

Insight to Security

State of Idaho, Office of the CIO, Cyber Security Newsletter



In this Issue:

Smart Phones, How Secure is your Information	1,2
Rogue Anti-Virus	3
I-Phone Vulnerability with SMS	4
Quick Notes—What's Happening	5

Smart Phones—How Secure is Your Information?(MS-ISAC)

All This in One Device!

Mobile communication devices (includes Blackberrys, iPhones, smart phones in general) have become indispensable tools for today's highly mobile society. Small and relatively inexpensive, these multifunction devices can be used not only for voice calls but also text messages, email, Internet access along with stand alone applications similar to those performed on a desktop computer. A significant amount of personal, private and/or sensitive information may accumulate or be accessed via these

devices. Additionally, some of these devices may allow you to access your home computer or your corporate network.

What Risks Do They Present?

While the devices offer many benefits and conveniences, they also pose risks to you and/or your organization's security. As these devices continue to take on the characteristics of personal computers, they also inherit the same potential risks. Some of the primary risks include the following:

Security of Smart Phones (from page 1)

- The portability of the device leads to a higher likelihood of loss of the device. Millions of mobile communication devices are lost each year.
- When Bluetooth and/or wireless (not cellular) communications are enabled, these devices are subject to the risk of eavesdropping and “highjacking”.
- “Malware” available, that if installed on your device, can allow a perpetrator remote access to your device to listen and record all of your calls, send text messages to the perpetrator whenever you make or receive a call, read all of your messages, make calls on your behalf from your phone, access all of the information on your phone, trace your location and enable the speaker functionally on the phone to listen in on conversations even when the phone is not in use.
- Sites purporting to offer “free games or ring tones” are major vectors for distributing malware.



While the reports of worms and viruses impacting these devices are relatively low, this is expected to increase in the future.

Despite the risks outlined above, many users do not understand how vulnerable their mobile device is or how to deploy important security settings and controls.

What Can I Do to Secure My Mobile Communication Device?

The following outlines steps you can take to protect your mobile communication device. Some of the steps are dependant upon the functionality of your device.

- Use a password to access your device. If the device is used for work purposes, you should follow the password policy issued by your organization.
- If the Bluetooth functionality is not used, check to be sure this setting is disabled. Some devices have Bluetooth-enabled by default. If the Bluetooth functionality is used, be sure to change the default password for connecting to a Bluetooth enabled device.

- Do not open attachments from untrusted sources. Similar to the risk when using your desktop, you risk being exposed to malware when opening unexpected attachments.
- Do not follow links to untrusted sources, especially from unsolicited email or text messages. Again, as with your desktop, you risk being infected with malware.
- If your device is lost, report it immediately to your carrier or organization. Some devices allow the data to be erased remotely.
- Review the security setting on your device to ensure appropriate protection. Be sure to encrypt data transmissions whenever possible.
- Enable storage encryption. This will help protect the data stored on your device in the event it is lost or stolen, assuming you have it password protected!
- Beware of downloading any software to your device. If the device is used for work, follow your organization’s policy on downloading software.

Before disposing of the device be sure to wipe all data from it and/or or follow your organization’s policy for disposing of computer equipment.

For more information on securing mobile communication devices, please visit:

National Cyber Alert System - Cyber Security Tip ST06-007, Defending Cell Phones and PDAs Against Attack

<http://www.us-cert.gov/cas/tips/ST06-007.html>

NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security

<http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf>

FTC Consumer Alert – The 411 on Disposing of Your Old Cell Phone <http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt044.shtm>

WTHR News story on “Tapping Your Cell Phone” <http://www.wthr.com/Global/story.asp?s=9346833>

Also see the I-Phone article on page 4



Your PC May Be Infected!
Click [here](#) to clean it!

Have you seen this advertisement or similar pop-up messages? A free PC scan or an offer to clean your computer of supposedly infected files are often attempts by malevolent persons or organizations to install malicious software (malware) such as a Trojan horse, keylogger, or spyware. Such software is referred to as rogue (fake) anti-virus malware.

How can my system get infected?

The primary way rogue anti-virus software gets on your system is the result of you clicking on a malicious link in an advertisement or similar pop-up message. The wording contained in the advertisement is usually something alarming, designed to get your attention and attempt to convince you to scan your PC or clean it immediately with the offered tool. The names of the fake programs sound legitimate, and often, in a further attempt to make the malware appear legitimate, the programs may prompt you to pay for an annual subscription to the service.



Won't my valid anti-virus and anti-spyware program protect my computer?

Though good anti-virus and anti-spyware programs will protect against many threats, they cannot protect against all malware threats, especially the newest ones. There are millions of different versions of malware, with hundreds more being created and used every day. It may take a day, a week, or even longer for anti-virus companies to develop and distribute an update to detect and clean the newest malware.

What can rogue anti-virus software do to my computer?

Just about anything, especially if you are using administrative-level access when using your computer. Rogue anti-virus software might perform many activities, including installing files to monitor your computer use or steal credentials, installing backdoor programs, or adding your computer to a botnet. The malware might even use your computer as a vehicle for compromising other systems in your home or workplace network.

Rogue anti-virus software can also modify systems files and registry entries so that even when you clean off some infected files or registry keys others might remain, or even allow the infections to be restored and active again after your system is rebooted. This type of



malware can block access to valid security sites so that you won't be able to patch or clean your system by visiting those valid sites.

What can I do to protect my computer?

Don't click on pop-up ads that advertise anti-virus or anti-spyware programs. Even though pop-up ads are used for valid advertising they can also be used for malicious purposes, like getting you to install fake security programs. If you are interested in a security product, search for it and visit its homepage, don't get to it through a pop-up ad.

Use and regularly update firewalls, anti-virus, and anti-spyware programs. It is very important to use and keep these programs updated regularly so they can protect your computer against the most recent threats. If possible, update them automatically and at least daily.

Properly configure and patch operating systems, browsers, and other software programs. Keep your system and programs updated and patched so that your computer will not be exposed to known vulnerabilities and attacks.

Turn off ActiveX and Scripting, or prompt for their use. ActiveX controls are small programs or animations that are downloaded or embedded in web pages, which will typically enhance functionality and user experience. Many types of malware can infect your computer when you simply visit a compromised site and allow anything to run from the website, such as ads. Turning off ActiveX and Scripting can help protect your computer if you inadvertently browse to or are unwillingly redirected to a malicious site. (Check with your IT personnel to see how to do this.)

Keep backups of important files. Sometimes cleaning infections can be very easy; sometimes they can be very difficult. You may find that an infection has affected your computer so much that the operating system and applications need to be reinstalled. In cases like this it is best to have your important data backed up already so you can restore your system without fear of

losing your data.

- **Regularly scan and clean your computer.** If your organization already has configured this on your computer, do not disable it. If you need to scan your computer yourself, schedule regular scans in your programs. Also, several trusted anti-virus and anti-spyware vendors offer free scans and cleaning. Access these types of services from reputable companies and from their webpage, not from an unexpected pop-up. (see some sources on next page)

Office of the CIO, Cyber Security Newsletter

650 W State St
Boise ID 83720

Phone: 208-332-1851

Email: terry.pobst-martin@cio.idaho.gov

**CHECK OUT
THESE
LINKS**

Links Websites about Rogue AV:

Partial Listing of Rogue Security Software: http://en.wikipedia.org/wiki/Rogue_software

Free Security Checks: www.staysafeonline.info/content/free-security-check-ups

About Pop-ups: www.msisac.org/awareness/news/2008-12.cfm

About Web Browser Attacks: www.msisac.org/awareness/news/2008-07.cfm

About Malware: www.onguardonline.gov/topics/malware.aspx

About Spyware: www.onguardonline.gov/topics/spyware.aspx

Free Check for File Infection: www.virustotal.com/

**Do you know the
last time your Anti-
virus scanned your
computer???**
**Take an active role
in ensuring your
computer and net-
work are secure.**

Apple Working to Resolve Vulnerability on I-Phones

Apple is currently trying to patch a serious SMS vulnerability on their iPhone. Apple is working to fix an iPhone vulnerability that could allow an attacker to remotely install and run unsigned software code with root access to the phone.

The attack in question exploits a weakness in the way iPhones handle text messages received via SMS (Short Message Service), said a security researcher, during a presentation at the SyScan conference in Singapore on July 2. He did not provide a detailed description of the SMS vulnerability, citing an agreement with Apple.

Though SMS is usually used to send short text messages between cell phones or other devices, it can also send binary code. If sent to an iPhone, the code is processed the without any user interaction. Each SMS message is limited to 140 bytes, but longer sequences can be sent to the phone as multiple messages that are automatically reassembled. This feature allows larger programs to be delivered to a phone.



The SMS vulnerability could allow an attacker to run malicious code on the phone that is sent by SMS over a mobile operator's network. This malicious code could include commands to monitor the location

of the phone using GPS, turn on the phone's microphone to eavesdrop on conversations, or make the phone join a distributed denial of service attack or a botnet, the researcher said.

Apple is working on an update or patch which will resolve the vulnerability; they expect to have a fix ready later this month. This is particularly important since the researcher who discovered the vulnerability will be discussing the attack in greater detail during a scheduled presentation at the Black Hat USA conference in Las Vegas from 25-30 July.



Quick Notes—What’s Happening

July 6, ZDNet – June malware report. June marked an increase in malware and the “highest rate of phishing attacks to date” on the Web, Fortinet’s latest report on online threats found. The threat management vendor released on July 6 its latest monthly report, which highlighted the current reign of Trojan horses and “disappointing” anti-spam campaigns. Of the overall 108 newly-reported vulnerabilities in June, 62 were active exploits, indicating an “all-time high” of 57.4 percent.

http://news.zdnet.com/2100-9595_22-318200.html



July 6, 2009, CNET News – On Monday, July 6, Microsoft warned of a hole in its Video ActiveX control. This vulnerability could allow an attack which would enable a hacker to take control of a PC if the user visits certain malicious Web sites. According to Microsoft, there have already been some attacks exploiting the vulnerability, which affects Windows XP and Windows Server 2003. In May, Microsoft also announced a vulnerability in how DirectX handles QuickTime files, and they have yet to provide a patch for that problem.

http://news.cnet.com/8301-1009_3-10280141-83.html; <http://support.microsoft.com/kb/972890>

July 5, Reuters – Goldman Sachs says “Russian hacker” tried to steal Goldman Sach’s critical processes. Over the July 4th holiday weekend, a Russian immigrant was arrested for trying to steal highly sensitive computer coding which gives Goldman Sach’s its “edge” in rapid stocks and commodities trading. The FBI appears to have been notified by the hacker’s former employer, Goldman Sachs itself, where Sergey Aleynikov, who is a US citizen and lived in the US for 19 years, was a Vice President. It’s difficult to tell whether or not this was real industrial espionage or just paranoia on the part of Goldman Sachs who lost Sergey Aleynikov to another company.



<http://blogs.reuters.com/commentaries/2009/07/05/a-goldman-trading-scandal/>

June 30, InformationWeek – Zeus Trojan variant steals FTP login details. A new Trojan malware has been detected harvesting FTP account information from compromised computers. The number of affected accounts identified by Prevx, a maker of computer security software, rose from 66,000 on June 24 to 74,000 two days later. According to the director of research at Prevx, the Trojan is highly infectious. “We rate this infection as critical,” he said in a blog post on June 28. “The infection has a ‘China Syndrome’ potential. It includes a cyclic infection which leverages infected PCs to automatically modify hi-volume Web sites to infect additional users who become part of the cycle.

<http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=218102149>

June 30, DarkReading – ‘Mafiaboy’: cloud computing will cause Internet security meltdown. A reformed black-hat hacker, better known as the 15-year-old “mafiaboy” who, in 2000, took down Websites CNN, Yahoo, E*Trade, Dell, Amazon, and eBay, says widespread adoption of cloud computing is going to make the Internet only more of a hacker haven. “It will be the fall of the Internet as we know it,” the hacker said on June 30 during a Lumension Security-sponsored Webcast event.

<http://www.darkreading.com/securityservices/security/attacks/showArticle.jhtml?articleID=218102139>



Michael Calce, aka “Mafia Boy”