Title:
Rootkits – Hidden Hazards on Your System

Word Count:
558

Summary:
With the rootkit in place, the hacker has a virtual backdoor into your system. He can read your keystrokes, record passwords, gather information from your network and change your data and files.

Keywords:
rootkits, root kits, spyware, malware, viruses

Article Body:
If you're concerned about security on your computer network, there's a new word to add to your vocabulary – rootkit. A rootkit is a set of utilities installed on your computer whose purpose is to hide what other programs are doing. They've been around for a few years, but they didn't really hit the security spotlight until November 2005. That was when researchers discovered that some CDs from Sony were installing a rootkit on user computers as part of their DRM (Digital Rights Management) software. The purpose of the rootkit was to prevent the DRM software from being detected and uninstalled – but there was an unintended side effect. The rootkit opened a security hole on those computers that couldn't be detected by standard security software, and left them vulnerable to attacks by malicious software and hackers.

That's bad news for users and IT professionals who depend on virus and spyware detection programs to alert them to an invader on their networks. Generally, when you're computer is infected by spyware or malware , it can be detected by monitoring your computer activity. You can check the running processes and find programs that shouldn't be loaded. You can run a virus or spyware scanner to find registry keys and files that fit certain patterns. You can monitor activity coming in over a network.

A rootkit makes all of those defenses worthless by hiding the keys, files, processes and communications from your computer operating system. What your computer can't see, it can't report and you can't fix. The methods used to hide the files and processes vary and are getting more and more sophisticated. Most do it by 'hooking' into a process that Windows expects to find running, either by replacing the process files, or by adding itself into them.

With the rootkit in place, the hacker has a virtual backdoor into your system. He can read your keystrokes, record passwords, gather information from your network and change your data and files. A hacker with access to your system through a rootkit can reinstall hacking programs, access your accounts and your users' accounts and wreak general havoc. It's the ultimate Trojan backdoor.

Once a rootkit is installed, it's virtually impossible to detect and remove. When a virus detection or spyware program runs, they don't see the rootkit processes – they see the process that's cloaking it. Some may alter their own files with the details and stats associated with the files that they're replacing so that operating systems don't notice a difference. A sysadmin who is an expert in network security may be able to detect it by running system checks from an uninfected machine, but most agree that once a rootkit has been installed, the only way to be sure you've removed it is to wipe the drive clean and install the operating system.

Because rootkits don't install themselves, you can block them by blocking attempts to penetrate your network. One way to effectuate this is to install a spyware or malware protection program to help prevent rootkits from being installed at the server level or on individual desktops. The key is to practice excellent network security at all times so that you block the programs that install rootkits.

Article Provided By: http://spyware-removal.thrcomputer.com