Volume 6, Number 2 **February 2009**

SANS OUCH! SANS Institute Security Newsletter for Computer Users

In This Issue

1. Consumer Awareness: Is My Computer Infected with a Virus? – 2. Scams and Hoaxes – 3. Microsoft and Apple Security Updates – 4. Security Newsbytes

1. Is My Computer Infected with a Virus? What Should I Do?

Be alert! After you open and run an infected program or attachment on your computer, you might not realize that you've introduced a virus until you notice something isn't quite right. Here are some signs that your computer *might* be infected:

• Your computer runs more slowly than normal
• Your computer stops responding or locks up often
• Your computer crashes and restarts every few minutes
• Your computer restarts on its own and then fails to run normally
• Applications on your computer don't work correctly
• Disks or disk drives are inaccessible
• You can't print normally
• You see unusual error messages
• You see distorted menus and dialog boxes

These are common symptoms of infection—but they might also indicate hardware or software problems that have nothing to do with a virus.

Be smart!
• Do not ignore the symptoms. Write them down, especially the text of any unusual error messages.
• Look for a pattern, and make a note of it. For example, are all of your applications affected? Is the problem only with printing? When does your system crash?
• Contact your network administrator (computer help desk) or your Internet Service Provider, or call the technical support number provided by the manufacturer of your system.
• Answer the technician's questions carefully, and describe the problem in as much detail possible. The more useful information you can provide, the quicker the problem will be resolved.
• The technician may advise you to stop using your computer. If so, follow that advice. Short-term inconvenience is better than losing all your data or having your identity stolen.
More information: http://www.microsoft.com/protect/computer/viruses/indicators.mspx

2. Scams and Hoaxes

- Mumbai Terrorist Attack Scam
Internet scammers are quick to capitalize on significant and newsworthy events such as terrorist attacks, wars, and natural disasters. One of the criminals behind this email scam claims to be "Anne Nanda," a woman who received gunshot wounds during the November 2008, terrorist attack in Mumbai, India. According to the message, with only weeks to live, Anne requires assistance in distributing a portion of some $28 million to charity and to help a faithful servant. However, the funds do not exist, nor is the message from a terrorist victim. The criminals responsible for the message will attempt to extract

money and personal information from any recipient who falls for the bait and replies.
More information: http://www.hoax-slayer.com/mumbai-terrorist-attack-scam.shtml

- Pastor Removal from Television - Petition Number 2493
According to this protest email, an anti-Christian organization has filed a petition (Petition Number 2493) asking the Federal Communications Commission (FCC) to put an end to all religious programming on radio and television. It requests that recipients "sign" and forward the email as a means of raising awareness of the issue and countering Petition 2493 by collecting at least one million names. However, the information in the email is untrue.
More information: http://www.hoax-slayer.com/petition-number-2493.shtml
http://www.hoax-slayer.com/petition-value.html

- Quick and Easy Survey Phishing Scam
According to this email, the recipient can have $90 credited to his or her bank account simply by participating in an "easy 8 questions survey." The message includes a link to a website where the recipient can supposedly fill out the survey and claim the reward. However, although the survey web page may look genuine, it is in fact designed to steal personal information including credit card details. The scam emails may include formatting and logos that make them look like valid company messages.
More information: http://www.hoax-slayer.com/quick-easy-survey-scam.shtml

3. 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 10th. 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.mspx
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 & iPods: Must be updated manually:
http://docs.info.apple.com/article.html?artnum=305744
http://support.apple.com/kb/HT1483

4. Security Newsbytes

- Downadup or Conficker Worm Bores into 20 Million PCs
An estimated 20 million Windows PC's have been infected by the "Downadup" or "Conficker" worm in just a few weeks. Downadup exploits a bug in the Windows Server service used by Windows 2000, XP, Vista, Server 2003 and Server 2008. Although Microsoft fixed the flaw with an "out of cycle" update in late October, about one third of all PCs have not yet been patched, according to Qualys Inc., a security company. Those PCs are the ones being hijacked by the worm. Once it's gotten onto a PC, Downadup generates a list of possible domains, selects one, then uses that URL to reach a malicious server from which it downloads additional malware to install on the hijacked computer.

More information: http://www.ireallyshouldstudy.com/technology/2009/01/26/the-conficker-worm-infects-20-million-computers/
http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx
http://www.microsoft.com/security/malwareremove/default.mspx

- Mac Malware Tide on the Rise
Less than a week after researchers spotted new malware targeting naive Mac users, two additional titles have been spotted. Trojan-horse software dubbed OSX.Trojan.iServices.B hitches a ride on pirated copies of Adobe Photoshop CS4 for Mac. A program used to generate a valid serial number to unlock the Adobe application installs a backdoor on machines that makes them part of a botnet. Another Trojan piggybacks off illicit copies of Apple's iWork 09 productivity suite. Trojans aren't the only threats preying on OS X users. Two new rogue applications that claim to offer malware protection for Mac users have recently been spotted. Rogue anti-virus programs have long been the bane of PC users. Now they're becoming increasingly common on the Mac platform, too.
More information: http://www.theregister.co.uk/2009/01/26/more_mac_malware/

- Spam Rises 150% in Two Months
The number of junk emails being sent to computer users around the world has risen more than 150 percent in two months, as spammers fight back against efforts to shut them down. In November, the level of spam junk emails fell dramatically after the plug was pulled on McColo Corp, an American company accused of providing the gateway for much of the world's junk emails. But, in just a few weeks, the world's biggest junk-email gangs have regrouped. According to data compiled by Google, computer users can expect to receive more unsolicited emails this year than ever before. Spammers use networks of compromised computers – known as "botnets"– to amass enough computing power to send millions of messages a day. The vast majority of owners of those systems do not know they are being used for this purpose.
More information:
http://technology.timesonline.co.uk/tol/news/tech_and_web/article5598661.ece

- Payment Processor Breach May Be Largest Ever
A data breach last year at Princeton, N.J. payment processor Heartland Payment Systems may have compromised tens of millions of credit and debit card transactions. Such figures may make the Heartland incident one of the largest data breaches ever reported. The company, which processes payments for more than 250,000 businesses, began receiving fraudulent activity reports late last year from MasterCard and Visa on cards that had all been used at merchants which rely on Heartland to process payments. Heartland called the U.S. Secret Service and hired two forensics teams to investigate. Last week investigators uncovered the source of the breach: a piece of malicious software planted on the company's payment processing network that recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients. Heartland does not know how long the malicious software was in place, how it got there, or how many accounts may have been compromised. The stolen data includes names, credit and debit card numbers and expiration dates.

More information:
http://voices.washingtonpost.com/securityfix/2009/01/payment_processor_breach_may_b.html

- "Obama quits" Spam Recruits Zombie Drones
Scammers are capitalizing on worldwide interest in Barack Obama's inauguration via a spam email campaign that claims the 44th President doesn't want the responsibility of saving a "sinking ship." Unwary recipients who click on the embedded links are redirected to lookalike Obama campaign websites designed to trick them into downloading malicious code that turns their computers into zombies on the Waledec botnet. Bogus sites with names like "greatobama" or "superobama" contain links to files called, for example, "barakspeech.exe." Users who run this file on an unprotected Windows PC infect their own systems. The fraudulent emails associated with the campaign come with subject lines such as "Amazing News."
More information: http://www.theregister.co.uk/2009/01/19/obama_quitsmlaware_spam_scam/

****

Copyright 2009, SANS Institute (http://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. We request that redistributions include attribution for the source of the material.
Readers are invited to subscribe for free at https://www.sans.org/newsletters/ouch.