How to fix a hijacked computer

Millions of computers have lost control of malicious hackers known as Cracker.

***TipsMake.com* - Your computer can cause a crime right now. Even if you read this article, malicious software can still be hidden somewhere on your computer without your knowledge. They will disrupt Web pages you visit or flood your inbox with advertisements. These are links that attack your computer and you may fall into this situation even though you haven't done anything wrong.**

Whether you call it a disconnected computer team or a botnet - a set of computers that have been attacked - this is still a bad thing. Millions of computers have lost control of malicious hackers known as Cracker. These crackers are always looking for ways to download and run some malicious software or malware. If you fall into their trap, it means your computer has been hacked.

What happens if your computer loses control - zombie? Zombie applications help crackers access your computer by attacking security holes or creating a back door. Once you have established administrative rights, he will control your computer. Some botnet applications also allow crackers to remotely control your computer. Some other software helps crackers access your personal information and steal that information.

One of the most popular botnet applications is spam distribution. Based on data from Symantec's MessageLabs, Cutwail botnet alone distributed 6.5% of all spam messages in February 2009. This means that innocent victims' computers have sent a lot of such messages to other people around the world.

Another botnet application is the distribution of denial of service attacks. First, the cracker will create a large botnet system by "lureing" the victim to run malicious software. Then, the cracker arranges an attack on a Web site's server at a given time. By the time of predetermined, botnet computers will simultaneously send messages to the target server. This sudden increase in Internet traffic will cause the Server to become unstable. Victims of attacks are often large firms, with a lot of visitors like CNN or Yahoo.

So, what do you do if you discover your computer is part of a botnet?

Recovered after being attacked by Botnet

Botnet applications often turn off programs that kill viruses and spyware. If your computer is slow, even if you don't use multiple applications at the same time, it means your computer is infected with zombies. Every time you visit a website that provides anti-virus or spyware programs, you always get errors or denial of service, and there are bad problems with your computer.

The best way to get rid of these botnet applications is really costly and time consuming: clean up your operating system and back up. have you backed up your hard drive? If not, you should regularly backup the drive in case something goes wrong.

If you have your own firewall software, you can block some applications that help someone access your computer remotely. Firewall acts as a filter between your computer and the Internet. Most firewalls have many security settings. First, install your firewall at the highest level of protection - this requires notification for any application that wants to access the Internet. Then restart your computer.

Also, pay attention to the requirements on your network. Write down the names of any applications you don't know, especially when you've just activated the application. Do not allow any application to look unreliable or you do not know how to access the Internet. If you get multiple requests for an application, that's the clearest sign of the intention to turn your computer into a zombie.

Not only that, you also have to do some research on the application-related Web to know if someone has identified it as malware. You will also have to find a list of files associated with the application and where you can find them on your computer. The only way to remove these files can help your computer get rid of malware. In fact, you can take steps a few times to be sure you have wiped them out - a small portion of malware can 'invite' other applications and programs to the 'party'.

Of course, this method is also a bit dangerous - you may unfortunately delete an important file that your operating system relies on to operate. It is better to completely wipe the computer than to find the infected files. However, the best advice is to avoid becoming a victim. Next, we will learn ways to help you avoid being turned into a part of the computer team that lost zombie control.

Avoid botnets and zombies

Refuse to download many antivirus and antispyware programs. These applications may be a source of attack and may make your computer handle other programs more slowly. They can also work together and make your operating system unstable. It is better to install only one application and stick with it.

Nobody wants to clean up their operating system and then have to perform a backup from the data copy, even if they only perform backups of some major parts. It is better to know what to be aware of and protect yourself before it's too late.

First, protect your system. Use password encryption for home networks as well as corporate networks. Install a firewall to prevent hacker attacks and pay attention to Internet traffic. Using a reliable antivirus and spyware program is not a bad idea either. You can find many types, copyrighted programs and free online applications.

Another way to protect your computer is to form a more careful Web access routine. Don't click on the random web links that you have never seen before. If you encounter a pop-up window asking you to download an antivirus software or claim that it will scan your computer for malware, do not click it. Usually, pop-up windows are scam - clicking that will help install malware on your computer.

Scam can attack you with many different lines, especially email. Therefore, you should avoid clicking on the links in the email. If you receive a notification from a bank that you do not have an account with, you should not click on any link because this is usually phishing scam for the purpose of extorting your money. Other scams try to trick you into clicking on the link with the promise of getting a big profit with just a little investment or even no investment at all. These things have been mentioned in previous articles like how hackers work, how phishing works, how trolls work . read these articles to better understand.

Finally, avoid suspicious sites, especially those related to unhealthy personal information, passwords or content. These addresses are bad guys online - accessing it is by handing malware to your computer. Today, many browsers will warn you if you try to access a famous address that has malware. Pay attention to these warnings - no matter what the content of the page is, it is not worth the cracker can access your computer.

If you keep your vigilance and Web access secure, you'll avoid having your computer become part of the zombie.