■ ***Tool Name:***

rat-king-parser

History

An open-source project primarily used in malware reverse engineering scenarios. It is often used in conjunction with Java-based RAT (Remote Access Trojan) analysis workflows.

■ ***Description:***

A Java bytecode parser and analysis tool focused on decompiling, analyzing, and extracting indicators from obfuscated Java Remote Access Trojans.

■ ***What Is This Tool About?***

rat-king-parser is designed to analyze obfuscated Java-based RATs by parsing their class structures and helping analysts extract useful Indicators of Compromise (IOCs), command-and-control (C2) URLs, and other behavior signatures.

■ ***Key Characteristics / Features:***

1. Parses Java bytecode (JARs, class files) 2. Identifies obfuscation patterns 3. Extracts hardcoded strings (IPs, domains) 4. Helps map functionality for MITRE ATT&CK; 5. CLI-based automation-friendly 6. Open-source and actively maintained 7. Compatible with Recaf or standalone 8. Outputs IOCs in readable formats

■ ***Types / Modules Available:***

- Class parser - String extractor - Method analyzer - Control-flow visualizer - IOC report generator

■ ***How Will This Tool Help?***

It helps malware analysts reverse engineer Java RATs by simplifying the deobfuscation and code tracing process, extracting actionable threat intel like C2 URLs and suspicious methods.

■ ***Proof of Concept (PoC) Images:***

(Insert screenshots of: terminal output, extracted strings, decompiled code, and C2 domains)

■ ***15-Liner Summary:***

1. CLI-based tool for Java malware 2. Analyzes JAR/class files 3. Extracts IOCs from obfuscated code 4. Lightweight and portable 5. Python-based (easy to modify) 6. Helps with TTP mapping 7. Compatible with Recaf workflows 8. Works on Windows/Linux/Mac 9. Useful in malware triage pipelines 10. No installation needed 11. Outputs JSON/CSV 12. Finds hardcoded IPs, domains 13. MITRE mapping-ready 14. Free and open-source 15. Created for malware analysts

■ ***Time to Use / Best Case Scenarios:***

- When reversing Java-based RATs - During static malware triage - When working with .class or .jar files - In sandbox output triage pipelines

■ ***When to Use During Investigation:***

- In the static analysis phase - During IOC extraction and mapping - While analyzing malware infrastructure - Before YARA rule generation

■■■ *Best Person to Use This Tool & Required Skills:*

Best User: Malware Analyst / Reverse Engineer Required Skills: - Basic Java understanding - Familiarity with bytecode/obfuscation - IOC and malware TTP extraction experience

■ *Flaws / Suggestions to Improve:*

- GUI would make usage easier - Needs better documentation - Could integrate auto-MITRE mapping - Add export to STIX/TAXII formats

■ *Good About the Tool:*

- Fast and lightweight - Effective in analyzing Java RATs - Helps uncover C2 infrastructure - Free and open-source