Exploring Attacks on Availability: Rootkits

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 200T: Cybersecurity, Technology, and Society, Professor Chris Brown

April 5, 2025

Assignment:

In this assignment, you will research and analyze different types of cyberattacks that target the availability of systems, networks, or data, which is one of the core principles of cybersecurity. Known as "Attacks on Availability," these are incidents where malicious actors attempt to disrupt access to critical resources, making them inaccessible to users. Such attacks can include Distributed Denial of Service (DDoS), ransomware, and other forms that focus on hindering legitimate access.

Objective:

You are tasked with providing a concise summary of a specific attack on availability. Use recent online sources to explore how these attacks occur, their impact on organizations, and possible defenses. Be sure to **cite at least one reputable** source to support your analysis.

In your response, address the following:

- Define what is meant by an "attack on availability."
- Describe a recent example of such an attack or a common technique used in these attacks.
- Briefly discuss the broader implications of these attacks on organizations and users.

Exploring Attacks on Availability: Rootkits

"Attacks on availability" refer to cyberattacks aimed at disrupting and preventing authorized users from accessing systems, networks, or data. One powerful malware method is a rootkit, a stealthy type of malware that grants attackers privileged access to a system while concealing its presence, often disabling or disrupting critical functions (Fortinet, 2025).

What are Rootkits? How Do They Work?

Rootkits seek the highest permissions, such as administrative-level control over a given computer system, without being detected. Computer systems usually have different rings or levels of permission, ranging from Ring 3 to 0, with Ring 3 being the Outmost Ring and Ring 0 being the innermost and highest permission level (Kaspersky, 2025). Operating in Ring 0 is also called the "kernel/root mode" or "kernel/root level": operations in this level allow a person to control access to device drivers, sound cards, and video displays like monitors. Administrative permissions can also include installing, deleting, and modifying programs, including opening, shutting down, and adjusting the filters of ports on those systems. Advanced rootkit techniques include Dynamic Link Libraries (DLL) Injection and placing a "Shim" or piece of software code between two host components, allowing the malicious code and users to intercept calls or commands between them and redirecting them to the software code's desired location. Therefore, the closer one is to the kernel, the more permissions and power one will have to change a network from the inside out.

Implications for Organizations and Users

The broader implications for organizations are severe. Rootkits can evade detection, leading to prolonged disruptions, data corruption, or system crashes, costing businesses operational potentially $300,000 to $1 million per hour for large enterprises—and compromising

sensitive data (Timilsaina, 2023). That translates to inaccessible services or devices for users, as rootkits can render systems unusable until eradicated, like the 2005 Sony BMG Rootkit scandal. Another example occurred in 2023; the "Horabot" campaign targeted Latin American organizations with a rootkit-enabled banking trojan. The attackers delivered the malware via phishing: an authorized account user clicked on malicious links, downloading the malware onto their systems where the malware deeply embedded itself in the network's systems. The malware allowed attackers to manipulate or disable services, effectively denying availability to legitimate processes.

Defenses & Remedies

Rootkits are extremely difficult to detect and remove because they operate at a system and network's kernel/root level. The OS is “blind” to these forms of malicious code, unable to detect what is outside its “line of sight” or system environment. There are various signs or warnings that show a system, or network is infected with a rootkit. If you are experiencing system crashes, software malfunctions, antivirus deactivations, or crashes, it is wise to scan to search for rootkit malware (Malwarebytes, 2025).

The best way to ***prevent*** rootkits is through a combination of different techniques. Some techniques include (1) implementing advanced endpoint detection tools to identify anomalies or suspicious user behaviors, (2) maintaining regular system updates to patch vulnerabilities, and (3) using secure boot processes to prevent unauthorized code from execution (Microsoft, 2022). Regular backups and integrity checks also help organizations recover swiftly, minimizing the impact of these covert, availability-threatening attacks. However, when attempting to quarantine and remove the Rootkit, one must first temporarily TURN OFF System Restore and routine backups to prevent the Rootkit from persisting or spreading through these mechanisms.

After administration verifies that the Rootkit is cleansed and removed from the system and network, the user or administrator may create a new clean restore point and enable routine backups again.

Lastly, the best way to ***remove*** rootkits is to boot from an external device (like a USB drive or External Hard Drive) and then scan the internal drive(s) to ensure that you can detect those rootkits. Using a qualified, dependable, and objective third-party device and antivirus program to scan within and without the OS system of your infected device will increase your chances of completely removing the Rootkit from your infected device(s) (Fortinet, 2025).

References

Fortinet. (2025, March 31). *What Is A Rootkit?* Retrieved from Fortinet: https://www.fortinet.com/resources/cyberglossary/rootkit

Kaspersky. (2025, March 30). *What is Rootkit – Definition and Explanation*. Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-rootkit

Malwarebytes. (2025, March 28). *Rootkit*. Retrieved from Malwarebytes: https://www.malwarebytes.com/rootkit

Microsoft. (2022, November 25). *What is a Rootkit?* Retrieved from Microsoft: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-a-rootkit

Sam, C. (2023, April 5). *Malware Basics: Rootkits*. Retrieved from Medium: https://medium.com/@samuel.i.steers/malware-basics-rootkits-9fd7def6e515

Timilsaina, B. (2023, December 28). *Common Types of Rootkits Attacks with Worst Examples of All Time*. Retrieved from BinaryIT: https://binaryit.com.au/types-of-rootkits-attacks-with-examples/