Abstract

Ransomware is a type of malicious software capable of disabling computer functions or encrypting all files, resulting in significant disruption. This research dynamically analyzes ransomware behavior on the Windows 11 operating system. Several ransomware samples were executed and analyzed to obtain a list of ransomware behaviors used for performance testing on the samples. This topic is important as ransomware attacks have increased significantly and become one of the most destructive cyber threats. Ransomware attacks have caused major disruptions to services such as BSI banking, making it crucial in this digital era to understand the behavior of suspicious files or processes and how to mitigate such threats.

This study conducts dynamic analysis of ransomware behavior on the Windows 11 operating system. In an isolated environment using Virtual Machines (VMs), this research employs tools such as Process Monitor, Wireshark, and ProcDOT to collect data and visualize ransomware behavior. The results of this study include the compilation of a list of ransomware behaviors used to build a detection system that can identify samples based on detected behaviors. The developed detection system shows a good detection rate, which has a detection percentage of 69%. These results show significant potential in identifying ransomware threats, although there is still space for improvement and further development.

Keywords: behavior, cybersecurity, detection system, dynamic analysis, ransomware