Monthly Cyber Security Tips

NEWSLETTER

September 2010 Volume 5, Issue 9

Detecting and Avoiding Fake Anti-Virus Software

From the DoIT Office of Security Services

Your Computer Is Infected with Malware!
Click **here** to purchase recommended anti-virus software!

You may be familiar with this or similar messages appearing on a website, urging you to take action purportedly designed to clean your allegedly infected computer. Unfortunately, these messages are often scams that attempt to install malicious software (malware) onto your computer. Such software is referred to as rogue (fake) anti-virus malware, and the incidents are increasing. Last year, the FBI reported an estimated loss to victims in excess of $150 million from this type of scam[1].

How can my system get infected?
These types of scams can be perpetrated in a number of ways, including via website pop-up messages, web banner advertisements, spam and posting on social networking sites. Scams are also appearing via the use of "tweeting." The rogue software scam generally uses social engineering to make the user believe his or her machine is infected and that by taking action (clicking on the link provided) the machine will be cleaned. If you click on the malicious link, you may be downloading malware onto your machine. 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.

Some varieties of rogue anti-virus programs will also get installed on your machine without any interaction by you: your machine could be compromised just by you visiting a website with a malicious ad or code and you wouldn't know.

What is the impact from rogue anti-virus software?
Rogue anti-virus software might perform many activities, including installing files to monitor your computer use, steal credentials, install backdoor programs, and add your computer to a botnet. The installation of malware could result in a high-jacked browser (i.e., the browser navigates to sites you did not intend), the appearance of new or unexpected toolbars or icons and sluggish system performance. Additionally, another concern related to rogue anti-virus software is the false sense of security you may have, erroneously believing your machine is protected by anti-virus software when in fact it is not.

What can I do to protect my computer?
Applying computer security best practices will help protect your machine and minimize any potential impacts.

[1] http://www.fbi.gov/cyberinvest/escams.htm

1. **Don't click on pop-up ads that advertise anti-virus or anti-spyware programs.** If you are interested in a security product, don't try to access it through a pop-up ad; contact the retailer directly through its homepage, retail outlet or other legitimate contact methods.
2. **Don't download software from unknown sources.** Some free software applications may come bundled with other programs, including malware.
3. **Use and regularly update firewalls, anti-virus, and anti-spyware programs.** Keep these programs updated regularly. Use the auto-update feature if available.
4. **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.
5. **Regularly scan and clean your computer.** Scan your computer with your anti-spyware once a week.
6. **Back up your critical files.** In the event that your machine becomes infected, having backups of your important files will facilitate recovery.

NOTE: Regarding the above recommendations, many organizations have formal processes that automatically update and patch appropriate software, scan computers and perform file back-ups. In these cases, no end user action is necessary.

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
Malware: www.onguardonline.gov/topics/malware.aspx
Spyware: www.onguardonline.gov/topics/spyware.aspx

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