A Study for Decrease False Positive and False Negative Antivirus Technique in File Partial Encryption

In Hoe Ku, Sang-Hoon Choi, Ki-Woong Park*

SysCore Lab, Sejong University, Seoul, 05006, South Korea
22110624@gsju.ac.kr,csh0052@gmail.com
Department of Information Security, Sejong University, Seoul, 05006, South Korea
woongbak@sejong.ac.kr

Keywords: AntiVirus, Ransomware, FalsePositive, FalseNagative, File Partial Encryption

Abstract

Antivirus is a solution for detecting and stopping software that performs malicious behavior on a computer system. Antivirus work on a signature basis, which is a blacklisting approach to detecting malware by collecting suspected file binary and behavior of process to extract unique features, and compare them to a rule set of unique features stored in a database. However, recent ransomware has exposed the limitations of signature-based antivirus. Ransomware is malware that executes process, seek file location, read file, encrypt file binary, overwrites, or delete original files after creation, as shown in Figure 1. In addition, the number of variants of ransomware is increasing fast due to the recent rise of the Ransomware-as-a-service(Raas) industry [1, 2]. This growing trend has limited the ability of traditional antivirus signature-based protection to detect and combat variants [3, 4]. Ransomware and legitimate processes both read and write to files, causing changes to the data in the file, making it difficult to distinguish between the maliciousness of a specific behavior. This can be time-consuming and hard to observe closely as the damage becomes more difficult to recover. This is because antivirus is not able to identify precise enough precursors to determine that a suspect's behavior is ransomware. Of particular note, recent ransomware has utilized "file partial encryption" techniques to increase the speed of encryption and evade antivirus detection. The ransomware will browse and read many directories and files before encrypting a partial of the target files. Taking advantage of this characteristic of ransomware to identify ransomware infections by looking at the distribution of system calls per file and file system access patterns can be expected to reduce the likelihood of antivirus false positives and false negatives. For example, a study by Harun Oz et al introduced a case of ransomware that utilizes JavaScript's File System Access (FSA) API based on a web browser to perform encryption after the user gains file permissions [5]. In particular, the study showed that antiviruses recognized the ransomware executed through the browser as normal. To overcome this problem of antivirus detection, the researchers proposed a defense based on monitoring system call distribution and file system activity patterns. For example, the ransomware's process was observed to make a single file access to a file in the test folder. However, in the case of a legitimate process, multiple file access patterns were observed. In addition, when system call monitoring is enabled, system calls made by the ransomware were found to be uniformly made for every file access, while calls made by the legitimate process were found to be randomly distributed across individual files as the file size varied. Given that most ransomware accesses all files before encrypting them, we can conclude that file system activity patterns and system call patterns can be leveraged to reduce the likelihood of antivirus false positives and false negatives. A limitation of using ransomware's system call and file system behavior patterns is that it requires a relatively long time to collect data. In the future, we plan to improve the hooking technique to evade the anti-debugging of ransomware and implement the system to stop the execution of ransomware by delaying the execution of suspicious processes using delayed computation, as shown in Figure 2.

The 7th International Conference on Mobile Internet Security (MobiSec'23), Dec. 19-21, 2023, Okinawa, JAPAN, Article No. P-34
*Corresponding author:Department of Information Security, Sejong University, Seoul, 05006, South Korea, Email: woongbak@sejong.ac.kr

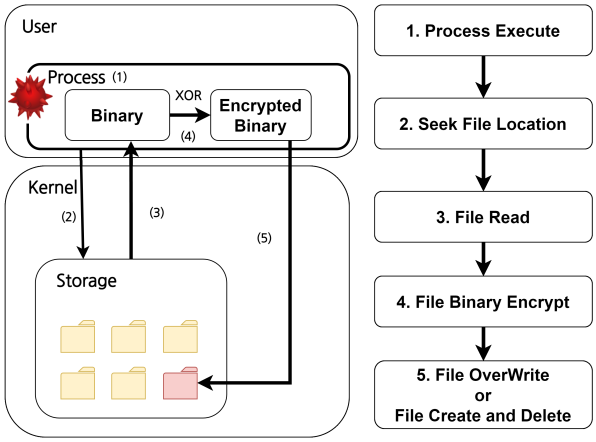

Figure 1: Ransomware encryption process.

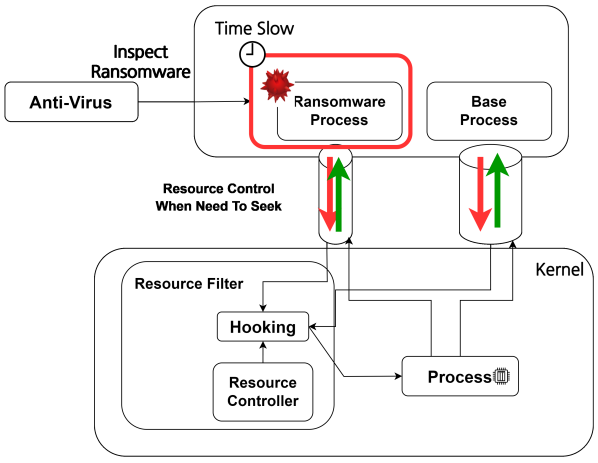

Figure 2: Using execution delay with hooking for ransomware execution delay.

Acknowledgement: This work was supported by the Institute of Information & Communications Technology Planning& Evaluation (IITP) , South Korea(Project No. RS-2022-00165794, Development of a Multi-Faceted Collection-Analysis-Response Platform for Proactive Response to Ransomware Incidents,40%, and Project No. 2022-0-007010001003, 30%), and a National Research Foundation of Korea (NRF), and the ICT R&D Program of MSIT/IITP, South Korea (Project No. 2021-0-01816, A Research on Core Technology of Autonomous Twins for Metaverse, South Korea, 30%).

References

[1] Craig Beaman, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, 111:102490, 2021.

[2] Harun Oz, Ahmet Aris, Albert Levi, and A Selcuk Uluagac. A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys (CSUR)*, 54(11s):1–37, 2022.

[3] Manabu Hirano, Ryo Hodota, and Ryotaro Kobayashi. Ransap: An open dataset of ransomware storage access patterns for training machine learning models. *Forensic Science International: Digital Investigation*, 40:301314, 2022.

[4] Ömer Aslan Aslan and Refik Samet. A comprehensive review on malware detection approaches. *IEEE access*, 8:6249–6271, 2020.

[5] Harun Oz, Ahmet Aris, Abbas Acar, Güliz Seray Tuncay, Leonardo Babun, and Selcuk Uluagac. {RøB}: Ransomware over modern web browsers. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 7073–7090, 2023.