Volume #4 - Issue #184
November 2nd, 2018

This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to HomeCyberDefense.net to sign up.

Remote Access Trojans

A remote access Trojan (RAT) is a malware program that gives a hacker administrative control over your computer. (By the way, these are also known as Remote Administrative Tools in the world of tech professionals.) RATs are usually downloaded invisibly with a user-requested program such as an email attachment that you are tricked into open, a malicious website that you click from a search, an infected program that you download, or a game. Once the host system is compromised, the

hacker may use it to distribute more RATs to other users in your contact lists.

Because a RAT enables administrative control, it makes it possible for the hacker to do just about anything on the targeted computer, including:

• Monitoring user behavior through keyloggers or other spyware. In other words, it lets the hacker actually see what keys you press on your keyboard after a site asks for your password.

• Accessing confidential information, such as credit card and social security numbers.

• Activating your computer's webcam for recording video, which is possibly the scariest concept in that someone can be watching you through your computer.

• Taking screenshots or pictures with the webcam.

• Distributing viruses and other malware.

• Formatting your drives to obtain information or spread itself through your system

• Deleting, downloading or altering files and file systems.

What can you do about RATS? Well, first you have to find them. Here are four steps to take if you suspect you have a RAT:

1) View Processes Running
Right-click your Windows toolbar and select "Task Manager." Click the "Processes" tab in Task Manager. This window gives you a list of programs running on your machine. Review them for any strange names or names that you don't recognize as typical programs. If you don't recognize the

name, type it into Google. Several sites tell you if a process is malicious, so you know if you have a RAT on your system.

2) Odd Startup Programs
In some cases, the hacker might want another program to start when you boot your computer. If you notice any strange programs that start up when you boot your computer, you might have a RAT. These secondary programs are usually malicious software also, so you'll need to remove them when you remove the RAT.

3) View the List of Installed Programs
Open Windows Control Panel and view the list of programs installed on your computer. If you notice any odd programs, then it could be malicious. In fact, the popular software TeamViewer used to collaborate remotely with people is often used as a RAT. If you didn't install it on your computer, you should remove it. This application gives remote access to authorized and unauthorized people.

4) Pay Attention to Your Internet Speed
It's hard to quantify a slow Internet connection. If you normally have fast speeds but lately your Internet connection is extremely slow, you should first check the router and wireless connection. However, if the hacker is downloading information from your computer, he uses the bandwidth and creates noticeable lag on the network. If you suspect that someone is remotely accessing your computer, the fastest way to stop it is to disconnect from the Internet.

RATs are among the scariest attacks out there. They can make your computer, and anything it connects to, vulnerable. But it's the experience of watching your computer carrying out actions on its own that is truly unnerving. What is really eye opening is do a Google search for "Remote Access Trojans" and you will find all kinds of sites that actually teach you how to build one and get it distributed.

Thank you for subscribing to our email!

Home Cyber Defense Weekly

is a service of

House of File Technologies