

RANSOMWARE BEHAVIOURAL ANALYSIS

Sushmita KM, Dr. P Kavitha

Student, Department of Computer Science with Cyber Security, Sri Ramakrishna College of Arts & Science, Coimbatore.

Associate Professor & Head, Department of Computer Science with Cyber Security, Sri Ramakrishna College of Arts & Science, Coimbatore

susmitamukundharaj@gmail.com, 23130053@srcas.ac.in, kavitha.p@srcas.ac.in

Abstract

Ransomware has become a major cybersecurity threat, and traditional signature-based detection methods are often ineffective against modern variants using advanced evasion techniques. This study proposes a behavior-based detection framework using entropy analysis, string pattern matching, file header inspection, MITRE ATT&CK mapping, and IOC detection within a sandbox environment to accurately identify ransomware threats.

Keywords— Ransomware Detection, Behavioral Analysis, Entropy Analysis, MITRE ATT&CK, Indicator of Compromise (IOC) Detection

I. INTRODUCTION

Ransomware has become one of the most severe and financially damaging cyber threats, especially as organizations increasingly depend on digital infrastructure across sectors like healthcare, banking, education, and government. Traditional antivirus and signature-based detection systems are no longer sufficient because modern ransomware uses advanced evasion techniques such as polymorphism, encryption, obfuscation, and anti-analysis methods to bypass static defenses. To address this challenge, the Ransomware Behavioral Analysis project introduces a behavior-driven detection framework that analyzes uploaded files for encryption patterns, suspicious commands, registry changes, shadow copy deletion attempts, and other ransomware-related indicators. The primary objective is to shift from reactive signature-based detection to proactive behavioral monitoring, identifying threats based on unavoidable malicious actions like file encryption and ransom execution. The system uses a multi-layer detection model combined with a weighted risk scoring mechanism to classify threats as low, medium, or high risk while providing transparent explanations of detected behaviors. Operating within a secure sandbox-style environment, the platform focuses on safe file-level analysis rather

than full endpoint monitoring. Although it is not designed as a complete enterprise EDR solution, it serves as a scalable, research-oriented prototype demonstrating the effectiveness of intelligent, behavior-focused ransomware detection.

II. LITERATURE REVIEW

A. Behavioral-Based Ransomware Detection Using Machine Learning

S. K. Sahay, R. M. Rao, and P. K. Verma (2023) proposed a behavior-driven ransomware detection system that focuses on identifying malicious activity through system behavior monitoring rather than relying solely on signature matching. Their study analyzes features such as abnormal file encryption rates, rapid file renaming operations, registry modifications, and suspicious API calls. A machine learning classifier trained on behavioral datasets improves detection accuracy against zero-day ransomware variants. The authors concluded that behavior-based detection models outperform traditional antivirus systems in detecting unknown ransomware families and emphasized the importance of feature selection and risk evaluation in improving classification performance.

B. Entropy-Based Detection of Encrypted Malware Payloads

J. Lee and M. Kim (2024) explored the use of Shannon entropy analysis for identifying encrypted or packed malware payloads. The study demonstrates that encrypted ransomware files typically exhibit high entropy values due to their random byte distribution. The authors proposed a threshold-based entropy evaluation approach combined with structural file analysis to distinguish legitimate compressed files from malicious encrypted payloads. Experimental findings indicate that entropy analysis can effectively function as an early-stage screening mechanism in malware detection systems.

C. MITRE ATT&CK-Based Ransomware Behavior Mapping

A. Fernandez and T. Roberts (2024) conducted research on mapping ransomware behaviors using the MITRE ATT&CK framework. Their study analyzed common ransomware techniques including data encryption for impact, persistence through registry modifications, command-line execution patterns, and shadow copy deletion. By correlating detected behaviors with standardized ATT&CK techniques, the approach enhances threat intelligence and improves interpretability of detection results. The study demonstrates that integrating framework-based mapping provides structured analysis and strengthens cybersecurity incident response strategies.

III. SYSTEM METHODOLOGY

A. System Architecture Overview

The proposed system follows a **modular architecture** designed to provide secure and accurate ransomware detection. The architecture consists of several components including the User Interface, Secure Upload Module, Sandbox Engine, Detection Modules, Risk Evaluation Engine, and Report Generator. Suspicious files uploaded by users are processed within an isolated environment to prevent potential compromise of the host system.

B. Secure Upload and Sandbox Environment

To ensure safe analysis of suspicious files, the system implements several security measures during file submission and processing.

- File size and format validation
- SHA-256 hash generation for file identification
- Temporary isolated storage environment
- No direct execution of uploaded files
- Controlled sandbox-based behavioral analysis

These mechanisms ensure that malicious files cannot directly interact with the host system during analysis.

C. Detection Modules

The system incorporates multiple detection modules to identify ransomware indicators.

- *Entropy Analysis*: Calculates Shannon entropy to detect encryption-like patterns. Files with entropy values greater than 7.5 are flagged as suspicious.
- *String Pattern Matching*: Extracts embedded strings to identify ransom notes, suspicious commands, and malicious scripts.
- *File Header Inspection*: Verifies file signatures and detects disguised extensions or structural anomalies.
- *MITRE ATT&CK Mapping*: Correlates detected behaviors with standardized adversarial techniques.
- *IOC Detection*: Compares extracted file attributes with known indicators of compromise.

D. Risk Evaluation and Reporting

All detected behavioral indicators are aggregated within a *weighted scoring model*. Each indicator contributes to an overall risk score that determines the probability of ransomware presence. The final output classifies files into **Low, Medium, or High risk categories** and generates a structured report summarizing detected behaviors and analytical findings.

IV. SYSTEM DESIGN

A. File Validation Module

This module validates the uploaded file's format, size, and integrity before analysis. It also generates

a unique SHA-256 hash value used for identification and tracking.

B. Entropy Analysis Module

The entropy analysis module calculates Shannon entropy values to detect encryption-like patterns typically associated with ransomware activity.

C. String Pattern Detection Module

This module extracts and analyzes embedded strings from files to identify suspicious commands, ransom messages, or malicious scripts.

D. Header Inspection Module

The header inspection module verifies file signatures and identifies anomalies such as spoofed extensions, hidden payloads, or manipulated file structures.

E. Risk Evaluation and Reporting Module

All behavioral indicators are aggregated and processed through a weighted risk scoring algorithm. The system then generates a detailed analysis report indicating detected threats and recommended mitigation steps.

V. PROPOSED ARCHITECTURE

The proposed architecture consists of the following major components:

1. *File Preprocessing Module* – Validates file format, extracts metadata, calculates hash values, and prepares the file for analysis.
2. *Behavioral Analysis Engine* – Performs entropy analysis, macro inspection, string extraction, command detection, and suspicious API pattern identification.
3. *Indicator Evaluation Module* – Detects ransomware-related behaviors such as encryption patterns, registry modifications, and shadow copy deletion attempts.
4. *Risk Scoring Engine* – Assigns weighted scores to behavioral indicators and calculates an overall ransomware probability score.

5. *Report Generation Module* – Generates a structured report presenting detected behaviors, threat level classification, and recommended mitigation measures.

VI. APPLICATIONS

The proposed system can be applied in several cybersecurity domains:

1. Cybersecurity research and academic analysis
2. Pre-deployment suspicious file scanning
3. Incident response and threat investigation
4. Threat intelligence and IOC identification
5. Malware awareness and cybersecurity training
6. Digital forensics analysis
7. Enterprise security prototype development
8. Detection of zero-day ransomware threats

VII. THREAT MODEL AND MITIGATIONS

A. Malicious File Exploiting the Analysis Server

Threat: Uploaded files may attempt to exploit vulnerabilities in the analysis server.

Mitigation: Files are processed in an isolated sandbox environment with strict input validation and file size restrictions.

B. Advanced Ransomware Evasion Techniques

Threat: Modern ransomware may use obfuscation, encryption, or packing techniques to evade detection.

Mitigation: A multi-layer detection approach combining entropy analysis, string pattern matching, header inspection, MITRE ATT&CK mapping, and IOC detection reduces evasion success.

C. Unauthorized Access to Uploaded Files

Threat: Sensitive uploaded files or analysis reports could be accessed without authorization.

Mitigation: Secure communication protocols (HTTPS), access control mechanisms, temporary

storage, and automatic deletion after analysis ensure data security.

VIII. FUTURE TRENDS

Future research directions include:

1. AI-driven malware detection models
2. Integration with automated threat intelligence platforms
3. Behavioral pattern prediction using machine learning
4. Integration with enterprise SIEM and EDR security systems

IX. CONCLUSION

The Ransomware Behavioral Analysis platform provides a secure and structured approach for detecting ransomware threats using behavior-based inspection techniques. Suspicious files are analyzed in a controlled sandbox environment to prevent host system compromise. The system integrates entropy analysis, string pattern matching, file header inspection, MITRE ATT&CK mapping, and IOC detection to identify ransomware behaviors effectively.

All behavioral indicators are processed through a centralized engine using a weighted risk evaluation model that generates probability-based threat

assessments. Detailed reports enhance usability for cybersecurity professionals, while the modular architecture supports scalability and future improvements. Overall, the proposed system demonstrates an efficient and reliable approach to detecting and analyzing ransomware threats.

REFERENCES

- [1] D. Sgandurra, L. Muñoz-González, R. Mohsen, and E. C. Lupu, “Automated dynamic analysis of ransomware: Benefits, limitations and use for detection,” Proc. Int. Conf. Risk and Security of Internet and Systems, 2016.
- [2] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “PayBreak: Defense against cryptographic ransomware,” Proc. ACM Asia Conf. Computer and Communications Security, 2017.
- [3] N. Scaife, H. Carter, P. Traynor, and K. R. B. Butler, “Cryptolock (and drop it): Stopping ransomware attacks on user data,” IEEE Int. Conf. Distributed Computing Systems, 2016.
- [4] MITRE Corporation, “MITRE ATT&CK Framework,” 2023. Available: <https://attack.mitre.org>
- [5] D. Ucci, L. Aniello, and R. Baldoni, “Survey of machine learning techniques for malware analysis,” *Computers & Security*, vol. 81, pp. 123–147, 2019.