Learn about hidden threats: Rootkit and Botnet

Attackers are always looking for the latest ways to access our computer system. The use of a hidden method such as rootkits and botnets is on the rise and you are more likely to become a victim

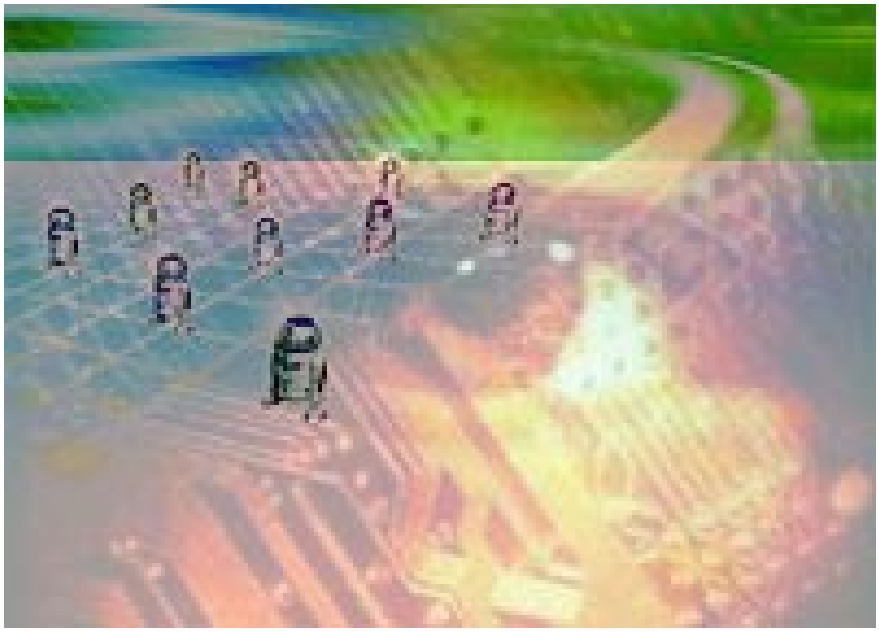
Attackers are always looking for the latest ways to access our computer system. The use of a hidden method such as rootkits and botnets tends to increase and it is easy for you to become a victim if you do not recognize and prevent it.

What is Rootkit and Botnet?

A rootkit is a piece of software that is installed and hidden on your computer without your knowledge. It may be in a larger software package or installed by an attacker, who has taken advantage of the vulnerabilities on the computer or knows that you have downloaded it (you can see more about Preventing attacks) public to steal your information for more information). Rootkits are not necessarily harmful to you, but they are dangerous in that they can hide their malicious activities. Attackers can access information and check your actions, change programs or perform other functions on your computer that you have not detected.

Botnet is a term provided from the idea of ??bot networks. Its most basic form, a bot is simply a computer program or a robot. In Botnet content, bots make computers can be controlled by someone or external sources. An attacker often gains control by infecting computers with a virus or other malicious code to give him access. Your computer can be part of a Botnet, even through it to perform normal operations. Botnets are often used to control activities from distributing spam and viruses to attacks denying DoS services.

Why are they regarded as threats?



The main problem of both is that they are hidden. Although botnets are not hidden like rootkits, we cannot detect them unless you search carefully and carefully. If a Rootkit has been installed, you may not know that your computer has been compromised, and traditional antivirus software cannot detect these malicious programs. Attackers also always create more sophisticated programs to upgrade themselves, making their programs even more difficult to detect.

Attackers can use Rootkit and Botnet to access and change personal information, attack other computers and may also be involved in other types of crimes, all of which are hidden in a way. secret. By using multiple computers, an attacker performs a series and affects their criminal acts. Because every computer in a Botnet can be programmed to execute the same command, an attacker can scan one of many computers to find vulnerabilities, check online actions or collect Important news when you enter in online forms.

How to protect yourself?

If you have a good habit, you can completely reduce the risks:

• Use and maintain antivirus software - Anti-virus software can identify and protect your computer against most of the detected viruses, so you can detect and delete these viruses. before it causes problems for you (see Learn about antivirus software). Because an attacker constantly writes new viruses, an important job for you is to update regularly for the virus tribute program. Some antivirus software vendors often provide anti-rootkit software.

• Firewall settings - Firewalls allow you to prevent many types of infections by blocking dangerous traffic before they can get inside your computer and traffic you send (see more articles). write about Learn about firewalls. Many operating systems often include it in the firewall, but you need to put it in enabled mode.

• Use good passwords - Choose good passwords to make it difficult for attackers, make them difficult to guess and use different passwords in different programs as well as devices. Do not select the option to save your password.

• Keep up-to-date with software - Install software patches so that an attacker cannot take advantage of known

issues or published vulnerabilities that harm you. Many operating systems provide upgrades automatically. If you have this option we recommend setting them up.

• Follow good security practices guidelines - Precautions should be taken when using email and browser to reduce unnecessary risks.

Unfortunately, if there is a Rootkit on the computer or an attacker is using your computer in a Botnet, you may not know about it. Even if you know that they are a victim, it is very difficult for ordinary users to remove them. An attacker can change some files on your computer, so simply deleting dangerous files may not solve this problem. If you believe that you are a victim, you should consider contacting a trained system administrator.

Due to the requirement, some software vendors are developing Rootkit eraser products and tools from your computer. If the software cannot locate and delete this infection, you may need to reinstall the operating system, usually a system recovery disk that is often created to provide a new computer. Note that reinstalling or restoring the operating system will delete all previous files and software that you have installed on your computer.