How Malicious Software Attacks Your PC by Shally

Article published on December 1st 2011 | Software

If you have the best antivirus and spyware removal tools running on your computer, yet your computer is infected. How is that possible? To answer this question, we will be discussing some of the common ways black hat coders get their code on a computer.

Drive-By Download Sites

If you install all available software patches and update your security software regularly, you are less likely to fall prey to malicious software attacks. One of the main problems is drive-by download sites. Drive-by download sites are sites that host malicious software. These sites are always looking for vulnerabilities in browsers and add-ons.

The way drive-by download sites work is simple. When you visit a rogue site, a script is installed on your computer. The script then creates buffers, which pave the way for malware to install on your computer. You don't have to click on a link or download anything to get your computer infected. The minute you visit the web site, a script gets downloaded on your computer.

Rogue Software

The majority of attacks these days need the user's permission. Users have to give administrative approval for an application to run the first time. The second time you run the program, the application creates backdoors that allow it to install malicious software on your computer , but this time, without your permission. What are we talking about here? We are talking about software you downloaded, it was scanned for viruses and it came out clean. This software opened a back door for another malicious program to be installed on your computer and wreak havoc.

Phishing

Information can be stolen from your computer when you click on a link in an email from someone you don't know. Because you clicked that link, you have given approval for malware to download behind the scenes to your computer. Phishing sites are hosted on free servers scattered around the world, especially in Asia.

Rogue Security Software

Rogue Security software continues to be a problem. Rogue security software shows unusual alerts just to force the users to subscribe to the full version of their dubious software to remove the false threats. It is hard to suspect anything as the criminals behind it do everything within their power to make them look legit.

If you subscribe, they take your money and then discover backdoors on your computer. Through this backdoor, they can come and go as they please. If you are lucky, they may only be interested in advertising information. If you are unlucky, they may be looking for your bank information, your personal identity, and login details for websites.

It is not enough to just enable a firewall on your computer and by having the right security software. You need to make conscious efforts being selective of the software you download. You also need to avoid lesser-known security software, as any of them could be scareware.

Shally - About Author:

Welcome to share my tips, guide, tutorial articles about how to make your compute run more quickly . http://www.acebyte.com,http://www.acebyte.com/acebyte-utilities-functions.html http://www.acebyte.com/privacy-protect.html

Hope more and more readers like my articles and my articles can help you.

Article Keywords:
disk defrag, malicious software, rogue software, spyware, uninstall manager