Texas Department of Information Resources
CYBER SECURITY TIPS
Monthly Newsletter
Office of the Chief Information Security Officer June 2009 | Volume 3, Issue 5

Rogue/Fake Anti-Virus Software: How to Spot It & Avoid 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 may 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 may also be 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.

The Conficker worm also downloads and launches a fake antivirus application, Spyware Protect 2009. As is typical with this sort of scam, the antivirus program claims to identify multiple problematic files and offers to remove them for the convenient fee of $49.95—credit cards happily accepted.[1]

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 remove the newest malware.

WHAT CAN ROGUE ANTI-VIRUS SOFTWARE DO TO MY COMPUTER?

Rogue anti-virus software can do 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.

[1] Conficker launches antivirus scam as malware hits Twitter:
arstechnica.com/security/news/2009/04/conficker-launches-antivirus-scam-as-malware-hits-twitter.ars

Rogue anti-virus software can also modify system files and registry entries so that even when you clean off some infected files or registry keys others might remain. They may 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. Just don't get to it through a pop-up ad.
2. Use and regularly update firewalls and 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. NOTE: 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.
5. Keep backups of important files. Sometimes cleaning infections can be very easy, but 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.

ADDITIONAL RESOURCES

For additional information on rogue anti-virus software, please visit:

- Partial Listing of Rogue Security Software: **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/**

DIR OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER
300 W. 15TH ST., STE. 1300 | AUSTIN, TX 78701 | WWW.DIR.STATE.TX.US/SECURITY

For previous issues of the Monthly Cyber Security Tips Newsletter, please visit **www.dir.state.tx.us/security/reading**.
For more information on Internet security, please visit the SecureTexas website at **www.dir.state.tx.us/securetexas**.
SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. Report serious information security incidents as quickly as possible to your agency's Information Security Officer and to DIR's 24/7 Computer Security Incident Notification hotline: (512) 350-3282.

Brought to you by:

MS-ISAC

www.msisac.org

Powered by:

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

www.us-cert.gov

Distributed by:

DIR Secure Texas

www.dir.state.tx.us/securetexas