Rootkits - potential dangers

Have you ever heard of rootkits somewhere? You do not really understand what is a rootkit? Is rootkit a worm, virus or trojan? Are rootkits really dangerous? ... In this article, we will help you read n

Have you ever heard of rootkits somewhere? You do not really understand what is a rootkit? Is rootkit a worm, virus or trojan? Are rootkits really dangerous? . In this article, we will answer questions about rootkits, and introduce some free software to help you " *quickly defeat the* " rootkit. .

Rootkit concept

The rootkit concept is used to describe mechanisms and techniques used by malware (malware is software that falsifies application program functions including viruses, spyware, and trojans .) trying to hide , avoid being detected by programs that fight spyware, viruses and system utilities. In fact, rootkits themselves are not malicious, but when they are used with "destructive" programs such as viruses, worms, spyware, trojans . it is much more dangerous. a lot of.

How dangerous are rootkits?

Rootkits don't really cause any bad effects. The only purpose of rootkits is to hide, and avoid being detected. However, the rootkit used to hide malicious code is very dangerous. Some worms, viruses, trojans and spyware are still capable of being active and undetected when using rootkits. Malware will not be detected even when the system is protected by the best antivirus programs. Therefore, Rootkit is really a very serious threat.

In fact, there are currently only a few spyware and viruses that use rootkits to hide. One of the typical examples of using a rootkit to infiltrate the system is the theft of the famous game source Half-Life 2.

Rootkits are more commonly used in spyware than viruses. One thing is for sure, that rootkits are still technically evolving, not much in fact, so the current threat of rootkits is not very large compared to the potential dangers of this technique.

Rootkit classification

Rootkits are categorized based on maintenance after restarting or operating in user mode (user mode) or in system level mode (kernel mode).

Persistent Rootkit (Persistent Rootkits)

Persistent root kit is a type of rootkit that combines with other malware to function every time the system boots. Because malware containing malicious code will be executed automatically every time the system starts or when the user logs into the system. They need to store code executing programs in the Registry, system files and methods that allow silently running code that users don't know about.

Rootkit on memory (Memory-Based Rootkits)

This type of rootkit is that malware does not have "persistent" code - only stored in memory, so this type of rootkit does not exist after rebooting.

Rootkit user mode (User-mode Rootkits)

User-based rootkits use a variety of methods to hide undetected. For example, user-mode rootkit will block all functions that call the API (Application Programming Interface) system like: FindFirstFile / FindNextFile. These functions are called by Windows file manager programs such as Explorer and the command prompt, to list all system file directories. When an executable application lists directories and files that may contain rootkits, these rootkits will block these functions and change the output data results to remove rootkit files from the list. listed.

Windows system APIs provide interfaces between user mode and system service. More complex user-mode rootkits block system files, Registry, and functions that list processes from system APIs. Therefore, any detection by file scanning programs that get results from Windows API listing functions is changed. Therefore, most anti-virus and spyware programs cannot detect rootkits.

Rootkit mode (Kernel-mode Rootkits)

The kernel mode rootkit is more dangerous than the above, they not only block system APIs but also manipulate data structures directly in kernel mode. A common technique for hiding malware processes is to remove these processes from the list of processes in kernel mode. Because the API functions that manage processes must depend on the content in these data structures, so when the rootkit changes the content of the system data structure, the tools like Task Manager or Process Explorer detectable.

What malware uses rootkit technology?

Some Rootkits have the same meaning and properties of rootkits known as Hacker Defender and FU. Some spyware and advertising using rootkit: EliteToolbar, ProAgent, and Probot SE. Trojans like: Berbew / Padodor and Feutel / Hupigon and some worms like: Myfip.h and Maslan worm also use rootkits.

Predictions about rootkits

Rootkits have actually become popular among spyware and they will also gradually become popular in viruses and worms. Virus writers are now more professional and also work for business purposes. Therefore, they fully have the skills and qualifications to install very complex rootkits into viruses and worms.

Rootkits can make hidden trojans and spam longer on infected machines. This is also a cause for future rootkit booms.

Why do antivirus programs do not detect rootkits before they can hide?

This is true but only in some cases. Because rootkits are often spread by open source, this means hackers can quickly change the rootkit code so that antivirus programs cannot be detected. Some new anti-virus software that can detect rootkits such as F-Secure Internet Security 2005 feature Manipulation Control. This feature has a mechanism to block malicious "manipulating" processes from affecting other processes. However, F-Secure Internet Security 2005 only blocks a few rootkits.

Rootkit removal software

Rootkit when combined with malware becomes much more dangerous. So what software can detect rootkits hiding in the system?

Here are some software that can detect and destroy rootkits:

RootkitRevealer is a very effective and completely free rootkit search and removal program, with a capacity of only 190KB. The program has a simple interface, just press Scan button and RootkitRevealer will do its job. For more information and how to use the program effectively. You can read more information in the tutorial or visit the Website: http://www.sysinternals.com/utilities/rootkitrevealer.html

BlackLight is F-Secure's rootkit removal software. Currently, the beta version of BlackLight is free, download it at: http://www.europe.f-secure.com/exclude/blacklight/index.shtml

Minh Phuc