Research Article

Digital Forensics for Ransomware-based Software

Shayan Chakraborty

Volunteer, Applied Forensic Research Sciences.

How to cite this article: Shayan Chakraborty. Digital Forensics for Ransomware-based Software. Medico Legal Update, Vol 23 Special Issue 2023.

Abstract

The rapid proliferation of ransomware attacks has posed significant challenges to individuals, organizations, and society. Ransomware attacks have become increasingly prevalent as information technologies continue to evolve and spread globally. Cybercriminals have increasingly used ransomware as a means of cyberattack, using various methods to penetrate target computers, encrypt system data, and demand payment for user access. Despite the development of security tools like firewalls, antivirus software, and automated analysis tools, they have limited effectiveness in safeguarding valuable assets stored in local or cloud storage resources. This research paper explores the field of digital forensics as a crucial tool in combating ransomware-based software. The research focuses on various aspects of digital forensics specific to ransomware, including malware artifacts, encryption algorithms, and communication channels employed by ransomware strains. By leveraging a comprehensive dataset of ransomware samples and real-world case studies, the study identifies key patterns, trends, and characteristics that aid in attribution and forensic analysis of ransomware incidents. The research proposes a framework for effective detection and mitigation strategies against ransomware attacks, enhancing organizations' ability to prevent and respond to ransomware incidents effectively. The findings contribute to the advancement of digital forensics in the context of ransomware-based software, providing valuable insights into the evolving tactics and techniques employed by cybercriminals. The proposed framework equips security practitioners and law enforcement agencies with a comprehensive set of tools and strategies to combat ransomware attacks effectively.

Keywords: digital forensics, ransomware, malware analysis, incident response, mitigation strategies.

Introduction

The alarming growth in attacks involving ransomware has become a major issue for individuals, organizations, and even entire countries throughout the world. Ransomware is a sort of malicious software that encrypts important data on infected devices and demands a fee to unlock it. Because of the huge financial losses, operational interruptions, and lost sensitive information generated by these assaults, ransomware has emerged as a critical cybersecurity concern of our day's work. The technique of gathering, analyzing, and preserving digital data, known as digital forensics, is crucial in detecting and countering ransomware-based malware[1]. Security practitioners and law enforcement agencies can use forensic techniques to learn more about the attack pathways, strategies, and perpetrators behind ransomware outbreaks. This information not only aids in the attribution of the attacks, but also in the creation of preventative steps to prevent future events. The goal of this study is to explore the subject of digital forensics with a focus on ransomware-based malware. This study efforts to uncover critical insights into the mode of operation of ransomware attacks by undertaking an in-depth investigation

Corresponding Author: Shayan Chakraborty, Volunteer, Applied Forensic Research Sciences.

E-mail: Shayanchakraborty87@gmail.com

of numerous ransomware strains, their features, and accompanying forensic traces[2]. Furthermore, the study aims to provide effective methodology, tools, and a complete framework for identifying, mitigating, and investigating ransomware incidents. Understanding the changing ransomware attack situation is crucial for staying ahead of hackers. This study addresses an important void in literature by concentrating on digital forensics methodologies for ransomware, offering insight on the difficulties and problems associated in forensic examinations of these harmful software occurrences[3]. This study's findings will give vital knowledge and practical recommendations to security practitioners, forensic investigators, and policymakers fighting ransomware assaults. In short, the goal of this research project is to develop digital forensics in the context of ransomware-based software. It is feasible to increase the efficacy of incident response, improve attribution capabilities, and adopt preventative measures to defend against ransomware attacks by having a complete understanding of ransomware assaults and their forensic consequences.

Ransomware Attack Lifecycle: Ransomware attacks follow a typical lifecycle that involves several stages. The first stage is the delivery mechanism, which involves sending a phishing email or exploiting a vulnerability. Once the delivery mechanism has been executed, the ransomware will try to infect the system. This can be done through various infection vectors, such as malicious email attachments, infected websites, or drive-by downloads. Once the ransomware has infected the system, it will begin to encrypt files and data. Encryption techniques used by ransomware attackers are usually strong and will make it impossible to recover the data without the decryption key. The ransomware will then display a ransom note that demands payment in exchange for the decryption key. The payment process varies depending on the type of ransomware. Some attackers demand payment in cryptocurrency, while others may ask for payment via wire transfer or credit card[4]. The ransom amount may also vary, depending on the attacker's demands and the value of the encrypted data. The following is an example of a typical ransomware attack:

1. Delivery Mechanisms: Ransomware can be delivered through various mechanisms, including:
   - Phishing Emails: Attackers send deceptive emails with malicious attachments or links. These emails often masquerade as legitimate organizations or individuals.
   - Exploit Kits: Attackers exploit vulnerabilities in software or web browsers to deliver ransomware to vulnerable systems.
   - Malvertising: Malicious advertisements on legitimate websites can redirect users to websites hosting ransomware.
2. Infection Vectors: Once the delivery mechanism is successful, ransomware enters the victim's system. Common infection vectors include:
   - File-Based Ransomware: Malicious files, such as executable files or macro-enabled documents, are executed to initiate the infection.
   - Drive-by Downloads: Visiting compromised websites can trigger automatic downloads of ransomware onto the victim's system.
   - Remote Exploitation: Attackers exploit vulnerabilities in network services or remote management tools to gain unauthorized access and deploy ransomware.
3. Execution and Persistence: Once inside the system, ransomware typically performs the following actions:
   - File Encryption: The ransomware scans the system for files and encrypts them using strong encryption algorithms, rendering them inaccessible.
   - Privilege Escalation: Ransomware may attempt to elevate its privileges to gain control over critical system functions and bypass security measures.
4. Encryption Techniques: Ransomware employs various encryption techniques to lock files and demand a ransom:
   - Symmetric Encryption: Ransomware uses a single encryption key to encrypt files. This key is typically generated locally and kept secret by the attackers.
   - Asymmetric Encryption: Some advanced ransomware uses asymmetric encryption,

where a public key encrypts files, and a private key, held by the attackers, is required for decryption.

5. Ransom Note and Communication: After the target network has been successfully infected with ransomware, ransom demands are issued. Hackers notify the victim of the attack and provide information on the ransom needed to stop it. Computer displays may display ransom demands, or a letter may be placed in the directory containing the encrypted data. In addition to a promise to restore access to the encrypted data when the ransom has been paid, ransom demands frequently include information about the ransom amount, the necessary payment method, and the deadline for payment. If there has been data exfiltration, the hacker may also agree to refrain from disclosing more information and provide proof that the data has been deleted. Typically, cryptocurrency (like Bitcoin or Monero) is asked for as payment.
6. Ransom Payment: Attackers demand payment in exchange for decrypting the victim's files. The payment process usually involves:
   - Cryptocurrency: Attackers prefer anonymous payment methods like Bitcoin or other cryptocurrencies to maintain their anonymity.
   - Payment Portals: Attackers may provide a unique payment portal accessible via the Tor network, allowing victims to make the ransom payment securely.

It is important to note that paying the ransom does not guarantee file recovery, and victims are encouraged to report the incident to law enforcement agencies to aid in tracking and potentially disrupting ransomware operations[5,6].

Digital Forensics Fundamentals: Digital forensics is the investigation and reconstruction of digital occurrences such as cybercrimes or data breaches via the gathering, analysis, and preservation of electronic evidence. Several important concepts and strategies engage in this process:

1. Evidence Gathering:
   - Disc Imaging: Using programmes such as dd, FTK Imager, or EnCase, create forensic copies (images) of storage devices.
   - Live Forensics: Using tools like Volatility or Mandiant Redline, collect volatile data from a running system.
   - Mobile Device Forensics: Using specialized tools such as Cellebrite or Oxygen Forensic Suite, extract data from mobile devices.
2. Protection of Evidence:
   - Write-Blockers: Using write-blockers, either hardware or software, to prevent changes to the original evidence during acquisition.
   - Hashing: The process of calculating and validating cryptographic hash values (MD5, SHA-1, SHA-256) to assure data integrity.
   - Chain of Custody: Maintaining a detailed record of all individuals who have had custody of the evidence to establish its authenticity and admissibility in court.
3. Evidence Assessment:
   - File System Analysis: Investigating the content, timestamps, and metadata of files to comprehend file-related operations.
   - Searching for certain words or patterns inside documents or system artefacts to find pertinent data is known as keyword searching.
   - Timeline analysis: The process of compiling an event timeline using system logs and file timestamps.
   - Link analysis is the process of identifying connections and patterns of behavior between items.
4. Reporting:
   - Grouping and Structure: systematically presenting facts together with a methodology, conclusions, and suggestions.
   - A report must adhere to the correct processes to be acceptable in court and satisfy legal criteria.

All things considered, digital forensics is extremely important for locating and recording valuable information from electronic evidence, aiding investigations, and supporting legal procedures[7,8].

Digital Evidence Collection and Preservation: Collecting, preserving, and analyzing digital evidence is crucial in investigating ransomware attacks. Following best practices ensures the integrity and admissibility of the evidence. The key practices and their significance in the context of digital evidence collection and preservation are:

1. Chain of Custody: The chain of custody refers to the chronological documentation of the evidence's custody, including its collection, storage, transfer, and analysis. It is essential for maintaining the integrity and admissibility of the evidence in legal proceedings.
2. Volatile and Non-Volatile Data Collection: Ransomware attacks may leave traces in both volatile (temporary) and non-volatile (persistent) data. Collecting both types of data is crucial for a comprehensive investigation.
3. Use of Forensic Tools: Digital forensic tools aid in collecting, preserving, and analyzing evidence efficiently and effectively. Best practices include Disk Imaging, File Integrity Verification, Malware Analysis Tools.
4. Effective Techniques for Ransomware Attacks: Ransomware attacks present specific challenges that require tailored techniques.
    - Memory Forensics: Analyzing volatile memory (RAM) to identify running processes, injected code, encryption keys, and evidence of ransomware activity using tools like Volatility.
    - Network Forensics: Capturing network traffic during and after an attack to identify communication with malicious servers, analyze network-based indicators of compromise, and uncover exfiltration attempts.
    - Ransomware Decryption Tools: Leveraging publicly available decryption tools and resources, such as the No More Ransom project, to recover encrypted files without paying the ransom[9].

Ransomware Analysis Techniques: Ransomware analysis techniques play a crucial role in understanding the behavior, Functionality, and underlying mechanisms of ransomware samples. By employing a combination of static and dynamic analysis, reverse engineering, and malware sandboxing, analysts can gain valuable insights into the ransomware's operation.

1. Static Analysis: Static analysis involves examining the ransomware sample without executing it. Key techniques and tools used in static analysis include:
    - File Metadata Analysis: Examining file properties, such as file type, size, creation/modification timestamps, and digital signatures, to gain initial insights into the sample.
    - Code Disassembly: Using disassemblers, such as IDA Pro or Ghidra, to analyze the ransomware's assembly code, understanding its logic, control flow, and high-level functions.
    - String Analysis: Extracting and analyzing strings within the ransomware binary to identify hardcoded URLs, encryption keys, command-and-control servers, or other indicators of the malware's behavior.
    - API and Library Calls: Identifying API and library calls within the ransomware code to understand its interactions with the operating system and other software components.
2. Dynamic Analysis: Dynamic analysis involves running the ransomware sample in a controlled environment to observe its behavior and interactions with the system. Key techniques and tools used in dynamic analysis include:
    - Malware Sandboxing: Executing the ransomware sample in a controlled and isolated environment, such as a virtual machine or an analysis sandbox, to monitor its activities without affecting the host system.
    - System Monitoring: Observing system-level events, such as file system modifications, registry changes, network connections, and process execution, using tools like Process Monitor or Wireshark.
    - Behavior Analysis: Studying the ransomware's actions, including file encryption, process injection, persistence mechanisms, and communication

with command-and-control servers, to understand its behavior and identify its unique characteristics.

3. Reverse Engineering: Reverse engineering involves dissecting the ransomware sample to understand its inner workings, algorithms, and anti-analysis techniques. Key techniques and tools used in reverse engineering include:
   - Code Decompilation: Converting the ransomware's compiled code back to a higher-level programming language, such as C or C++, using tools like IDA Pro or Ghidra.
   - Code Debugging: Analyzing the ransomware's execution flow, variable values, and memory modifications using debuggers, such as OllyDbg or x64dbg, to gain insights into its behavior and identify key functions.
   - Malware Unpacking: Analyzing and unpacking any packed or obfuscated sections of the ransomware code to reveal its original structure and functionalities.

These techniques collectively aid in understanding the ransomware's infection methods, propagation mechanisms, encryption algorithms, anti-forensic techniques, and command-and-control communication. The analysis results can inform incident response efforts, help develop detection signatures, and guide the development of effective mitigation strategies.

Ransomware Detection and Prevention: Ransomware attacks have become increasingly sophisticated, necessitating robust detection and prevention mechanisms. Various approaches and tools are employed to detect and prevent ransomware attacks.

1. Anomaly Detection:
   - Baseline Analysis: Establishing normal system behavior and identifying anomalies like unusual file access or high CPU usage.
   - Statistical Analysis: Using statistical algorithms to detect outliers and unusual patterns in logs, network traffic, or user behavior.
   - User and Entity Behavior Analytics (UEBA): Monitoring user and entity behavior for rapid file modifications or mass encryption.
2. Signature-Based Detection:
   - Antivirus Software: Using databases of known ransomware signatures to detect and block known variants.
   - Indicators of Compromise (IOCs): Using file hashes, names, or server addresses to identify and block known ransomware.
3. Behavior-Based Detection:
   - Heuristics: Detecting ransomware based on predefined behavioral rules, such as rapid file encryption.
   - Endpoint Detection and Response (EDR): Monitoring system-level activities to identify ransomware behaviors.
4. Machine Learning (ML) Algorithms:
   - Supervised Learning: Training ML models on labeled datasets to identify ransomware characteristics.
   - Unsupervised Learning: Applying clustering or anomaly detection to identify unusual patterns.
   - Ensemble Methods: Combining multiple ML models for enhanced detection accuracy.

It is important to note that no single detection technique is foolproof, and a layered defense approach is recommended. This involves combining multiple detection methods and tools to increase the chances of detecting and preventing ransomware attacks effectively[10].

Ransomware Digital Forensics Challenges: Ransomware attacks have become a pervasive and sophisticated threat, targeting individuals, businesses, and even critical infrastructure. Digital forensic investigators face unique challenges when dealing with ransomware incidents due to the encryption algorithms used, anti-forensic techniques employed by ransomware authors, and the continuous evolution of ransomware variants.

1. Encryption Algorithms: Ransomware employs strong encryption algorithms to render victim files inaccessible until a ransom is paid. The use of robust encryption algorithms such as AES, RSA, or their variants poses significant challenges to investigators. Key points include:
    - Encryption Strength: Modern encryption algorithms are impossible to break, making file recovery without the decryption key highly unlikely.
    - Encryption Speed: Ransomware operates at high speeds, encrypting files rapidly and leaving minimal traces, limiting the time window for detection and response.
2. Anti-Forensic Techniques: Ransomware authors employ various anti-forensic techniques to hinder investigation efforts and increase the likelihood of successful attacks. Key challenges include:
    - Data Destruction: Some ransomware variants delete shadow copies, event logs, and other system artifacts that could aid in the investigation.
    - Code Obfuscation: Ransomware authors obfuscate their code to evade detection by antivirus software and make analysis more difficult.
    - Tor and Onion Services: Ransomware operators often use the Tor network and onion services to remain anonymous and communicate with victims, complicating attribution, and tracing efforts.
3. Evolution of Ransomware Variants: Ransomware continues to evolve rapidly, posing challenges to investigators who need to keep pace with new techniques and tactics. Key considerations include:
    - Polymorphic and Fileless Ransomware: Some ransomware variants change their code and behavior to evade signature-based detection, making them harder to identify and analyze.
    - Ransomware-as-a-Service (RaaS): The rise of RaaS platforms allows less technically skilled individuals to launch ransomware attacks, leading to a broader range of ransomware variants and increased attack volume.
    - Diversification of Targets: Ransomware attacks now target not only individual users but also critical infrastructure, healthcare organizations, and government entities, amplifying the potential impact and complexity of investigations.
4. Technical Aspects of Ransomware Digital Forensics: Investigative methodologies and technical approaches play a crucial role in ransomware incident response. Key considerations include:
    - Isolation and Preservation: Isolating infected systems and preserving the state of the compromised environment to prevent further damage and ensure the integrity of evidence.
    - Memory Analysis: Extracting volatile data from system memory to identify running processes, network connections, and cryptographic artifacts that can aid in analysis and attribution.
    - Traffic Analysis: Examining network traffic for indications of command-and-control servers, communication protocols, and data exfiltration attempts, which can provide valuable insights into the ransomware operation.

The encryption algorithms used by ransomware, the anti-forensic techniques employed by ransomware authors, and the evolution of ransomware variants all present significant challenges. However, with the adoption of new techniques and tools, investigators are making progress in combating ransomware attacks and recovering encrypted data without paying the ransom[11].

Ransomware Research Landscape: This research provides an overview of critical research areas in combating ransomware threats. From advanced analysis techniques to emerging technology risks, the focus encompasses detection, prevention, attribution, and incident response best practices. Addressing legal concerns and promoting collaborative intelligence sharing aims to foster a resilient cybersecurity community prepared to counter evolving ransomware challenges.

- Advanced Ransomware Analysis Techniques:
    - o Develop methods to dissect sophisticated ransomware strains and identify weaknesses.

- Understand behavior and encryption algorithms of ransomware attackers.

- Automated Ransomware Detection and Classification:
  - Design efficient machine learning and AI-based methods for automated detection and classification.
  - Create robust models to analyze ransomware samples accurately.

- Ransomware Attribution and Tracking:
  - Develop methodologies and tools to trace the origins of ransomware attacks.
  - Improve attribution to hold perpetrators accountable and prevent future attacks.

Additionally, understanding ransomware attacker behavior, establishing incident response best practices, developing threat intelligence sharing platforms, and investing in training and capacity building are essential components in combating ransomware attacks effectively[11].

Conclusion

This review paper has provided a comprehensive overview of digital forensics for ransomware-based software, shedding light on the critical aspects of this evolving and complex domain. Ransomware continues to pose significant threats to individuals and organizations worldwide, making digital forensics an indispensable tool in understanding, mitigating, and responding to such attacks. Through the exploration of assorted topics, including ransomware attack lifecycles, digital forensics fundamentals, challenges faced by investigators, evidence collection techniques, and analysis methods, this paper underscores the importance of a robust and initiative-taking approach to ransomware incident response. Despite the advancements in digital forensics, ransomware authors constantly evolve their techniques, necessitating ongoing research and development to stay one step ahead. Addressing the legal and ethical considerations surrounding ransomware investigations is equally crucial, ensuring that investigations uphold principles of privacy and data protection. Moving forward, researchers and practitioners must collaboratively work to develop innovative detection, prevention, and response strategies. By continuously refining digital forensics methodologies and staying abreast of emerging trends, the field can better equip itself to combat the ever-changing landscape of ransomware-based software threats.

Conflict of Interest: Authors do not have any conflict of interest.

Source of Funding: No funding provided.

Ethical Clearance: No ethical required for the work.

References:

1. Zimba, A., Mulenga, M. A dive into the deep: demystifying wannacry crypto ransomware network attacks via digital forensics. International Journal on Information Technologies and Security 10(2): 57-68. 2018.
2. Solomon, M. G., Cichonski, M. J. Ransomware: A practical guide to responding to ransomware attacks. Syngress. 2021
3. Hale, M. Digital forensics of ransomware attacks. CRC Press. 2022
4. Liska, A. Ransomware: The complete guide to prevention, detection, and recovery. Scyrion. 2023
5. Cowen, D. Ransomware: A guide for businesses. Syngress. 2023
6. Farber, D. J. The ransomware response playbook: A step-by-step guide to mitigating the impact of ransomware attacks. CRC Press. 2022
7. Ablon, Y., & Szor, M. The ransomware playbook: Understanding and responding to ransomware attacks. MIT Press. 2022
8. Cimpanu, C. Ransomware: A beginner's guide. No Starch Press. 2023
9. Ferguson, P., & Moore, T. Ransomware: The definitive guide to preventing, detecting, and responding to ransomware attacks. Packt Publishing. 2021
10. Green, B. Ransomware: The ultimate guide to understanding, preventing, and recovering from ransomware attacks. Syngress. 2022
11. Jaquith, A. Ransomware: A survival guide for businesses. Apress. 2022.