History and Overview on the Impact of RootKits

Sebastian Stovall

CYSE600

06-02-2024

Introduction

Rootkits can be one of the most complex and hard to detect malware programs to deal with. They can perform functions such as modifying files, and hiding processes, all while being completely hidden, making them a vital tool for hackers. As such, understanding how this malware works and how to detect it is evidently important in the cybersecurity field.

Article reviews

Name of Article	Review
Matrosov, Rodionov, E., & Bratus, S. (2019). *Rootkits and bootkits reversing modern malware and next generation threats* (1st edition.).	Provides multiple case studies involving several types of rootkits and how they attacked different systems. Also contains a brief overview on rootkits and how they can be detected
Elisan, Davis, M. A., Bodmer, S. M., & Lemasters, A. (2017). *Hacking Exposed Malware and Rootkits: Security Secrets & Solutions, Second Edition* (Second Edition). McGraw-Hill/Osborne.	Provides a detailed overview of rootkits and their history, gives oriented background on how rootkits started off as a normal tool for users and become abused as a form of malware. Also provides a timeline on rootkit history

Analysis

Rootkit technology is used primarily to elevate privileges on an operating system. Rootkits are classified into types based on where they are in an operating system. "This escalation provides attackers with two major features that are quite useful when conducting an attack campaign against a target: Maintain access and Conceal existence through stealth" (Hacking Exposed Malware and Rootkits). The types include firmware rootkits, application rootkits, memory rootkits, boot-loader rootkits, and kernel mode rootkits. Kernel Mode rootkits operate at the kernel level of the operating system, providing it with the most control over an OS.

In 1999, the first malicious rootkit was established, called NT Rootkit, which targeted Windows systems. These rootkits later evolved into complex systems such as a new form that began to steal people's financial data in 2008. The system would install keyloggers into people's computers and obtaining their log-in credentials. The malware, later named Mebroot, was also "Invisible to all anti-rootkit and anti-malware utilities, including those from leading security and antivirus vendors, this rootkit downloaded malware that logged all keystrokes typed into the computer." (Hacking Exposed Malware and Rootkits). This Rootkit would then be spread through websites created to spread the virus, including pornographic and illegal sites. Eventually however a mitigation strategy was found, "the easiest way to remove it was to run the fixmbr command from within the Windows recovery console, which was available by booting the Windows XP CD (included with all Windows installations). This overwrote the rootkit's entry on MBR with a standard Windows MBR. Also, some of the latest BIOS settings allowed users to make the MBR read-only. If set to read-only, any modification to the MBR caused a BIOS warning." (Hacking Exposed Malware and Rootkits).

MebRoot's story led to a new era of Rootkit's being developed. Bypass tools have been built using software taken from old MebRoot systems to learn how to detect similar Rootkits in Operating systems. Mitigation strategies such as keeping systems updated, and being cautious online are two examples of lessons that can be taken from the MebRoot virus. Rootkits are a more robust type of malware that require keen attention to detail in order to be discovered and maintained, and it is the responsibility of cybersecurity professionals to develop new strategies against this malware.

Work's Cited

Elisan, Davis, M. A., Bodmer, S. M., & Lemasters, A. (2017). *Hacking Exposed Malware and Rootkits: Security Secrets & Solutions, Second Edition* (Second Edition). McGraw-Hill/Osborne.

GeeksforGeeks. (2022, November 2). *Types of rootkits*. https://www.geeksforgeeks.org/types-of-rootkits/

Matrosov, Rodionov, E., & Bratus, S. (2019). *Rootkits and bootkits reversing modern malware and next generation threats* (1st edition.).

Wikimedia Foundation. (2024, April 29). *Rootkit*. Wikipedia. https://en.wikipedia.org/wiki/Rootkit#:~:text=The%20first%20malicious%20rootkit%20for,programmable%20logic%20controllers%20(PLC).