

In This Issue

1. *Spyware Mini-Quiz* – 2. *Malware* – 3. *Scams and Hoaxes* – 4. *Microsoft and Apple Security Updates* – 5. *Security Screw-Up of the Month* – 6. *Security Newsbytes*

1. Spyware Mini-Quiz

- (1) Approximately how many computers on the Internet are infected with spyware?
- a. 25%
 - b. 45%
 - c. 60%
 - d. 80%
- (2) What is the single best thing you can do to protect your computer against spyware?
- a. Disable Active-X in Internet Explorer
 - b. Protect your computer with a firewall
 - c. Install anti-spyware and keep it updated
 - d. Only browse websites that you know and trust

Answers appear at the end of this OUCH.

2. Malware

Gozi variant: a new strain of an older Trojan, which spreads through infected PDF files, and pilfers financial information. The exploit has turned Adobe's PDF Reader program into a malware installer that loads Gozi Trojan onto victims' computers--another compelling reason to patch Acrobat Reader as well as the full version of Acrobat without delay.

More information: http://www.theregister.co.uk/2007/10/26/new_gozi_strain/ & <http://www.adobe.com/support/downloads/detail.jsp?ftpID=3806>

Pidief.A. This is another Trojan, which spreads through infected PDF files, attached to spam emails typically targeted at all recipients in an entire organization. The emails have subject lines such as "invoice," "statement" or "bill" and contain no text in the body. If the attached PDF is opened using a vulnerable version of Adobe software, the computer will execute code that lowers Windows security settings and installs a bevy of malware. Adobe has issued patches for Acrobat Reader as well as the full version of Acrobat. (See also "Gozi variant" above.)

More information: http://www.theregister.co.uk/2007/10/24/pdf_exploit_in_the_wild/ & <http://www.adobe.com/support/downloads/detail.jsp?ftpID=3806>

Bayrob variant: a new strain of the Trojan that appeared on eBay seven months ago that is spreading as an attachment to an email sent in response to an eBay bid. Once loose on the recipient's computer, it redirects traffic bound for eBay to a phony look-alike website. The Trojan spoofs sensitive pages on eBay, including the "ask a question" messaging feature for online auctions, and inflates the user feedback score of the purported buyer.

More information:

http://www.theregister.co.uk/2007/10/19/return_of_trojan_bayrob/page2.html

3. Scams and Hoaxes

Merrill Lynch Phishing Scam

Bait: An "Urgent" email message claiming that Merrill Lynch customers must click a link and "follow the prompts to answer and record answers to five personalized security questions." The message is not from Merrill Lynch, and the embedded link opens a bogus webpage designed to resemble the genuine Merrill Lynch website. Victims may be tricked into revealing private information that can be collected by scammers and used for identity theft and fraud.

More information: <http://www.hoax-slayer.com/merrill-lynch-phishing-scam.shtml>

Pennsylvania's Anti-Cell Phone Law Isn't

Bait: A PDF attachment to an email warning Pennsylvania drivers that making or receiving cell phone calls will be illegal effective November 10th. The attachment, dubbed a "legislative brief" about the bill's passage, is a hoax. "There's no bill that has passed on legislation yet," State Rep. Bob Bastian said.

More information:

<http://www.dailyamerican.com/articles/2007/10/13/news/news297.txt>

4. Microsoft and Apple Security Updates

Microsoft provides free security updates for Windows, as does Apple for Mac OSX and the iPhone.

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 November 13th. Also check manually every two weeks to make sure all of the updates have been installed.

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

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 Screw-Up of the Month

TJX Maxxes Out on Credit Card Heist

According to court documents filed by a group of banks, more than 94 million accounts fell into the hands of criminals after TJX suffered a protracted security breach that started in 2005 and went on for 17 months. That is about twice as many compromised credit card accounts as the Massachusetts-based retailer admitted to originally.

In March TJX had claimed that information from only 45.7 million accounts had been hijacked, but rumors persisted that the number was much higher. When pressed for details about how their servers had been breached, when, and by whom, TJX clammed up, and offered the defense that such information "if revealed publicly, could serve as a road map for persons trying to attack TJX's computer system or other participants in the

payment card system.” The dodging and weaving have gone on unabated, and riled VISA, MasterCard and a host of banks, who have sued TJX in order to force disclosure. In court documents the plaintiffs lambasted TJX’s use of poor math and fuzzy logic in an attempt to contain the damage. “Unlike other limited data breaches where ‘pastime hackers’ may have accessed data with no intention to commit fraud, in this case it is beyond doubt that there is an extremely high risk that the compromised data will be used for illegal purposes. Faced with overwhelming exposure to losses it created, TJX continues to downplay the seriousness of the situation.”

The 94 million number doesn’t bode well for TJX or for boatloads of its customers whose financial identities may be in jeopardy. Analysts are estimating the total costs to TJX may ultimately run as high as \$1 billion, including legal settlements and lost sales.

Editor’s note: (Wyman) Back in March when this story first broke, TJX revealed reluctantly that over and over again and month after month, thieves had helped themselves to oodles of personal information stored on TJX’s supposedly secure back-end financial transaction servers. Imagine their glee in finding out that, with security of such low caliber in place, it was sure to be a long time until anybody would check the doors and windows. TJX’s defense is so threadbare that it is charitable of the bankers to stop short of calling the retailers liars and a bunch of chickens. Tossing out (of all things) a security rationale for continuing to withhold information will not carry the day in court. What business would be dumb enough to leave its networked data systems open to a TJX Copy-Cat Attack? Time to give credit where it’s due: TJX could not have provided the means and opportunity for the largest credit card heist in history without setting up feeble computer security in the first place, then later failing to monitor or improve that security, and finally ignoring what must have been many indications over a period of nearly a year and a half that something was really wrong.

More information:

http://www.theregister.co.uk/2007/10/24/tjx_breach_estimate_grows/

<http://www.eweek.com/article2/0,1895,2206680,00.asp>

http://www.boston.com/business/globe/articles/2007/10/24/court_filing_in_tjx_breach_doubles_toll/

6. Security Newsbytes

World Series Ticket Sales Fall Prey to Network Attack

When online ticket sales were halted by the Rockies management only a few hours after they began, early reports put the blame on too many enthusiastic fans trying to grab up tickets all at once. But once the dust had settled, and Paciolan--the Irvine, California-based company whose automated ticketing system was responsible for selling the World Series tickets—had a look under the hood, it became clear that the breakdown was not the fault of over-eager fans, but the work of Bad Guys who had carried out an “external malicious attack” on the computerized ticket sales system.

More information: <http://www.eweek.com/article2/0,1895,2205511,00.asp> & http://www.computerworld.com/action/article.do?command=viewArticleBasic&taxonomyId=16&articleId=9043598&intsrc=hm_topic

Websense Warns Consumers of Online California Fire Scams

Websense, Inc. today announced that its security research team has discovered suspicious online scams designed by criminals to steal money from those donating to the California fire effort, and offered these tips to consumers donating online. (1) Ensure you are dealing with legitimate organizations by contacting them on your own. (2) Remember that legitimate organizations do not approach people aggressively for money and donations. (3) Be wary of groups claiming to be affiliated with legitimate organizations and asking for donations, or that ask you to visit their website or participate in an auction to support the donation effort. The sites may be fraudulent or host malicious code designed to steal your personal information.

More information:

<http://money.cnn.com/news/newsfeeds/articles/prnewswire/LATH24425102007-1.htm>

Storm Worm Dubbed “Internet Public Enemy Number One”

The Storm Worm has infected so many machines that it is now one of the most powerful supercomputers, and it’s on the loose. With more than a million processors and a Petabyte (1 quadrillion bytes, i.e. lots) of RAM, the Storm Worm botnet is capable of sending out staggering amounts of spam and viruses, while launching devastating attacks against security researchers or anyone else who might oppose it. Security researchers believe that the Storm Worm botnet consists of between 1 and 10 million PC’s worldwide.

More information: <http://www.pcworld.com/article/id,138694/article.html> & <http://www.pcworld.com/article/id,138898/article.html>

Wi-Fi Security System Broken

Still more holes have been picked in WEP*, a wireless networking security measure widely deployed in homes and businesses worldwide. The latest exploit lets criminals defeat firewalls and spy on where someone goes and what they do online. Experts say that WEP security is comprehensively “broken,” but compatibility issues will force many people to continue using it even though it can be hacked in minutes by an amateur.

More information: <http://news.bbc.co.uk/2/hi/technology/7052223.stm>

* http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

OUCH November Security Mini-Quiz Answers

- (1) d. While expert opinions vary, most sources agree that 80% is a reliable estimate.
- (2) c. Antispyware is as important as antivirus software for protecting your computer.

Copyright 2007, 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>.