What is a Rootkit?

A rootkit is a harmful software tool or program that allows a threat actor to take remote control of and access to a computer or other system. While there are actual applications for this kind of software, such as remote end-user support, the majority of rootkits create a backdoor on victims' computers so that harmful programs, such as viruses, ransomware, keylogger programs, or other malware, can be introduced or the system can be used as a platform for additional network security attacks. Rootkits commonly try to stop antivirus and endpoint antimalware software from detecting harmful software.

Rootkits are available for purchase on the dark web. They can be used as a social engineering technique that deceives users into granting permission for the rootkits to be placed on their systems, or they can be installed as part of scams. Once installed, the rootkits typically grant remote attackers admin rights to the system. A rootkit grants the remote actor access to and control over nearly every feature of the operating system (OS) once it is installed. While most antimalware programs can now search for and remove rootkits hidden within a system, older antivirus programmers sometimes have difficulty identifying rootkits.

What Can a Rootkit Do?

Malicious software called a rootkit is created to covertly take over a computer or network and get illegal access and control. To evade discovery, it has the ability to change kernel functions, change system processes, and get around security measures. Attackers may be able to monitor user activities, steal confidential data, and run more malware with the help of rootkits. They are especially difficult to find and eliminate as they have the ability to change system settings in order to retain persistent access. Rootkits pose serious security hazards because they threaten the integrity of operating systems and applications by thoroughly embedding themselves into the system.

Rootkit Protection

- **Antivirus and Anti-Malware Software:** Use the most recent versions of antivirus and anti-malware software to identify and get rid of rootkits. Certain security tools include capabilities designed specifically to identify rootkits.
- **Regular System Updates:** To fix security holes that rootkits may exploit, make sure your operating system and apps are up to date.
- **Behavior-Based Detection:** Make use of software designed to keep an eye on anomalous system activity, since this may point to the existence of a rootkit.
- **System Integrity Checks:** To identify unauthorized modifications, periodically confirm the accuracy of system files and settings.
- **Least Privilege Principle:** Limit user rights in accordance with the least privilege principle to lessen the possible impact of a rootkit.

Well-Known Rootkit Examples

- **Stuxnet:** An advanced rootkit that manipulates industrial control systems to undermine Iran's nuclear program.
- **Alureon (TDSS):** Known for its capacity to aviod detection and alter system operations, Alureon (TDSS) is frequently utilized for financial theft and the construction of botnets.
- **Zeus:** Mostly a banking Trojan, Zeus has the ability to conceal its existence and keep control over compromised computers by utilizing rootkit technology.

- **Rootkit.Reveton:** A rootkit for ransomware that poses as law enforcement and demands ransom payments.
- **Carberp:** Known for its ability to steal data and operate stealthily, it frequently targets financial data and uses rootkit tactics to evade detection.

How Rootkits Work?

- **Privilege Escalation:** In order to obtain more privileges and a deep degree of system control, rootkits frequently take use of security holes or social engineering techniques.
- **Installation:** The rootkit installs itself and becomes deeply ingrained in the system when access is obtained. To stay in control, it could alter firmware, kernel modules, or system files.
- **Hiding Techniques:** Rootkits employ a number of strategies to evade discovery. These include intercepting system calls to evade detection by security software and concealing files, processes, or registry entries.
- **Persistence:** Rootkits make sure they don't stop working when the system restarts. They may change system settings to load at boot, or they may install themselves in startup places.
- **Nefarious Activities:** They may carry out a number of malicious tasks, such as data theft, user activity monitoring, and the introduction of new viruses, when they have root access.

What Can be Compromised During a Rootkit Attack?

- **System Integrity:** Rootkits can alter or corrupt system files and configurations, affecting the stability and reliability of the operating system.
- **Sensitive Data:** Personal information, financial details, and confidential documents can be stolen or manipulated by rootkits.
- **User Privacy:** Rootkits can monitor and record user activity, capturing keystrokes, screenshots, or other private information.
- **Network Security:** They can create backdoors for remote access, compromise network communications, or launch attacks on other systems.
- **System Performance:** Rootkits may degrade system performance by consuming resources or interfering with normal operations.

Symptoms of Rootkit Infection

- **Performance Issues:** Sluggish system performance, unexpected slowdowns, or frequent crashes.
- **Unusual Network Activity:** Unexplained network traffic or connections to unknown or suspicious IP addresses.
- **System Instability:** Frequent system errors, crashes, or unexpected reboots.
- **Altered Files:** Unexpected changes to or disappearance of files, or altered system configurations.
- **Unrecognized Processes:** Suspicious or unknown processes running in the background, which may not be visible through standard task managers.

Tips for Preventing a Rootkit Attack

- **Keep Software Updated:** Regularly update your operating system, applications, and security software to patch vulnerabilities.

- **Use Reliable Security Tools:** Install and maintain reputable antivirus and anti-malware software that includes rootkit detection capabilities.
- **Enable Automatic Updates:** Configure your system and applications to automatically install updates and patches.
- **Practice Safe Browsing:** Avoid clicking on suspicious links, downloading unknown files, or visiting untrusted websites.
- **Implement Least Privilege:** Use user accounts with minimal privileges and avoid operating with administrative rights unless necessary.

How Rootkit Functions?

Rootkits are unable to spread on their own, thus they must infect systems through covert techniques. When unaware consumers allow rootkit installer programs to install on their systems, the rootkits install and remain hidden until hackers activate them. Rootkits contain malicious software such as banking credential stealers, password stealers, keyloggers, antivirus disablers, and bots used in distributed denial-of-service attacks.

Rootkits are installed using the same common vectors as other malicious software, such as email phishing campaigns, executable malicious files, crafted malicious PDF or Microsoft Word documents, connecting to compromised shared drives, or downloading rootkit-infected software from risky websites.

Why are Rootkits so Dangerous?

- Rootkit viruses can spread using misleading threat vectors such as faulty downloads, spam emails, and exploit kits. Some rootkits even use Trojans such as Perkier malware to compromise a system's security.
- They are stealthy With other types of malware, a deeply hidden rootkit will not produce many symptoms. It may even avoid your security software, making it difficult to fix. Some rootkits can only be destroyed by formatting the storage disc and restarting the operating system.
- They are eligible Rootkits, also referred to as the "Swiss Army Knives of Malware" by some specialists because of their flexibility. Some rootkit tools can steal login credentials and financial information, disable security protocols, log keystrokes, and perform other functions. Other rootkits allow a hacker to get backdoor access to a machine and install more software. With the correct rootkit, a hacker can convert a system into a bot and form a botnet to launch DDoS (Distributed Denial-of-Service) assaults on websites.

Types of Rootkits

Bootloader rootkit

When you switch on a computer, the bootloader loads the operating system. A bootloader rootkit infiltrates this mechanism, infecting your machine with malware before the operating system is ready for use. Bootloader rootkits are less of a threat currently, because of security mechanisms such as Secure Boot.

Firmware rootkit

Firmware is a sort of software that gives basic control over the hardware it is designed for. Firmware can be found on a wide range of equipment, including mobile phones and washing machines. A firmware rootkit is difficult to detect because it hides in firmware, where most cybersecurity tools do not look for malware.

Kernel Rootkits

The kernel of your operating system functions similarly to the nervous system. It's a key layer that helps with essential tasks. A kernel rootkit can be disastrous since it targets a critical component of your computer and grants a threat actor significant control over the system.

Memory rootkit

Memory rootkits live in your computer's RAM and can slow down your system while doing malicious functions. You can usually erase a memory rootkit by restarting your computer, as this clears all processes from your machine's memory.

Application rootkit

An application rootkit may replace your ordinary files with rootkit code, granting the rootkit creator access to your machine each time you execute the infected files. However, this sort of malware is easier to detect because files containing rootkits can act abnormally. In addition, your security tools have a better chance of detecting them.

Examples of Rootkit Attacks

Phishing and social engineering attacks: Users who read spam emails and unintentionally download malicious software put their PCs at risk of becoming infected with rootkits. Rootkits also employ keyloggers to obtain user login information. A rootkit, once installed, can allow hackers to access sensitive user information and take control of computer operating systems.

Application rootkit attacks: Rootkits can install themselves on widely used programs, such as word processing and spreadsheet programs. Hackers employ application rootkits to acquire access to users' information every time they open infected programs.

Network and Internet of Things (IoT) attacks: IoT devices and edge computing present significant security risks since they lack the security protections that other systems and centralized computers use. Hackers discover and attack these flaws by adding rootkits through vulnerable points of entry. This allows a rootkit to travel throughout a network, taking over PCs and workstations and turning them into zombie machines under external control.

OS attacks: After getting into a system, a kernel mode rootkit can launch an attack against the operating system. The assault may involve changing OS functionality, decreasing system performance, and potentially accessing and deleting data. Kernel mode rootkits often break down systems when a user accidentally opens a malicious email or runs a download from an untrusted source.

Credit card swipe and scan attacks: Criminals infected credit card swipers and scanners with rootkits. The rootkits are designed to collect credit card information and deliver it to servers controlled by hackers. To address this, credit card companies have implemented chip-embedded cards, which are more robust to attacks.

Popular Rootkit Examples

- Lane Davis and Steven Dake wrote the first known rootkit in the early 1990s.
- NTRootkit was one of the earliest malicious rootkits targeting the Windows operating system.
- HackerDefender - this early Trojan modified/augmented the OS at the lowest level of function calls.
- Machiavelli, the first rootkit for Mac OS X, was released in 2009. This rootkit generates covert system calls and kernel threads.
- Greek wiretapping, In 2004/05, attackers built a rootkit that targeted Ericsson's AXE PBX.

- Zeus, discovered in July 2007, is a Trojan horse that steals financial information using man-in-the-browser keyboard tracking and form capture.
- Stuxnet is the first known rootkit for industrial control systems.
- Flame is a computer malware that was found in 2012 that infects machines using the Windows operating system. It can capture audio, screenshots, keyboard activities, and network traffic.