Ransomware Simulator Project Report

---

1. Introduction

Ransomware has become one of the most damaging forms of cyber threats in recent years. It works by encrypting files on a victim's machine, rendering them inaccessible, and demanding a ransom for their decryption. Understanding the behaviours, encryption methods, and propagation techniques of ransomware is critical to devising effective countermeasures.

The objective of this project is to build a **Ransomware Simulator** that allows for the simulation of various ransomware behaviours. By simulating different ransomware types, the tool will provide insights into how ransomware operates and affects systems, enabling deeper analysis and study in a controlled environment.

---

2. Objective

The primary goal of this project is to create a simulator capable of mimicking the behaviour of multiple ransomware variants. Key objectives include:

- Simulating encryption processes used by real-world ransomware (e.g., AES, RSA, hybrid encryption).
- Allowing users to select different ransomware types and customise their behaviour (such as partial vs. full encryption).
- Generating realistic file extensions and ransom notes.
- Providing insights into how ransomware might propagate through systems and networks.
- Including advanced ransomware features such as hiding encryption keys and privilege escalation techniques.

---

3. Key Features

1. **Multiple Ransomware Types**: The simulator supports various ransomware types such as Conti, Ryuk, REvil, Maze, etc. Each ransomware has distinct characteristics, encryption methods, and target file types.
2. **Encryption Techniques**: Simulates multiple encryption algorithms (e.g., AES, RSA, hybrid) used by real ransomware, accurately replicating their behaviour.
3. **Customizable Simulation**: Users can customise how the ransomware behaves:
    - Target specific directories and file types.
    - Partial or full encryption of files.
    - Custom file extensions appended to encrypted files.
4. **Random Extension Generator**: For each ransomware type, the simulator generates random file extensions for encrypted files, adding a layer of realism.

5. **Thread Usage**: The simulator leverages multi-threading to simulate how ransomware might encrypt files in parallel, improving performance and mirroring real-world attacks.
6. **Key Hiding Techniques**: Implements methods to conceal the encryption key from users, using techniques modelled after real ransomware behaviour.

---

4. Project Methodology

4.1 Data Collection and Analysis

The first step in building the simulator involved gathering detailed information about various ransomware types. We created an Excel sheet with attributes for 20 ransomware types, analysing their:

- Encryption methods.
- Targeted file types.
- Propagation techniques.
- Methods for hiding encryption keys.

From this analysis, we identified patterns and behaviours that helped guide the design of the simulator.

Ransomware	RaaS	Target	Initial Access (via)	Discovery	Di
Play	yes	enterprise and individual	Valid Accounts (T1078), External Remote Servic	AdFind (Active account discovery), G	ye
Black Beasts (Black Basta)	yes	critical infrastructure sector	phishing, exploitation, valid accounts	QakBot stealer (AKA QBot or Pinksli	Ye
Bianlian	yes	private critical infrastructur	rdp with valid accounts, phishing	Advanced Port Scanner, PingCastle (a	ye
Cerber	yes	multiple industries	phishing emails, compromised websites and malv	Netview, Netstat	ye
Conti	yes	enterprise	Phishing emails, RDP	AdFind, CobaltStrike	ye
PYSA	yes	Educational institutions, bu	Phishing emails, RDP	-	Ye
REVIL	yes	Businesses, healthcare, gov	Phishing emails, software vulnerabilities	-	Ye
MAZE	yes	Businesses, healthcare, gov	Phishing emails, RDP, software vulnerabilities	-	Ye
Lockbit	Yes	Various industries, includin	Phishing emails, RDP, Exploit Public-Facing Ap	AdFind, BloodHound	Ye
WANNACRY	no	Businesses, healthcare	Phishing emails, EternalBlue exploit	-	No
Karakurt	No	No Specific sector	Intrusion Brokers, Log4Shell, Outdated VPN's, P	-	No
Royal	Yes	Manufacturing, Communic	Phishing Emails	Yes (Chisel)	No
Avaddon	Yes	international public and pri	Intrusion Brokers	Yes BLACKCROW and DARKRAVE	Ye
Bad Rabbit	No	Primarily Russian media ag	Drive-by-Download	Yes DROP	No
Cl0P	Yes	US Government + File Trai	Phishing Emails	Yes	No
HIVE	Yes	energy, healthcare, financia	distributed through malicious ZIP files and phishi	Yes, Uses Tor	Ye
DOPPLEPAYMER	Yes	Healthcare, government, fir	Phishing emails, exploit kits, malicious attachme	Yes	Ye
EGREGOR	Yes	Retail, logistics, healthcare	Phishing emails	Yes	Ye
BLACKCAT	Yes	Various, particularly enterp	Phishing emails, compromised RDP credentials, (	Yes, Uses Tor	Ye
CRYPTOLOCKER	No	Windows users, both indivi	Phishing emails, malicious attachments	Yes	Ye

Fig.1: A Snapshot of Excel with all the 20 different ransomware.

Ransomware Key Attributes

- **RaaS (Ransomware as a Service)**: Specifies whether the ransomware operates as a service.
- **Target**: Types of organisations or sectors primarily targeted.
- **Initial Access (via)**: The method used to gain initial access to the target system (e.g., phishing, RDP, exploit kits).
- **C2 (Command and Control)**: Indicates whether the ransomware uses Command and Control communication channels.
- **Custom Malware**: Denotes if the ransomware uses custom-developed malware.

- **Disable Antivirus?**: Whether the ransomware attempts to disable antivirus software on the target system.
- **Data Exfiltration**: Specifies if data is exfiltrated prior to encryption.
- **Lateral Movement**: Indicates if the ransomware spreads laterally across networks.
- **Privilege Escalation**: Whether the ransomware seeks to escalate privileges on the infected system.
- **Delete Shadow Copies/Backups**: Indicates if shadow copies and system backups are deleted to prevent recovery.
- **File Encryption**: Whether files are encrypted by the ransomware.
- **Encryption Technique**: The encryption algorithms used (e.g., AES, RSA, ChaCha20).
- **File Extension**: The file extension added to encrypted files (e.g., .play, .cl0p).
- **Double Extortion**: Specifies if the ransomware uses double extortion by threatening to leak exfiltrated data.
- **Modify Boot Loader (MBR)?**: Indicates whether the ransomware modifies the bootloader or Master Boot Record (MBR).
- **Persistence**: Persistence techniques used to maintain access to the system.
- **Payment Mode**: The method of ransom payment (e.g., Bitcoin, Monero).
- **Mail Type**: The type of email used for communication (e.g., encrypted, plain).
- **Data Extortion**: Whether data extortion is employed.
- **Zip Type**: The type of zip or compression used, if any (e.g., AES Zip).
- **File Directory Discovery**: Whether file directories are enumerated or discovered.
- **Remote Access Software**: Software used for remote access (e.g., AnyDesk).
- **Ransom Note**: Details about the ransom note, including possible URL links.
- **Tools**: Tools used by the ransomware for its operations (e.g., Cobalt Strike, Bloodhound).
- **Additional Notes**: Any additional information relevant to the ransomware variant.

4.2 Ransomware Selection and Simulation Development

To validate our approach, we began by selecting specific ransomware types such as Conti, Play, and LockBit. These variants were chosen for their distinct encryption methods, attack patterns, and real-world impact. By simulating each individually, we replicated their behaviour, encryption strategies (such as AES and RSA combinations), and specific file-targeting mechanisms.

This exercise provided crucial insights into how different ransomware types operate in practice. It also allowed us to refine our simulator to better handle different ransomware behaviours. Once these initial simulations were complete, we generalised the simulator to include additional ransomware types by extending the attributes and behaviours stored in the JSON configuration file.

4.3 Development of Encryption and Decryption Codes

A GitHub repository was created to manage the development of encryption and decryption algorithms suitable for different ransomware types. The encryption methods implemented include:

- **AES**: Symmetric encryption used by ransomware such as Ryuk.
- **RSA**: Asymmetric encryption for more sophisticated ransomware like REvil.
- **Combined Encryption**: Some ransomware use both AES and RSA in combination.

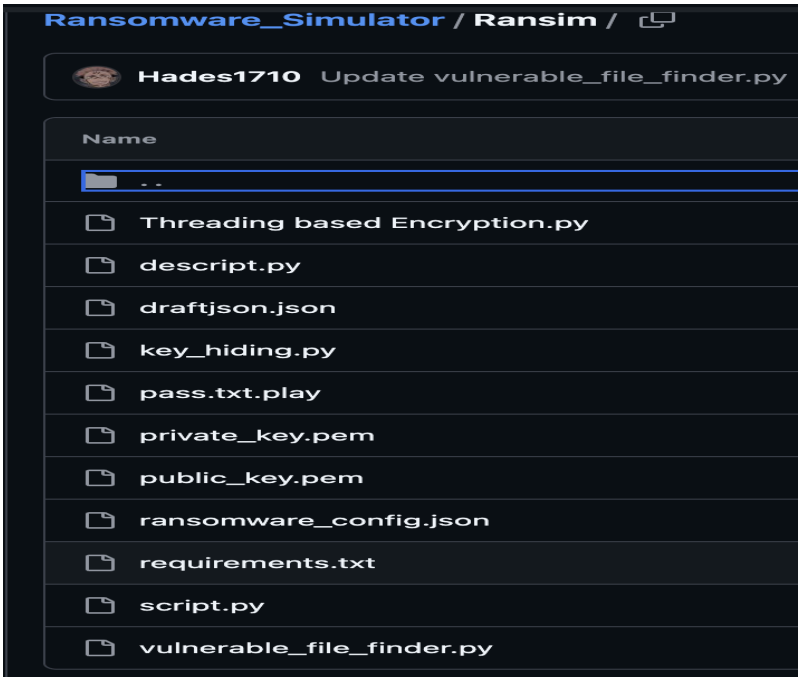

Fig. 4: In the Ransim directory all the codes for coordinating different ransomware's simulation are available.

4.3 JSON-Based Ransomware Configuration

We developed a JSON file that holds attributes and corresponding details for each ransomware type, including:

- Name of the ransomware.
- Encryption algorithm.
- File extensions targeted for encryption.
- Ransom note templates.

This allows for easy configuration and customization of the simulator.

4.4 File Extension Targeting and Random Extension Generation

The simulator includes a feature that allows users to specify which file types will be encrypted (e.g., `.docx`, `.jpg`, `.pdf`). Additionally, a random file extension generator was implemented, which simulates ransomware behaviour by appending unique extensions (e.g., `.conti_crypt_xyz123`) to encrypted files.

4.5 Thread Usage

The simulator incorporates thread usage to handle file encryption tasks in parallel, significantly improving the efficiency and mimicking how some ransomware operates in the wild.

4.6 Key Hiding Techniques

To simulate advanced ransomware behaviours, the simulator includes methods to hide the encryption key, preventing users from easily accessing it. These techniques vary depending on the ransomware being simulated.

---

5. Current Status and Achievements

So far, the following components of the ransomware simulator have been developed:

- Detailed analysis of 20 ransomware types.
- Creation of encryption and decryption codes based on various techniques.
- A JSON-based configuration file for storing ransomware attributes.
- Implementation of file extension targeting and random extension generation.
- Multi-threading support for parallel encryption.
- Basic key hiding techniques.

---

6. Next Steps and Future Enhancements

- **Privilege Escalation Simulation**: The next phase will involve incorporating privilege escalation techniques to simulate how ransomware elevates its access on a victim's machine.
- **State Machine and Architecture for Network Spread**: Future improvements include building a state machine to model how ransomware spreads from one system to another within a network. This will provide a detailed view of ransomware propagation behaviour.
- **Advanced Ransomware Features**: Adding support for more sophisticated ransomware behaviours such as double extortion (where both encryption and data theft occur).

---

7. Conclusion

This ransomware simulator serves as a powerful tool for analysing the behaviour of various ransomware types in a controlled environment. By enabling the customization of ransomware behaviours, encryption methods, and file targeting, this project allows for deep insights into ransomware attacks and their impact. Future enhancements, such as privilege escalation and network propagation, will make the simulator even more comprehensive and useful for cybersecurity research and analysis.