State of Oklahoma
Monthly Cyber Security Tips
NEWSLETTER

May 2009

Volume 4, Issue 5

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

From the Desk of CPT Jeff Elliott, Oklahoma Office of Homeland Security

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 to you 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.

Any kind of website could host ads for rogue anti-virus: news sites, sports pages, and social networking sites as well as "riskier" sites such as hacker blogs. Some varieties of rogue anti-virus programs will also get installed on your machine just by you visiting a website with a malicious ad or code, and you might never know you've been impacted.

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. For example, one recent rogue anti-virus program reportedly installed several

malicious Trojan files, and also made over two-dozen different changes to ensure that the malware stayed on the system and stayed running. This type of malware also often blocks access to valid security sites (anti-virus and anti-spyware companies, and operating system and application update 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?

1. **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.
2. **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.
3. **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.
4. **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. (You can limit the functionality of your Internet browser through its configuration choices, but be sure to look for a guide if you are unfamiliar with how to limit scripting and active content—see below for resources.)
5. **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.
6. **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.

For more information, please visit:

Partial Listing of Rogue Security Software: http://en.wikipedia.org/wiki/Rogue_software
Free Security Checks: www.staysafeonline.info/content/free-security-check-ups
Pop-ups: www.msisac.org/awareness/news/2008-12.cfm
Web Browser Attacks: www.msisac.org/awareness/news/2008-07.cfm
Malware: www.onguardonline.gov/topics/malware.aspx
Spyware: www.onguardonline.gov/topics/spyware.aspx
Free Check for File Infection: www.virustotal.com/

For more monthly cyber security newsletter tips visit:
www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. Organizations have permission--and in fact are encouraged--to brand and redistribute this newsletter in whole for educational, non-commercial purposes.

Brought to you by:

MS-ISAC

www.msisac.org