Understanding Hidden Threats: Rootkits and Botnets

Original release date: August 24, 2011 | Last revised: February 06, 2013

Attackers are continually finding new ways to access computer systems. The use of hidden methods such as rootkits and botnets has increased, and you may be a victim without even realizing it.

What are rootkits and botnets?

A rootkit is a piece of software that can be installed and hidden on your computer without your knowledge. It may be included in a larger software package or installed by an attacker who has been able to take advantage of vulnerability on your computer or has convinced you to download it. Rootkits are not necessarily malicious, but they may hide malicious activities. Attackers may be able to access information, monitor your actions, modify programs, or perform other functions on your computer without being detected.

Botnet is a term derived from the idea of bot networks. In its most basic form, a bot is simply an automated computer program, or robot. In the context of botnets, bots refer to computers that are able to be controlled by one, or many, outside sources. An attacker usually gains control by infecting the computers with a virus or other malicious code that gives the attacker access. Your computer may be part of a botnet even though it appears to be operating normally. Botnets are often used to conduct a range of activities, from distributing spam and viruses to conducting denial-of-service attacks.

Why are they considered threats?

The main problem with both rootkits and botnets is that they are hidden. Although botnets are not hidden the same way rootkits are, they may be undetected unless you are specifically looking for certain activity. If a rootkit has been installed, you may not be aware that your computer has been compromised, and traditional anti-virus software may not be able to detect the malicious programs. Attackers are also creating more sophisticated programs that update themselves so that they are even harder to detect.

Attackers can use rootkits and botnets to access and modify personal information, attack other computers, and commit other crimes, all while remaining undetected. By using multiple computers, attackers increase the range and impact of their crimes. Because each computer in a botnet can be programmed to execute the same command, an attacker can have each of them scanning multiple computers for vulnerabilities, monitoring online activity, or collecting the information entered in online forms.

What can you do to protect yourself?

If you practice good security habits, you may reduce the risk that your computer will be compromised:

- **Use and maintain anti-virus software** - Anti-virus software recognizes and protects your computer against most known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date. Some anti-virus vendors also offer anti-rootkit software.
- **Install a firewall** - Firewalls may be able to prevent some types of infection by blocking malicious traffic before it can enter your computer and limiting the traffic you send. Some operating systems actually include a firewall, but you need to make sure it is enabled.
- **Use good passwords** - Select passwords that will be difficult for attackers to guess, and use different passwords for different programs and devices. Do not choose options that allow your computer to remember your passwords.
- **Keep software up to date** - Install software patches so that attackers can't take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Follow good security practices** - Take appropriate precautions when using email and web browsers to reduce the risk that your actions will trigger an infection.

Unfortunately, if there is a rootkit on your computer or an attacker is using your computer in a botnet, you may not know it. Even if you do discover that you are a victim, it is difficult for the average user to effectively recover. The attacker may have modified files on your computer, so simply removing the malicious files may not solve the problem, and you may not be able to safely trust a prior version of a file. If you believe that you are a victim, consider contacting a trained system administrator.

As an alternative, some vendors are developing products and tools that may remove a rootkit from your computer. If the software cannot locate and remove the infection, you may need to reinstall your operating system, usually with a system restore disk that is often supplied with a new computer. Note that reinstalling or restoring the operating system typically erases all of your files and any additional software that you have installed on your computer. Also, the infection may be located at such a deep level that it cannot be removed by simply reinstalling or restoring the operating system.

Author

Mindi McDowell