ABSTRACT

The rapid development of information technology not only provides convenience for users but also introduces various cybersecurity threats, such as the spread of malware. One of the most dangerous types of malware is the Remote Access Trojan (RAT), which allows attackers to remotely control a victim's system without their knowledge. This study aims to analyze the behavior of the ramez.exe malware, which executes the remcos.exe payload, using the Memory Forensics and YARA Rules methods to comprehensively understand its characteristics, activities, and operational patterns. The research employed a qualitative descriptive approach by conducting digital forensic analysis on a malware sample through two main stages: memory analysis (runtime analysis) using the Volatility Framework, and static pattern analysis (signature-based analysis) using YARA Rules. The analysis was carried out based on 16 research parameters, including process activity, network connections, registry modifications, file artifacts, unique strings, external domains, and the internal structure of the malware. The results show that ramez.exe functions as a dropper executing the remcos.exe payload, running in the background of the operating system, and connecting to the IP address 147.185.221.26:40252, located in Carson, United States. Based on Memory Forensics analysis, malicious process activities such as system injection, creation of child processes, registry modification, and persistence mechanisms were identified, ensuring that the malware remains active after a system restart. Meanwhile, the YARA Rules analysis successfully detected critical strings and patterns such as rmclient.exe, sysinfo.txt, dxdiag, cmd.exe, image/jpeg, and http://geoplugin.net/json.gp, indicating the malware's ability to collect system information, execute remote commands, and communicate covertly with an external server. Overall, it can be concluded that the Memory Forensics and YARA Rules methods complement each other in the malware analysis process. Memory Forensics is effective in detecting dynamic artifacts that occur in memory, while YARA Rules excels at identifying static artifacts and the internal structure of files. The combination of both methods provides a comprehensive and in-depth analysis of the behavior of ramez.exe, which is categorized as a Remote Access Trojan (RAT).

***Keywords**: Memory Forensics, YARA Rules, Malware, ramez.exe, Remote Access Trojan (RAT).*