbytes*

1. Malware

Silentbanker. A Trojan that intercepts the bank account information in a user's email before that information has been encrypted (coded), and then sends that information to a central attacker database. Silentbanker can intercept online banking transactions that normally are well guarded by two-factor authentication* procedures. During a banking transaction, Silentbanker will change the user's bank account details over to the attacker's account, while mimicking what the user would expect to see from a typical banking transaction.

More information: <http://www.networkworld.com/news/2008/011408-silentbanker-trojan.html?page=1>

* http://en.wikipedia.org/wiki/Two-factor_authentication

* <http://www.bcs.org/server.php?show=ConWebDoc.9382>

WORM_SILLYFDC.CY. A worm that disables Windows Automatic Updating and the Task Manager (a part of Windows that provides information about your computer's performance, services and running applications). The worm is dropped by other malware on infected websites and spreads via removable devices such as USB sticks and portable drives. Affected computers are unable to get Windows updates automatically. Disabling the Task Manager makes it impossible to check the running processes in order to shut down the infection.

More information:

http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM_SILLYFDC.CY

Secret Crush. Adware* with over 50,000 daily users on Facebook that invites people to find out who amongst their friends has a secret crush on them. Users tempted to discover more have to invite at least five other Facebook users to install the application before their mystery admirer is revealed. However, no secret crush is ever revealed. Instead users are directed to an external website that invites Facebook users to download potentially unwanted applications that will display pop-up advertising.

More information: <http://www.sophos.com/pressoffice/news/articles/2008/01/facebook-adware.html>

*Adware: A form of spyware, installed and activated on your computer without your consent, that collects information about your browsing patterns and uses it to display targeted advertisements as pop-ups in your web browser.

Storm Worm *encore*. A Trojan repackaged yet again. This incarnation of the "Dorf" Trojan sends out emails posing as messages of love in an attempt to lure unsuspecting users to dangerous websites. The emails sport subject lines such as "Falling In Love with You," "Special Romance," and "You're In My Thoughts." The body of the email

contains a link to a website that is actually one of the many compromised computers in the worldwide Storm botnet. The website displays a large red heart, while installing malware onto the visitor's computer.

More information: <http://www.sophos.com/pressoffice/news/articles/2008/01/love-storm.html>

Win 32/Agent. A Trojan-like malware that found its way onto a popular brand of digital photo frames sold by Best Buy, both online and in-store. The affected frames are limited to the 10.4-inch version (model# NS-DPF10A) of Best Buy's own Insignia brand photo frames, although there are reports of the same malware found on similar devices bought from Sam's Club. Best Buy spokesperson Nissa French said the virus was apparently introduced at some point in the manufacturing process.

More information:

http://www.theregister.co.uk/2008/01/25/best_buy_digital_frames_virus/ & <http://isc.incidents.org/diary.html?storyid=3892>

WORM_IRCBOT.SN. A polyglot* worm that opens randomly chosen network ports to an Internet Relay Chat server and then uses that connection to open a backdoor, allowing the attacker to take control of your computer. The worm spreads by sending MSN users a link to a malicious site that downloads a copy of the worm. The link is sent with messages that suggest the website contains pictures, either of the sender or of the recipient, with the provocative questions like: "do I look dumb in this picture? I want to put it on myspace." [sic].

More information: http://www.virusbtn.com/news/2008/01_24a.xml

* <http://en.wikipedia.org/wiki/Polyglot>

2. Scams and Hoaxes

Economic Stimulus Scam. The perpetrators of this fraud are thieves portraying IRS agents. They are soliciting Social Security and bank account numbers or other information supposedly needed to process the tax rebates expected to be part of the economic stimulus package from Washington.

More information: <http://www.kansascity.com/business/story/470366.html>

[Editor's Note (Reichert): You've probably heard this before, but let me repeat it – The IRS does not solicit such information by e-mail or phone. That should be your first clue that this is a scam.]

Reverse Nigerian 419 Scam. An email claiming to be from a United Nations supervised entity called the "Nigerian Government Reimbursement Committee." According to the message, the "lucky" recipient has been identified as a past victim of 419 scammers and has therefore been awarded the sum of \$150,000 as reimbursement. He or she is warned to keep the payment secret because the US Secret Service and Nigeria's Economic and Financial Crimes Commission have "swange into action" [sic] to apprehend further scammers. The message itself is a scam of the exact same type the senders are pretending to combat.

More information: <http://www.hoax-slayer.com/victims-reimbursement-scam.shtml>

Identity Thief Exploits Hotel Business Center and Internet Lounge Computers.

Simbaqueba Bonilla, a Colombian national, pleaded guilty January 9, 2008 to an indictment involving an identity theft scheme in which he installed keylogging software on hotel business center computers and Internet lounges in order to steal passwords, account data, and other personal information. The computer fraud scheme had more than 600 victims worldwide, including U.S. Department of Defense employees. Simbaqueba used money obtained in the scheme to buy expensive electronic devices, including a home theater system, and to fund luxury travel to Hong Kong, France, Jamaica, the U.S., and other locations.

More information: http://www.infoworld.com/article/08/01/10/Colombian-man-pleads-guilty-to-computer-fraud_1.html

[Editor's Note (Reichert): How many of you have sent sensitive personal information (bank accounts, user IDs and passwords, etc.) over a public-use computer or an open wireless connection offered at internet cafes, coffee shops, or hotels? Those of you that raised your hand should rethink how important your personal information is to you. Editor's note (Rietveld): Maybe the Department of Defense should mandate that all of its employees subscribe to OUCH! if they still think hotel business center computers and Internet lounges are safe ways to send personal information.]

eBay Special Offer: Buy a Car and Get Nothing

Shaqir Duraj, a Kosovo refugee who moved to Canada, decided in October 2007 to buy himself a new car. He'd heard about scams on eBay, so he searched for a seller with high satisfaction rating. He found a very nice car, available for \$20,000, offered for sale by a member with 98 percent customer satisfaction rating. He won the bid and sent the money to the seller, but weeks later hadn't received the car. He contacted eBay officials, who wrote him a letter saying that someone had temporarily taken over, or hijacked, the eBay seller's page, and that he would have to contact police and the FBI. Because Shaqir had not used the eBay payment system—he'd been duped into using a phony look-alike webpage--eBay will not provide protection for the transaction.

More information: <http://news.softpedia.com/news/eBay-039-s-Special-Offer-Buy-A-Car-And-Get-Nothing-72756.shtml>

Editor's Note (Wyman): This is a good example of how you can do everything right and end up getting hung out to dry anyway. Remember that 1. Any eBay seller's page might be hijacked, and nowadays in a totally convincing way; 2. Before laying out more money than you can afford to lose, obtain the name, phone number, and address of the seller, and contact the seller directly. While not foolproof, this makes it harder for a Bad Guy to impersonate a *bona fide* seller.

3. Security Screw-Up of the Month

Data Lost on 650,000 Credit Card Holders. Personal information on about 650,000 customers of J.C. Penney and up to 100 or more other retailers could be compromised after a computer tape went missing. GE Money, which handles credit card operations for J.C. Penney and many other retailers, said that the missing information includes Social Security numbers for about 150,000 people. The information was on a backup computer tape that was discovered missing last October. It was being stored at a warehouse run by Iron Mountain Inc., a data storage company, and was never checked out, but can't be

found either, said Richard C. Jones, a spokesman for GE Money, part of General Electric Capital Corp. Jones said there was "no indication of theft or anything of that sort," and no evidence of fraudulent activity on the accounts involved.

More information:

<http://ap.google.com/article/ALeqM5iZchJDcVnuQDNpJsok2PSP5vwRQD8U808VO0>
&
http://www.news.com/Credit-issuer-says-data-lost-for-650%2C000-customers/2100-1029_3-6226913.html?tag=cd.top

4. Microsoft and Apple Security Updates

Microsoft and Apple provide free security updates for their software products.

Windows: Microsoft issues patches for all Microsoft products on the second Tuesday of each month as well as out-of-cycle patches on any day of the month. The next scheduled release date is February 12th. Check manually too, once every two weeks, to make sure all of the updates have been installed.

More information: <http://www.microsoft.com/athome/security/default.aspx>

OS X: Updates are issued frequently, and their contents may differ depending on which processor is in your Mac (PPC or Intel).

More information: <http://www.apple.com/support/downloads/>

iPhones: Must be updated manually:

<http://docs.info.apple.com/article.html?artnum=305744>

5. Security Newsbytes

Computer Security Consultant Charged with Creating Botnet of 250,000 Computers

In the first prosecution of its kind in the nation, a well-known member of the "botnet underground" was charged today with using "botnets" - armies of compromised computers - to steal the identities of victims across the country by extracting information from their personal computers and wiretapping their communications. John Schiefer, 26, of Los Angeles, agreed to plead guilty to four felony counts: accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud.

More information:

http://www.ibls.com/internet_law_news_portal_view.aspx?s=sa&id=1147

Drive-by Download* Menace Spreading Fast

Booby-trapped web pages are growing at an alarming rate with unsuspecting firms acting as nurseries for botnet farmers, according to a new study. Security watchers at Sophos** are discovering 6,000 new infected webpages every day, the equivalent of one every 14 seconds. Four out of five of these webpages actually belong to innocent companies and individuals, unaware that their sites have been hacked. Websites of all types, from those of antique dealers to ice cream manufacturers and wedding photographers, have hosted malware on behalf of virus writers.

More information:

http://www.theregister.co.uk/2008/01/23/booby_trapped_web_botnet_menace/

* http://en.wikipedia.org/wiki/Drive-by_download

** <http://www.sophos.com/>

Pharming*: Home Router Attack Serves Up Counterfeit Webpages

A security researcher says he has observed criminals using a new form of attack that causes victims to visit spoofed banking pages by secretly making changes to their high-speed home routers. According to Symantec researcher Zulfikar Ramzan, the attack changes a router's settings which can then send a user to a rogue web site instead of the one they requested. Malicious code embedded in an email message he uncovered caused the URL for a popular Mexico-based bank to map to a fraudulent website controlled by the attackers.

More information:

http://www.symantec.com/enterprise/security_response/weblog/2008/01/driveby_pharming_in_the_wild.html &

http://www.theregister.co.uk/2008/01/23/pharming_attack_in_the_wild/

* <http://en.wikipedia.org/wiki/Pharming>

Copyright 2008, SANS Institute (www.sans.org).

Editorial Board: Bill Wyman, Alan Reichert, Barbara Rietveld, Alan Paller. Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. Readers are invited to subscribe for free at <https://www.sans.org/newsletters/ouch>.