A ROOTKIT: THE WORST MALWARE EVER

Of all the malware ever to infect millions of computers, the species known as the "rootkit" may well be the nastiest. Rootkits are very difficult to detect; even harder to find once their effects have been detected; and eradicating them can be difficult.

A rootkit is a stealthy form of malware that is designed to take control of the infected computer without the user's awareness. With a rootkit implanted in your computer, cybercriminals can use your system to commit crimes, transmit your private data to a bad guy, or use your computer to send spam emails. Rootkits can even lock you out of your own system, but typically they want to run undetected.

A rootkit is a type of malware package that is extremely difficult to detect and eradicate. That's because a rootkit actively hides itself from standard operating system tools like Task Manager and Windows Explorer. But even worse, rootkits often elude detection by popular anti-malware software. Once embedded in your computer, a rootkit may disable anti-malware programs or modify operating system components so that built-in security functions ignore the rootkit and whatever it does.

How can a computer become infected with a rootkit? There are many possibilities: Compromised websites, unpatched security holes in your operating system, vulnerabilities in application software; rogue anti-malware software, USB flash drives, and infected downloads from websites.

Because rootkits are meant to operate in stealth mode, it can be difficult to detect them on your computer. Since you typically can't see a rootkit, you can only infer the possibility of one from otherwise inexplicable or abnormal behavior on your system. **Some symptoms of potential rootkit infection include**:

- Your anti-virus program has been disabled.
- A spate of system crashes (the Blue Screen of Death) on a system that previously ran trouble-free.
- Random system slowdowns indicating that something invisible is consuming network or system resources. Task Manager's Performance or Networking tabs may indicate an unusually high level of CPU or network activity.
- Erratic behavior of input and pointing devices, i.e., mouse freezes, keyboard does not respond.
- You can't access certain Web sites, particularly sites devoted to security issues, or cannot open your Web browser at all.
- Unusual increase in network traffic; something is using your Internet connection without your knowledge.

Once the rootkit is active on your system, it can do all sorts of nasty things. Keystroke logging, password stealing, spam spewing, and monitoring of your activities are all possible. And worse, you may not realize that any of this is happening. If you sense that your computer or Internet connection is slower than it should be, or you notice any of the symptoms above, it's a good idea to scan for rootkits.

Removing a Rootkit

Eradicating a rootkit once it's entrenched in your operating system is very difficult. One possibility is to use a recovery disc, to return your system to its original "factory fresh" condition. It's a bit extreme, because you'll lose all your personal files, software that you've installed, and customized settings. If you have backup copies of your documents, photos and music, and installation media for your software, you could restore them after using the recovery disc.

But if you're doing regular full system backups, you could instead try restoring your system from a known good state. This is easier and less destructive than the full system wipe that a recovery disc will do. If you haven't been making backup images regularly, however, or you suspect the rootkit is also embedded in your disk image discs, then you can try a rootkit removal utility.

There are several free and paid products available. The following are from trusted sources and have achieved a good reputation for detecting and removing rootkits:

- Sophos Anti-Rootkit is a free, advanced rootkit detection program which can be operated from a friendly graphical interface or the command line.
- UnHackMe by Greatis Software is a highly-rated anti-rootkit utility. It can be a bit overwhelming for novice users, but if you read the wizard's somewhat technical instructions and follow them carefully, cleaning out a rootkit is a pretty straightforward process. UnHackMe is free to use for 30 days, and costs $34.90 to purchase.
- Kaspershy's TDSSKiller rootkit removal utility is a free download that's often recommended for disinfecting systems that have rootkits.
- Trend Micro Rootkit Buster scans your system's hidden files, registry entries, active processes, driver software, and can even detect Master Boot Record rootkits.

Beware of downloading rootkit removal utilities from any unknown third-party distribution site. The rootkit removal tool itself may be malware. Also, it's best to run multiple rootkit scanners on a system you suspect is infected. No anti-malware program catches everything.

Tips for Staying Safe

Since rootkits are sneaky and hard to detect, you might not even know if you've been infected. So preventing rootkits from installing themselves on your computer is the best strategy. To stay safe use a firewall, make sure your anti-virus software is up-to-date and periodically do a rootkit scan with one or more of the tools listed above.

It's also a good idea to use the Internet only from a *limited user account*, not from an administrator account. And finally, be careful what you download and click on!