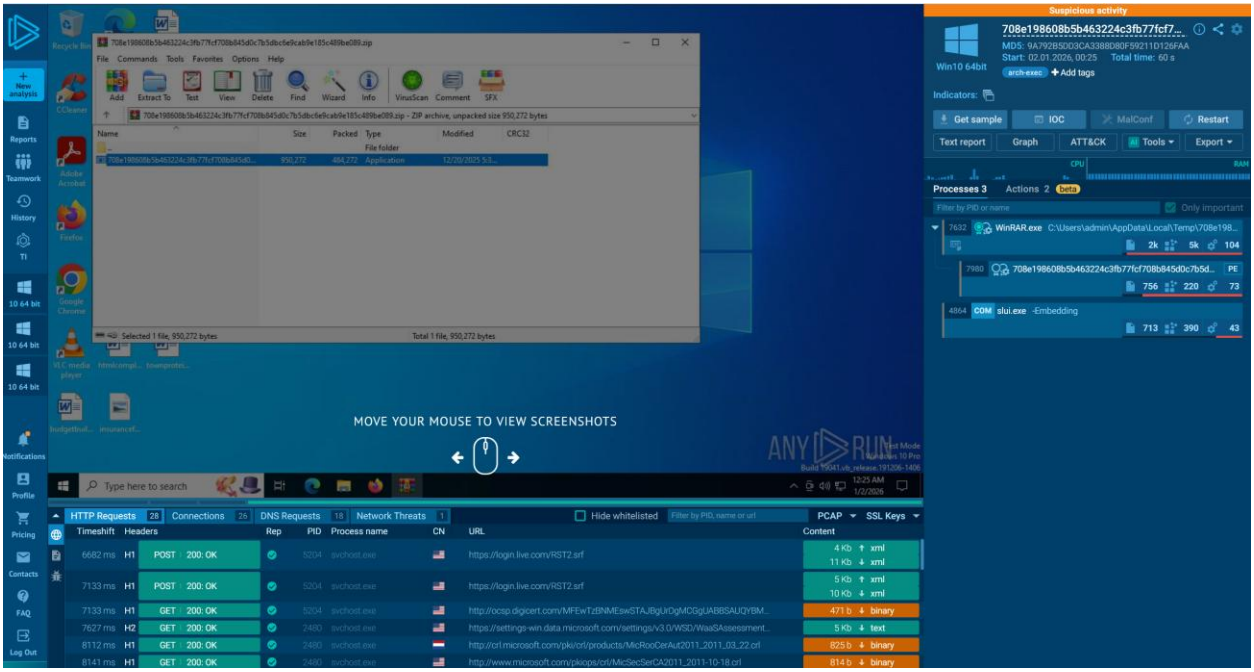
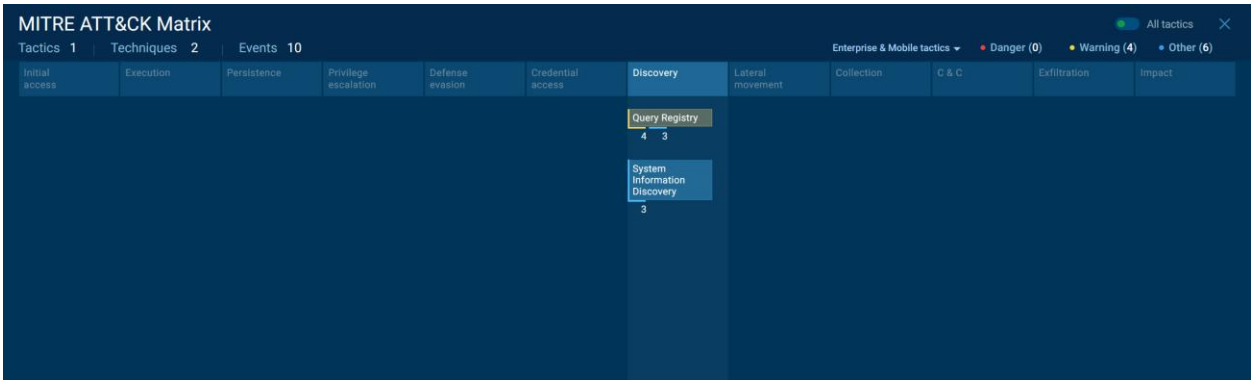
Malware Behavioral Analysis & Intelligence Mapping

By Adam Mohmoud

This project showcases a deep-dive behavioral analysis of a suspicious ZIP archive conducted within the ANY.RUN interactive sandbox environment. The primary objective was to dissect the execution chain of the file, identify high-fidelity Indicators of Compromise (IOCs), and map observed adversary behaviors to the MITRE ATT&CK framework to support detection engineering and incident response.



This lab report documents the behavioral analysis of a suspicious ZIP archive using the ANY.RUN interactive sandbox. The objective was to identify Indicators of Compromise (IOCs), map observed behaviors to the MITRE ATT&CK framework, and interpret potential threat implications.



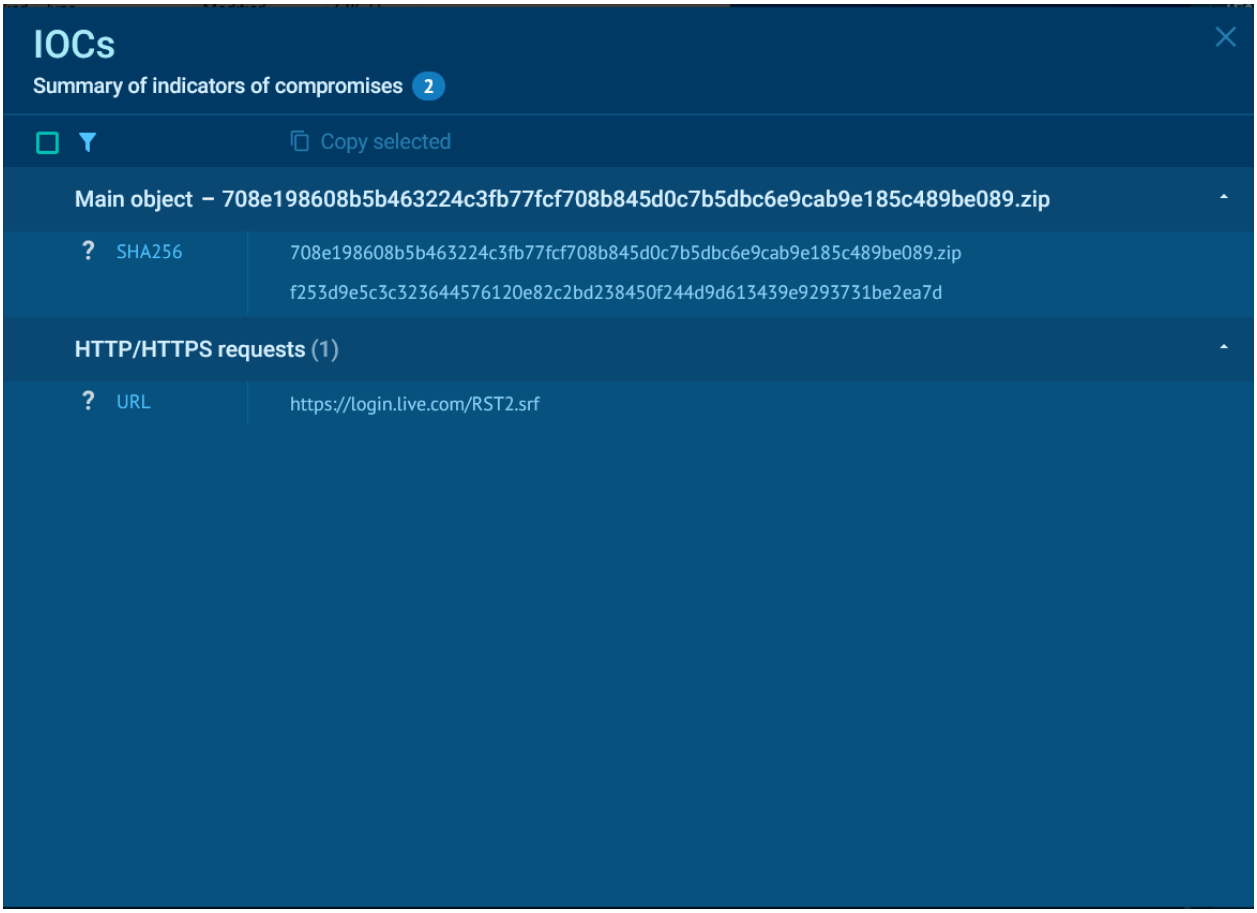
This demonstrates how adversaries use legitimate-looking infrastructure and system reconnaissance to prepare for lateral movement or privilege escalation. Mapping this behavior to the MITRE ATT&CK provides context to the behavior and supports detection engineering and incident response.

T1012 – Query Registry: Adversaries use this technique to extract system configuration, software details, and environment variables from the Windows Registry. This reconnaissance helps tailor payloads, identify security tools, or prepare for privilege escalation. This is used to gather system configuration and software details.

Indicators: Warning detection level: 3 & 4

T1082 – System Information Discovery: Enumerates host details such as OS version, hostname, and hardware to understand the environment they have infiltrated.

Indicators: Warning detection level 3

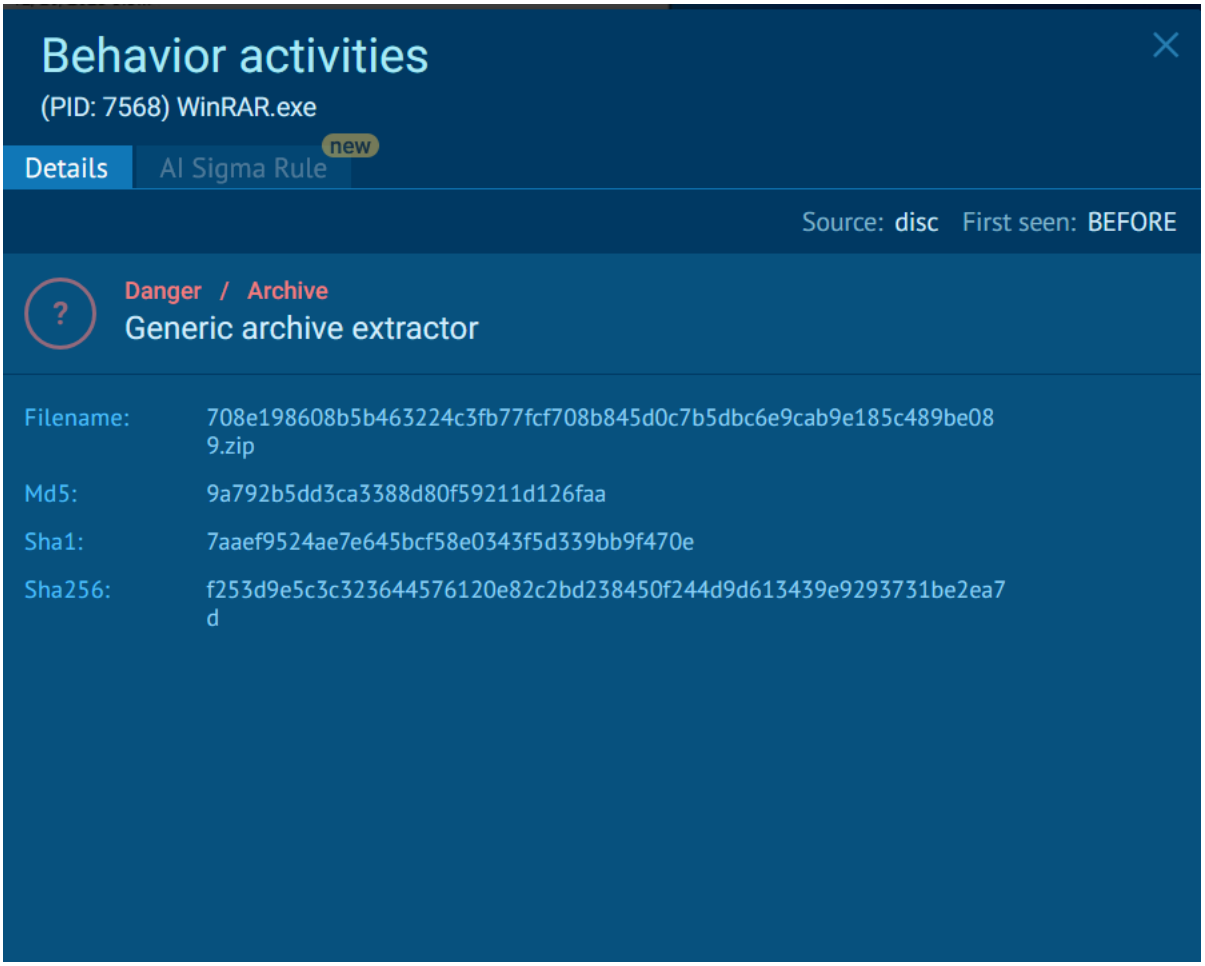


These IOCs suggest the ZIP file is part of a phishing or credential-harvesting campaign. The hash and URL should be blocked or monitored in enterprise environments. The use of a Microsoft domain may be intended to bypass user suspicion or evade basic filters.

File Name: 708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.zip

SHA256 Hash: f253d9e5c3c323644576120e82c2bd238450f244d9d613439e9293731be2ea7d

Behavior: Likely used to deliver or conceal a payload; flagged during sandbox execution.



The sandbox identified WinRAR.exe (PID: 7568) performing a generic archive extraction operation on a suspicious ZIP file. This activity was flagged as “Danger / Archive” due to the context in which the archive was handled rather than the archive tool itself.

Why is this behavior suspicious?

While WinRAR is a legitimate utility, malware frequently abuses archive extractors to:

- Unpack malicious payloads hidden inside compressed files

- Evade static detection by delivering malware in compressed form
- Stage secondary executables or scripts for later execution

Summary

The process tree provided in the JSON shows a single process with the command line "\"C:\\Users\\admin\\AppData\\Local\\Temp\\Rar$EXb7632.19199\\708e198608b5b463224c3fb77fcf708b845d0c7b5dbc6e9cab9e185c489be089.exe\"". The process is located in the temporary folder of the user "admin".

Legitimate programs may use temporary folders to store files during their execution. In this case, the process is located in the temporary folder, which suggests that it may be a legitimate program that is using the temporary folder for its execution.

However, the presence of a long and complex command line, with multiple paths and file names, can also be a sign of malicious activity. Malware often uses obfuscated command lines to hide its true purpose and evade detection. Therefore, further analysis is needed to determine if this process is indeed malicious or if it is a legitimate program using the temporary folder for its execution.