Leveraging File Hash Monitoring as a Proactive Early Warning System for Cybersecurity

Author: Joshua A. Reyes
Advisor: Lisabel Rodriguez
Electrical & Computer Engineering and Computer Science

Abstract

This study examines the behavior of Hidden Tear, an open-source ransomware, through a controlled attack conducted in a Windows 11 virtual machine. Autopsy was used to track and verify file hashes before, during, and after the ransomware attack. The findings indicate that although Hidden Tear alters the file hashes during encryption, it restores them to their original state upon decryption, thereby preserving file integrity. These results highlight the efficacy of file hash monitoring as a crucial technique for security analysts to detect and analyze ransomware attacks. The study advocates for further research into automated hashing tools to enhance capabilities for rapid identification and prevention of ransomware threats by facilitating real-time monitoring of changes in file properties.

Introduction

Ransomware has emerged as one of the most disruptive threats in today's digital landscape. Imagine turning on your computer, only to find all your files locked, and a demand for payment staring you in the face. This nightmare scenario has become increasingly common, affecting individuals, businesses, and even critical infrastructure. Ransomware is a type of malicious software that encrypts a victim's files, rendering them inaccessible until a ransom is paid. Over the past decade, we have witnessed a dramatic surge in ransomware attacks, both in frequency and severity, causing widespread concern and significant financial losses [1]. In 2022, these incidents rose by 13% compared to 2021, according to Verizon's Data Breach Investigation Report [2]. Statista projects that around 70% of businesses faced at least one ransomware attack in 2022, marking the highest annual rate on record. Cybercriminals are using more aggressive tactics, including data infiltrations and the threat of data leaks, to pressure companies into paying ransoms [2]. The rising tide of ransomware is fueled by ransomware as a service (RaaS), a model that allows even those with limited technical skills to launch sophisticated attacks. The consequences are dire: hospitals unable to access patient records, companies crippled by locked data, and local governments brought to a standstill. It is within this context that the study on Hidden Tear, an open-source ransomware, was conducted. Hidden Tear was initially developed for educational purposes, providing a glimpse into the mechanics of ransomware without malicious intent [3]. However, its availability has made it a popular subject of analysis in the cybersecurity community.

Background

Given this growing threat, it is crucial to develop effective methods to detect and mitigate ransomware attacks. This study focuses on Hidden Tear, an open-source ransomware initially created for educational purposes. By analyzing Hidden Tear in a controlled environment, the study aims to gain a deeper understanding of ransomware operations without any malicious intent. During the experiments, it was discovered that while Hidden Tear changes file hashes during encryption, it restores the original hashes after decryption. This finding suggests that monitoring file hash changes could be a powerful tool for detecting ransomware activity. The insights from this study could lead to the development of automated hashing tools, aiding security analysts in quickly identifying and responding to ransomware attacks. By advancing detection capabilities, the goal is to enhance cybersecurity measures, protect data integrity, and minimize the devastating impact of ransomware on society.

Problem

As computer systems begin to be targets of increased ransomware attacks, it is important to understand the impact of these attacks, how they behave, and, in the event of being the victim of one, whether a post-incident analysis of the file hash may provide useful information on the type of ransomware. If a computer system is infected with ransomware, is a fingerprint always left behind in the file hash? Should security professionals recommend the implementation of an auto-hashing tool into the processes of any computer environment, to ensure that proper recovery is done by comparing previously logged hashes with post-incident hashes?

Methodology

To safely analyze the malware, modifications were necessary. This was achieved using Microsoft Visual Studio, a comprehensive development environment, to compile the source code into an executable file. This process not only familiarizes students with software development and debugging, but also with the intricacies of malware construction and deployment.

The executable was then tested within a highly controlled environment using Oracle VM VirtualBox. This virtualization software creates a contained, isolated operating system on a single physical machine, allowing for the safe execution of potentially harmful software without risking the integrity of the host system. The choice of a Windows 11 ISO from Microsoft for the virtual machine ensured compatibility with the latest Windows security features and system architecture.

Results and Discussion

The results obtained from this study aims to aid cybersecurity professionals in understanding the behavior and impact of ransomware on computer systems and can move the discussions of automated file hashing of computer files for backup and restoration in the event of a cybersecurity incident.

Figure 1 shows the USB storage device with the files that will be used to execute the Hidden Tear ransomware attack. It includes a text file named “adobe” that will steal the computer’s information (name, device, OS) and store the decryption key the attacker could provide once payment is received

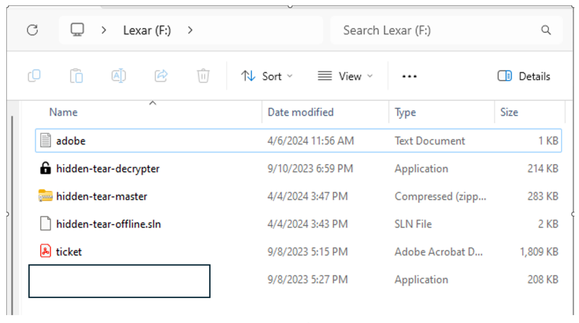

Figure 1
Hidden Tear initial files in USB storage device

With the ransomware ready to be executed, file hash validation was done using the forensic tool Autopsy before releasing the malware to the wild. This allowed the study to maintain credibility by ensuring that an immutable foundation was created before the launch. Figure 2 demonstrates the steps taken in Autopsy to read each file hash and each file extension to confirm that all three file types chosen were included in the sample.

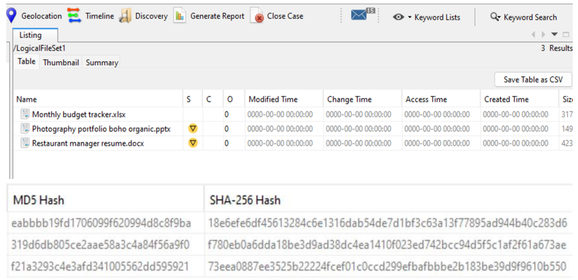

Figure 2
Results from Autopsy SHA-256 for all files prior to encryption

Once the files were encrypted, Autopsy was engaged again to import the encrypted files and observe the SHA-256 Hash values. Because there was a change to the file property, a change in the hash value was observed. Figure 3 shows the new hash value for each file.

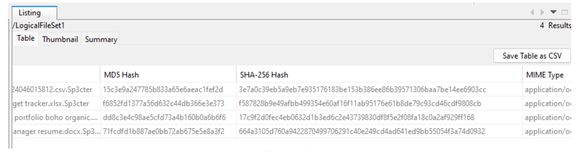

Figure 3
File hash change after malware execution

Figure 4 shows the hash value post decryption and confirmed that the file hashes returned to their original value.

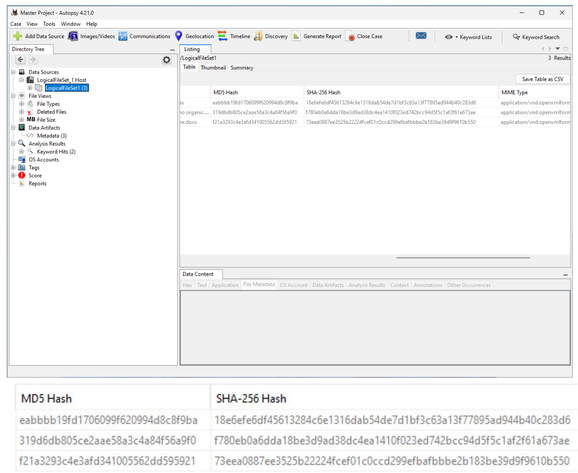

Figure 4
File Hash Values Post Decryption

Conclusions

This study of the Hidden Tear ransomware has illuminated critical aspects of ransomware behavior, particularly regarding its impact on file integrity. By executing Hidden Tear within a controlled virtual environment and meticulously analyzing file hash changes, we established that while the ransomware alters file hashes during the encryption process, these hashes revert to their original state upon decryption. This crucial finding emphasizes the importance of file hash monitoring as an effective method for detecting ransomware activity, providing a potential early warning system for security analysts. The ability to monitor file hashes in real time can serve as a frontline defense, alerting to unauthorized changes indicative of ransomware operations.

The employment of Autopsy was crucial in validating our approach, facilitating the verification of file hashes and demonstrating its practical application in real-world cybersecurity scenarios. The ability to verify and compare file hashes before and after ransomware attacks highlights the critical role that automated hashing tools can play in cybersecurity protocols. These tools can significantly enhance the speed and accuracy of ransomware detection, improving response times and mitigating potential damage. Incorporating such technologies into standard cybersecurity measures can fortify defenses against increasingly sophisticated ransomware attacks. Additionally, engaging with real-world malware in a controlled environment provides hands-on experience, essential for future cybersecurity professionals, while emphasizing the importance of adhering to ethical guidelines and legal frameworks.

The insights from this research advocate for the development of advanced automated hashing tools, crucial for the rapid identification of ransomware attacks and playing a significant role in recovery efforts. Ensuring the integrity of restored files post-attack is essential for maintaining data reliability and trust. As ransomware continues to evolve and pose significant threats across various sectors, advancements in cybersecurity measures are imperative. Automated hashing tools could become indispensable in verifying file integrity, thus supporting comprehensive recovery strategies and enhancing overall cybersecurity defenses.

Future Work

Future research should focus on refining these tools and exploring their integration into broader cybersecurity systems. By enhancing our detection and prevention capabilities, we can bolster our defenses against the ever-growing threat of ransomware. Integrating automated hashing tools into existing cybersecurity frameworks can provide a robust mechanism for real-time monitoring and response, ultimately safeguarding data and infrastructure from potential breaches. As we continue to advance in the field of cybersecurity, developing such proactive measures is crucial in staying ahead of malicious actors and ensuring the resilience of our digital environments. Should all files be monitored in this manner? No. However, having an immutable file that is known throughout an organization that is created with the intention to serve as an early warning system could be of great aid in the event of a malware attack.

References

[1] R. Richardson and M. M. North, “Ransomware: Evolution, mitigation and prevention,” DigitalCommons@Kennesaw State University, Jan. 1, 2017. Available: https://core.ac.uk/download/pdf/231830935.pdf

[2] Fortinet, “50 ransomware statistics and latest ransomware trends for 2023.” Accessed May 28, 2024. Available: https://www.fortinet.com/resources/cyberglossary/ransomware-statistics

[3] WatchGuard, “Ransomware – Hidden Tear.” Accessed May 28, 2024. Available: https://www.watchguard.com/wgrd-ransomware/hidden-tear