Malware Analysis Report: Akira Ransomware Sample

Analyst: Supreet Bhuvanagiri Sadashiv Shetty
Date: 23/03/2025
Sample Identifier: Akira Ransomware Sample
SHA256: bcae978c17bcddc0bf6419ae978e3471197801c36f73cff2fc88cecbe3d88d1a

---

1. Executive Summary

This report documents the analysis of the **Akira Ransomware Sample** malware, a 64-bit ELF executable targeting Linux environments. The sample is suspected to be a variant of the Akira ransomware. The analysis was performed using static and dynamic analysis techniques with tools such as **Ghidra** and **AnyRun**. This report presents key findings, including indicators of compromise (IOCs) and observed behaviours, to provide insight into the malware's functionality and tactics. As a beginner in cybersecurity and malware analysis, this report demonstrates my developing skills in reverse engineering, dynamic analysis, and threat intelligence.

2. Analysis Objectives

- Identify key functions and behaviors of the malware.
- Extract and document critical indicators such as ransom note messages.
- Analyze the malware's anti-VM and evasion techniques.
- Document dynamic execution behavior using an interactive online sandbox (AnyRun).

3. Tools and Methodology

Tools Used

1. **Ghidra:** For static reverse engineering, decompilation, and string analysis.
2. **Hybrid Analysis:** To obtain initial static and dynamic reports (including Falcon Sandbox results).
3. **AnyRun Sandbox:** For interactive dynamic analysis and behavioral observation.
4. **Linux Command-Line Utilities:** strings, strace, etc.

4. Technical Findings

4.1 Static Analysis

- **File Characteristics:**
  - Type: 64-bit ELF executable (statically linked)
  - Size: 2.68
  - Architecture: x86-64
- **Key Findings in Ghidra:**
  - **Ransom Note Generation:**
    - The ransomware contains a hardcoded ransom message.
    - The message also includes the unique identifier code used for victim tracking.
  - **Anti-VM Techniques:**
    - The sample exhibits known anti-VM tricks (e.g., CPUID checks) as indicated in the Hybrid Analysis report.

4.2 Dynamic Analysis

- **Execution Behavior:**
  - The malware exits with the message "No path to encrypt" when an expected directory structure is not found.
  - System call monitoring (using strace) showed rapid execution and early termination in a non-target environment.
  - The AnyRun sandbox captured the malware's execution in a Linux (Ubuntu 20.04) environment and confirmed anti-analysis behaviors.
- **Indicators of Compromise (IOCs):**
  - **File Hashes:** SHA256, MD5, SHA1 as documented.
  - **Ransom Note:** The embedded ransom message and code for victim tracking
  - **Anti-VM Artifacts:** Presence of CPUID-based VM detection.
  - **YARA Signatures:** Matches for known ransomware patterns (e.g., AES encryption routines).

5. Output

5.1 Ransom Note Output (Ghidra)

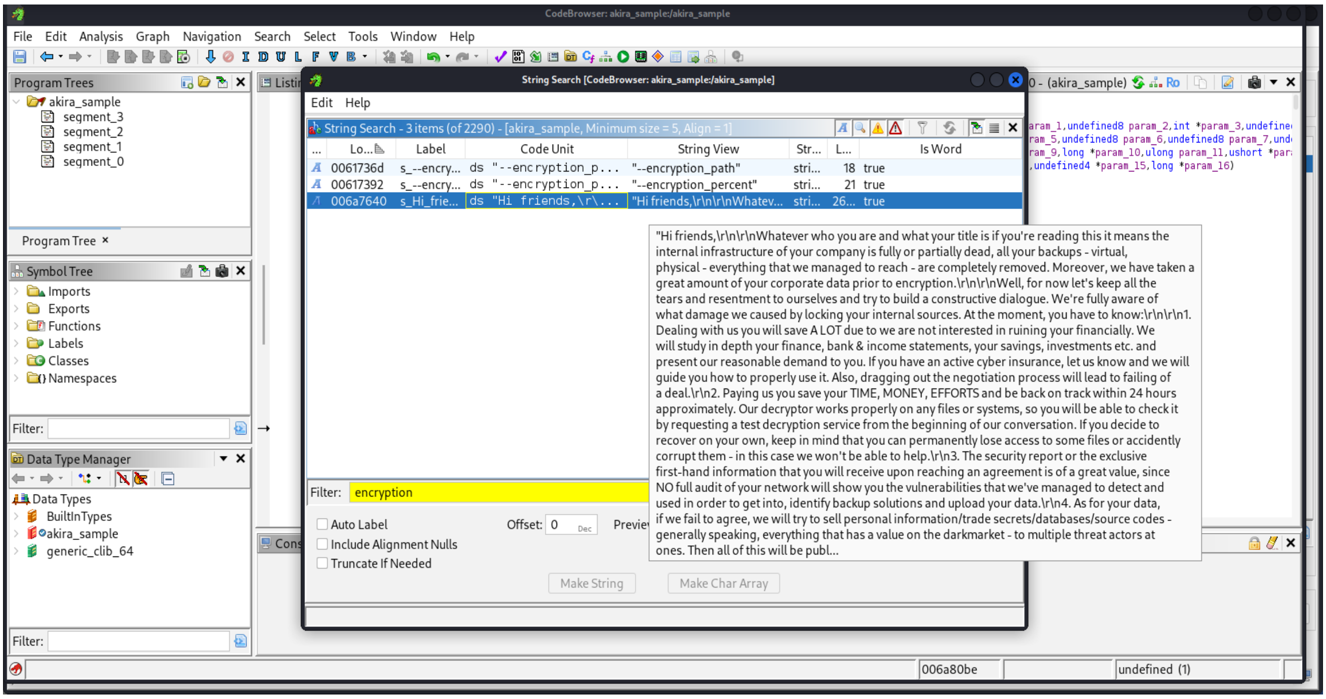

Figure 1: This screenshot shows the ransom note message

5.2 Dynamic Execution Output (AnyRun)

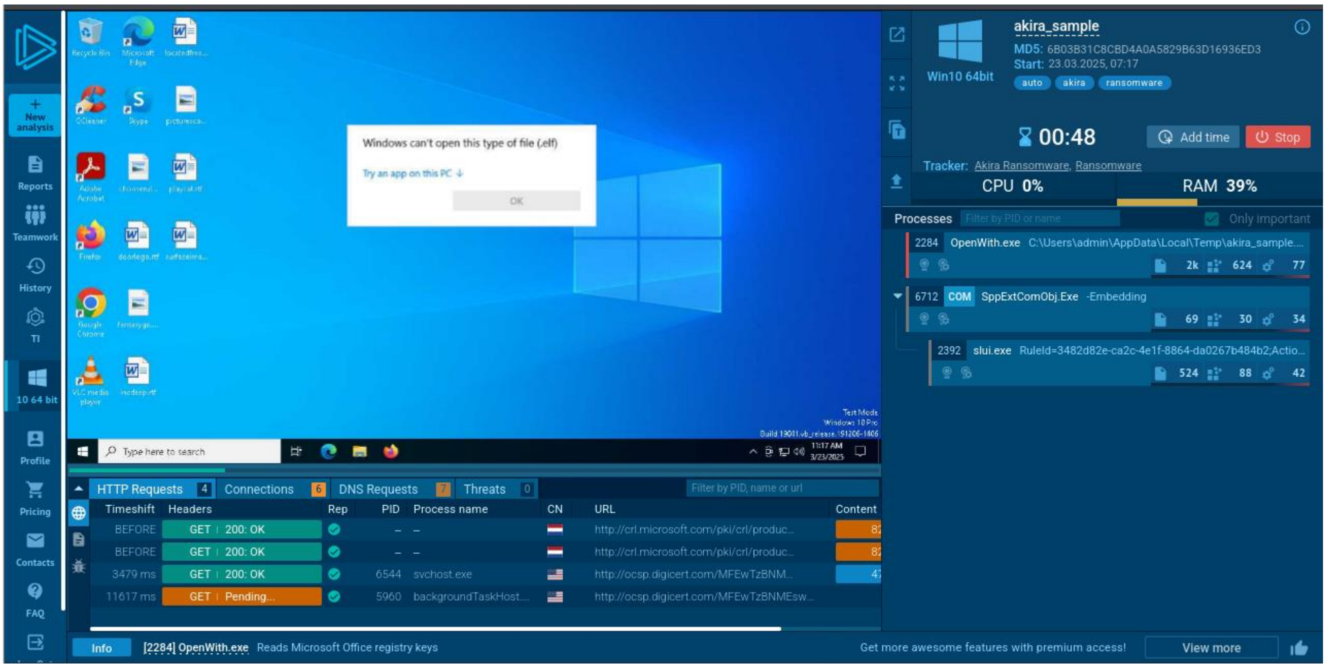

Figure 2: This screenshot captures the malware execution details as observed in the AnyRun interactive sandbox

6. Conclusion:

The analysis of the Akira Ransomware Sample reveals that the malware employs time-based seeding for its cryptographic routines and includes anti-VM evasion techniques. The embedded ransom note serves as a key IOC for tracking and threat intelligence purposes. This exercise demonstrated proficiency in using industry-standard tools such as Ghidra and AnyRun, Hybrid Analysis and provided practical experience in both static and dynamic analysis.