BRANDEFENSE
CYBER THREAT INTELLIGENCE

How to Uproot Rootkit Threats

Author: Threat Intelligence Team

Release Date: 26.05.2022

Report ID: TR29042022RK

Overview to rootkits

A rootkit is a malicious software program that gives an attacker unauthorized access to a computer or network. Rootkits can be used to gain root or administrative privileges on a system, allowing the attacker to install additional malware or steal sensitive data.

Rootkits are closely related to other malware types and typically installed by trojans, viruses, or other malware. The most distinctive features that distinguish it from other malware are an effort to persistence and stealthy.

Why do hackers use rootkits?

Hackers use rootkits to gain administrator-level privileges on a system, which they can then use to steal sensitive information, install other malware, or sabotage the system. Rootkits are difficult to detect and remove because they often disguise themselves as legitimate files or programs. Additionally, rootkits can persist even after a system has been rebooted, making them even more resistant to detection and removal.

Once installed, rootkits can hook into the operating system kernel and intercept system calls which allows them to hide from security scanners and other tools used to detect and remove malware. Rootkits can also disable security features on a system, such as an antivirus software.

Types of rootkits

We categorize rootkits based on where the attacker has injected them into the target computer system. Rootkit software can reside in an application, hardware/firmware, kernel, or bootloader (BIOS). The types of rootkits we describe below range from the easiest to infect the target system to the most challenging and complex to detect and remove.

Application

Rootkits that run in user mode by targeting applications or standard files that frequently run on the target system are also called User-mode rootkits. This type of rootkit can modify processes, network connections, files, and system services and is the only type that modern antivirus applications can detect.

Kernel

Such rootkits run in the operating system kernel and are also known as Kernelmode rootkits. This rootkit, which can run in the most privileged part of the operating system, aims to maintain the secrecy of the security breach with its ability to change the operating system as a whole.

Firmware/Hardware

Firmware is low-level software that controls computer hardware and runs directly on the hardware. Such rootkits can change hardware firmware such as CPU, GPU, hard disk, and network cards.

Bootkits

Bootloader, which we also call Boot Manager or Bootstrap Loader, is a program responsible for booting the system. Bootkits are designed to be loaded into the boot process as early as possible to control all the startup stages of the operating system and replace system code and drivers before antivirus and other security components are loaded. Bootkits are loaded from the Master Boot Record (MBR) or boot sector.

Infection methods

Rootkits' methods of infecting the target system vary according to rootkit types.

User-mode rootkits are often part of other malware and are distributed through typical infection methods such as phishing/social engineering and unpatched security vulnerabilities.

Bootkits can be infected by booting the operating system using malicious driver software.

Rootkits have a significant disadvantage. The higher the degree of danger (see rootkit types, respectively), the more difficult it becomes to install on the system. Sometimes, rootkits can also be installed manually by malicious people or thirdparty people that we call **Insiders**.

Threat actors which use rootkits

Below are some of the well-known threat actors that use rootkits in their operations.

- APT28
- APT41
- Warzone RAT (MaaS)
- TeamTNT
- Stuxnet

Mitigation

Rootkits are not easily mitigated in preventive checks because they misuse system features. However, you can protect yourself against rootkit threats by paying attention to a few fundamental issues.

- Keep your operating system and software up to date. Attackers often exploit known vulnerabilities to install rootkits. By keeping your system up-to-date, you can reduce the risk of these exploits being successful.
- Use a reputable antivirus program and scan your system regularly. Antivirus programs can detect and remove rootkits, but they need to be kept up-to-date in order to be effective.
- Be cautious when downloading files from the internet. Only download files from trusted sources, and be sure to scan them with an antivirus program before opening them.
- Don't click on links or open attachments in emails unless you are certain of their source. Emails are a common way for attackers to deliver rootkits.

Detection

Signature-Based

It is one of the most widely used methods for detecting malware threats and can also be used to detect rootkits. However, the detection rate is low as it can only be used to detect the presence of previously detected rootkits in the system.

Behaviour-Based

It is possible to detect abnormal behaviors in the target system according to heuristics and behavior patterns. We can derive specific patterns by examining the potential activities of the rootkits seen so far. The advantage of this method over the Signature-Based detection method is that it can detect previously unknown rootkits.

Diff-Based

The diff-based detection method is generally used to detect kernel-mode rootkits. The basic approach in this method is to compare two different system views. The first view shows a clean system installation with the usual data structures. By comparing the second view taken by the rootkit detector with the first view, the changes/differences in the data structures are revealed. Detecting a difference indicates the presence of a rootkit.

Integrity Check

It works similarly to a diff-based check, but Integrity Check is used to check for unauthorized changes to system files. First, the hash value of each system file is calculated as a basis for showing that the system is clean. Then, when needed, the system's current state is compared with the hash values in its previously used base state.

Conclusion

Rootkits are a type of malware that can be difficult to detect and remove. They are designed to gain access to a computer system and then conceal their presence in order to avoid detection. Rootkits can be used to give an attacker control over a system, steal sensitive information, or launch attacks on other systems.

If you suspect that your system may be infected with a rootkit, it is important to seek professional help to remove the malware and secure your system. In most cases, a rootkit can be removed only by rebuilding the compromised system.