VOLUME 3, ISSUE 1

FEBRUARY 2010

InsighT to Security

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

In this Issue:

Cyber Security Trends	1,2
Cyber Attacks Worsening	3
Quick Security Highlights	4,5
How do I update Windows applications?	5
Rogue Anti-Virus Details	6

Cyber Security Trends (from MS-ISAC)

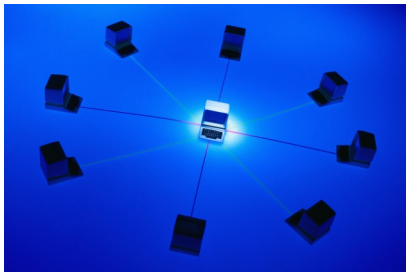
As 2010 unfolds, it's an opportune time to assess the cyber security landscape and prepare for what new challenges may lie ahead, as well look at which current threats may continue.

- **Scareware – fake/rogue security software:** These fake anti-virus sales pitches are preceded by a pop-up which presents a realistic-looking report of infected files. If a user clicks anywhere on the pop-up or browser, they are launched. There are over 40 million types of malicious software (malware), with hundreds more being created and used every day. This type of scam can be particularly profitable for cyber criminals -- as many users believe the pop-up warnings and are lured into downloading and paying for the special software to "protect" their system. See page 6 for more information.

- **Malware, worms, and Trojan horses:** These will continue to spread by

Cyber Security Trends (from page 1)

email, instant messaging, malicious websites, and infected non-malicious websites. Some websites will automatically download the malware without the user's knowledge or intervention. This is known as a "drive-by download." Other methods will require the users to click on a link or button.



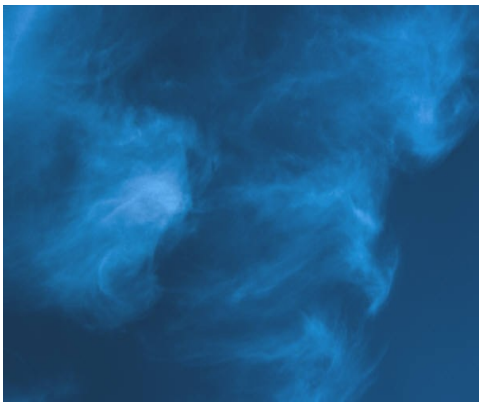
- **Botnets and zombies:** These threats will continue to proliferate as attack techniques evolve and become available to a broader audience, with less technical knowledge required to launch successful attacks. Botnets designed to steal data are improving their encryption capabilities and thus becoming more difficult to detect.

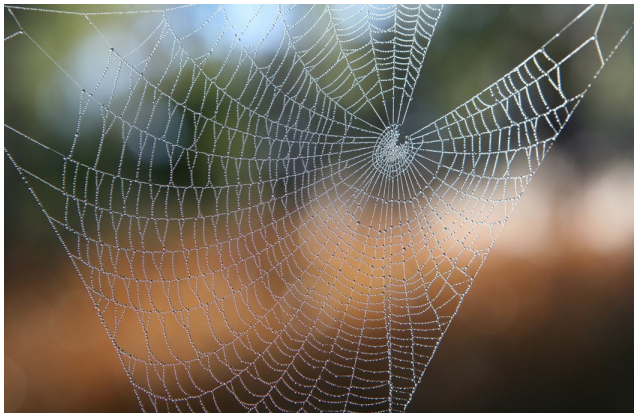
- **Attacks on user applications software** - With most organizations or users getting automated updates for their operating systems, user application vulnerabilities are now an increasingly popular means of attacking systems. User applications, also known as client-side software, include programs such as Internet browsers, media players, PDF readers, etc. This software will continue to have vulnerabilities and subsequently be targeted by various malwares.

- **Ransom attacks** occur when a user or company is hit by malware that encrypts their hard drives or they are hit with a Distributed Denial of Service Attack (DDOS) attack. The cyber criminals then notify the user or company that if they pay a small fee, the DDOS attack will stop or the hard drive will be unencrypted. This type of attack has existed for a number of years and is now gaining in popularity.

- **Social Network Attacks:** Social network attacks will be one of the major sources of attacks in 2010 because of the volume of users and the amount of personal information that is posted. Users' inherent trust in their online friends is what makes these networks a prime target. For example, users may be prompted to follow a link on someone's page, which could bring users to a malicious website. Or, by playing a "game" they could reveal personal information such as those items which are used for security questions with on-line banks.

- **Cloud Computing:** Cloud computing is a growing trend due to its considerable cost savings opportunities for organizations. Cloud computing refers to a type of computing that relies on sharing computing resources rather than maintaining and supporting local servers. The growing use of cloud computing will make it a prime target for attack.





- **Web Applications:** There continues to be a large number of websites and online applications developed with inadequate security controls. These security gaps can allow a criminal to compromise the site, leading to the infection of the site's visitors.

- **Budget cuts** will be a problem for security personnel and a boon to cyber criminals. With less money to update software, hire personnel and implement security controls, enterprises will be trying to do more with less. By not having up-to-date software, appropriate security controls or enough personnel to secure and monitor the networks, organizations will be more vulnerable.

Cyberattacks Worsening (NASCIO, Charles Robb)

Homeland Security.

Attacks on Critical Infrastructure

Owners and operators of critical infrastructure in more than a dozen countries say their information technology networks and control systems are under constant attack, costing individual companies an average of about $6 million for each day of downtime, according to a report released today. "The situation is becoming worse not better," said the report, prepared by the Center for Strategic and International Studies based on a survey of 600 security executives for critical infrastructure in 14 countries.

Not prepared for Cyber Attacks

Nearly a third of executives said their own sector was either not prepared or not well prepared to deal with cyberattacks from sophisticated adversaries, but there was significant variation among nations. Notably, 60 percent of respondents said their sector is already under attack from governments, with the largest group -- 36 percent -- saying they were most worried about attacks coming from the U.S. government.

“When executives were asked about the likelihood of a major cyberattack on their infrastructure. Forty percent said they believe a major attack will occur in the next year, while 80 percent said a major attack would occur within five years,” said Stewart Baker, the former Homeland Security Department policy chief who helped prepare the report.

Charles Robb is the National Association of State Chief Information Officers (NASCIO) Senior Policy Analyst

NASCIO
Representing Chief Information Officers of the States

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

Security Websites:

Good websites to surf:

http://www.sans.org/

http://www.cert.org/

http://www.msisac.org/

http://csrc.nist.gov/

http://www.issa.org/

http://www.infragard.net/

http://www.ic3.gov/

http://www.securityfocus.com/

http://www.snopes.com/

http://www.nationalterroralert.com/

Don't trust any e-mails from unknown people unless you believe strongly it is a legitimate e-mail.

Do NOT click on any links in suspicious e-mails.

Quick Security Highlights

February 11, Adobe—(International) **Adobe Systems Inc. issued an emergency update to its Acrobat and Reader** applications, repairing two critical vulnerabilities that could be used by attackers to crash the program and take control of an affected system. It also issued updates for its **Flash Player and Adobe AIR**, an application currently being advertized strongly by the New York Times right now. The updates for Reader is for all operating systems, to include Macintosh and UNIX. An attacker can exploit the Adobe Acrobat and Reader vulnerabilities by users opening a specially crafted PDF document. An attacker can exploit the Adobe Air and Flash Player vulnerabilities by users visiting a specially crafted website. Successful exploitation of one of these vulnerabilities could result in an attacker gaining the same privileges as the logged-on user. Depending on the privileges associated with the user, the attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Go to www.adobe.com and look for "Downloads", "Updates" and then search for the different applications you have installed on your computer to find the latest update. Or, open your application, select "Help" and "Check for updates."

———————————————————————————————-

February 5, V3.co.uk – (International) **Top search results riddled with malware.** Many Internet users are not aware that the search results they may get from any search engine are not necessarily safe results. If they click on the links without some type of filtering, they may connect to a webpage that is infected with malicious software (malware), according to a new report from Websense. The security firm recently reported that criminals who write and distribute malware have increased their efforts to get noticed by manipulating search results to drive traffic in their direction. Almost 14 percent of searches for current "buzz words", such as celebrities or current events, lead to malware sites or links, the report said. More worrying is the finding that 71 percent of pages found to be infected were legitimate sites that had been poisoned in some way. Websense reported growth of 225 percent in malicious web sites over the second half of last year. Web 2.0 sites also proved popular with malware writers. Websense said that 95 percent of comments on blogs were spam or led to malicious pages. Tools, such as McAfee Site Advisor can help reduce, but may not eliminate, the risk associated with using links.

Quick Security Highlights (continued)

February 5, V3.co.uk – (National) **U.S. Cybersecurity Enhancement Act sails through House.** The Cybersecurity Enhancement Act was passed by the U.S. House of Representatives by a huge margin, 422:5, better than expected. This indicates the act will likely pass through the Senate. It calls for the National Science Foundation to spend $396m over the next four years to fund cyber security research, including $94m to fund scholarships into security research, on the proviso that those who receive them work in the public sector for the same number of years as their studies. The National Institute of Standards and Technology will develop a strategic plan for national security within a year and will also set out technical security standards for the industry as a whole. Federal agencies spend $6bn annually on cyber security to protect a $72bn IT infrastructure, according to the Office of Management and Budget. "Critical infrastructures ranging from electrical grids, to oil production facilities to telecoms and transportation networks are under constant attack from cyber criminals," said the Chief Technology Officer at McAfee.

January 27, SC Magazine – (International) **Expect attacks on the new iPad.** The popularity of Apple devices has encouraged criminals to develop malicious software (malware) designed to attack the growing number of those devices, according to a report from Intego. With the announcement of the new iPad, Apple's new revolutionary tablet, most people will not question its security issues. The device is already being touted as a game-changer in the publishing industry because it introduces a new digital platform, with a screen just under 10 inches, for the delivery of newspaper and magazine content. What is likely to follow within months of the debut, if history is any precedent, is a new wave of malware targeting the device. Users tuning in for their daily news feed or perusing copies of their favorite magazines may become victims of new iterations of malware likely intended to steal their passwords and personal information to then be offered for sale in the nether regions of cyberspace.

How do I update my Microsoft Windows applications? (repeated due to popular demand)

Windows Update is a Microsoft service that provides updates for the Windows operating system and other Microsoft software. Installing Windows updates, such as "service packs" and other patches, is necessary to keep your Windows system secure.

To activate Windows Update, go to Settings/Control Panel/Automatic Updates. When you turn on Automatic Updates, Windows routinely checks the Windows Update web site for high-priority updates that can help protect your computer from the latest viruses and other security threats.

These updates can include security updates, critical updates, and "service packs." Depending on the setting you choose, Windows automatically downloads and installs any high-priority updates that your computer needs, or notifies you as these updates become available.

Rogue (Fake) Anti-Virus Software: How to Spot It & Avoid It!

Have you seen this advertisement or similar pop-up messages? This is a fake warning that your computer supposedly has infected files and it is an attempt by criminals to install malicious software (malware) on your computer. It may install a Trojan, a keylogger, or some spyware.

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 or just visiting an infected webpage. The wording contained in the advertisement is usually something alarming, designed to get your attention and attempt to convince to you scan your PC or clean it immediately with the offered tool.

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

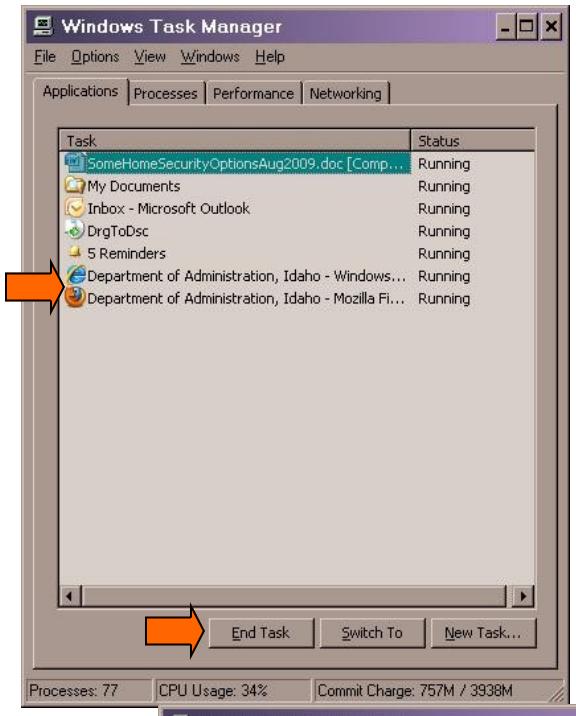
Though good anti-virus and anti-spyware programs will protect against many threats, they cannot protect against all malware threats, especially anything brand new that the criminals have just started using. There are millions of different versions of malware, with hundreds more being created and used every day.

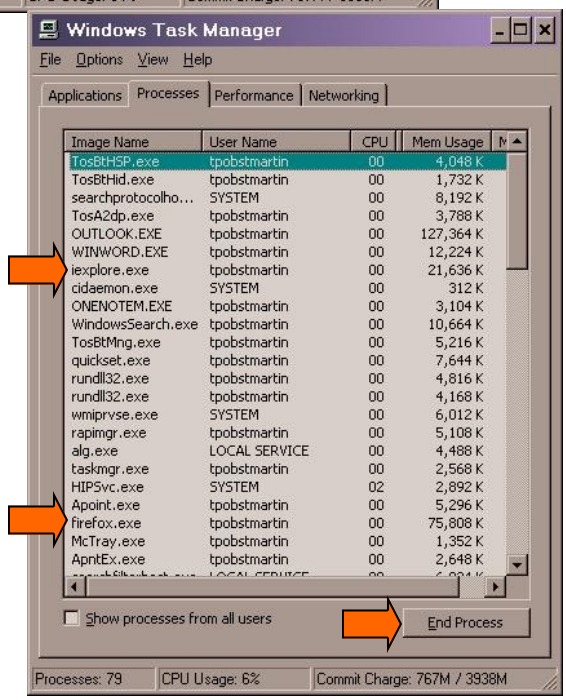
What can rogue anti-virus software do to my computer?

Just about anything, especially if you are using administrative-level access when using your computer: installing files to monitor your computer use or steal credentials, installing backdoor programs, adding your computer to a botnet, compromising other systems in your home or workplace network.

What can I do to protect my computer?

- **Don't cluck ANYWHERE on the webpage—anywhere you click could activate a download or installation.** Close your browser without clicking on it. One great way to do this is to use Windows Task Manager (Ctrl, Alt, Del) to end the Task or to stop the Process. See the images below.





- **Use and regularly update firewalls, anti-virus, and anti-spyware programs.**
- **Properly configure and patch operating systems, browsers, and other software programs.**
- **Turn off ActiveX and Scripting, or prompt for their use.**
- **Keep backups of important files.**
- **Regularly scan and clean your computer.**