ROOTKITS

By Alena Durel

WHAT IS IT?

Allows a malicious entity to gain privileged administrator access to a user's computer

Often hides within other processes running on the computer

Used primarily to cloak and protect other malware

Can be used to disable security software, install and hide a keylogger, steal data, even use your computer as a botnet for a distributed denial-of-service (DDoS) attack

TYPE OF VULNERABILITY

- A rootkit is a malicious program that can be used as a delivery method to distribute malware onto a computer, and is not necessarily classified as malware or a virus itself
  - Rootkits can introduce malware and spyware to a system, and could turn it into part of a botnet
- It is often delivered by tricking the end-user with social engineering and phishing schemes

HOW DOES IT WORK?

1. Rootkits are often delivered through phishing schemes, coupled with other malware, or through corrupted download links (typically from suspicious third-party websites)

2. Dropper: Delivers the rootkit to the system which starts the loader once the victim activates the dropper

   Loader: Installs the rootkit onto the device, often using a buffer overflow to place the rootkit in otherwise inaccessible memory

3. Once the rootkit has been delivered, it gives the hacker unlimited access to the host system, normally only given to the system's admin account

4. Rootkits use the concept of *modification*, which locates and changes certain software, allowing them to introduce malicious code or spyware into the system

"What Is a Rootkit and How to Remove It?", Avast

"The Basics of Rootkits: Leave No Trace", informIT

DIFFERENT TYPES OF ROOTKITS

Firmware	Targets the firmware of the device instead of the operating system (OS) and can affect the hard drive and BIOS (used to start the system and manages data flow)
Bootloader	Replaces the system's bootloader with an infected one which activates the rootkit before the OS is fully loaded
Memory	Lives in random-access memory (RAM) and can greatly affect RAM speeds, however, it is short-lived

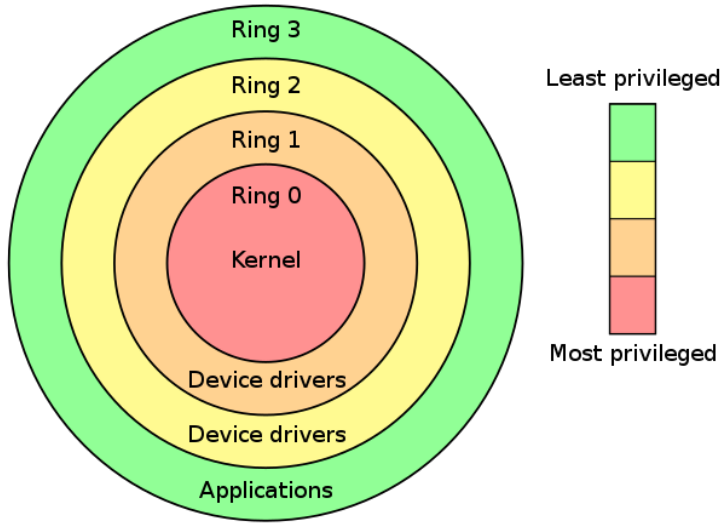
"What is Rootkit – Definition and Explanation", Kaspersky

DIFFERENT TYPES OF ROOTKITS

Application	Replaces files with rootkit files and allows the hacker to access your computer every time you open an infected application (i.e., Word, Notepad, Paint)
Kernel	Perhaps the most dangerous rootkit as it target the very core of the system and can not only access files, but also change how the OS functions
Virtual	Hosts the target system as a virtual machine (VM) and is able to subvert the OS without modifying the kernel

"What is Rootkit – Definition and Explanation", Kaspersky

- Intel x86 microchips have 4 rings of access control, although most operating systems only use Rings 0 and 3
  - The lower the ring, the less access restrictions there are, making kernel rootkits significantly more dangerous
  - There are some specific instructions only available in Ring 0 as they can alter the CPU's behavior of access the hardware
- Hardware rootkits affect the hardware and the BIOS of a system, which can drastically change the way a computer functions
- Memory rootkits can significantly slow down RAM speeds



ARCHITECTURE

HOW CAN IT BE FIXED?

- It is extremely difficult to spot a rootkit installed on your PC
  - Look for strange behavior on your computer such as programs not running smoothly or being extremely slow to load
  - Run rootkit removal software
  - Run a boot-time scan
- If these fail, the best option might be to back up your data and perform a clean install of the operating system

"What Is a Rootkit and How to Remove It?", Avast

HOW CAN IT BE PREVENTED?

Install antivirus software and keep your computer and applications up to date

Be alert to phishing schemes and educate yourself on what they might look like

Do not click on untrusted links or download files sent be people that you don’t know

Be wary of unreliable websites and drive-by downloads

“What is a Rootkit? And How to Stop Them”, Norton

SHOULD WE BE CONCERNED?

- Rootkits take both time and money to develop and as such would likely warrant a high-end target
  - Often target large companies such as telecommunications and financial companies
  - Can also be used target individuals such politicians and other high-ranking officials
- Rootkit attacks are also declining as security systems improve defenses and many newer CPUs offer built-in kernel protection

"How Does Rootkit Work?", N-ABLE

"Almost Half of Rootkits are Used for Cyberattacks Against Government Organizations", ZDNet

The Basics of Rootkits: Leave No Trace. InformIT. (n.d.). Retrieved March 29, 2022, from https://www.informit.com/articles/article.aspx?p=408884&seqNum=5

Burdova, C. (2022, February 23). *What is a Rootkit and How to Remove it?* Avast. Retrieved March 29, 2022, from https://www.avast.com/c-rootkit

How Does Rootkit Work? N-ABLE. (2019, July 10). Retrieved March 29, 2022, from https://www.n-able.com/blog/how-does-rootkit-work

Kaspersky. (2022, March 9). *What is Rootkit – Definition and Explanation*. Kaspersky. Retrieved March 29, 2022, from https://www.kaspersky.com/resource-center/definitions/what-is-rootkit

Osborne, C. (2021, November 3). *Almost Half of Rootkits are Used for Cyberattacks Against Government Organizations*. ZDNet. Retrieved March 29, 2022, from https://www.zdnet.com/article/almost-half-of-rootkits-are-used-to-strike-government-targets/

Rafter, D. (2020, April 30). *What is a Rootkit, and How to Stop Them*. Norton. Retrieved March 29, 2022, from https://us.norton.com/internetsecurity-malware-what-is-a-rootkit-and-how-to-stop-them.html

Ring zero. Ring Zero | Rootkits: Subverting the Windows Kernel. (n.d.). Retrieved March 29, 2022, from https://flylib.com/books/en/1.242.1.37/1/

What are Rootkits and Why are They Bad News for Your PC? SOPHOS. (2019, December 29). Retrieved March 29, 2022, from https://home.sophos.com/en-us/security-news/2019/what-is-a-rootkit

REFERENCES