Aria-body, Software S0456 | MITRE ATT&CK®

Archived: 2026-04-02 10:59:04 UTC

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

Aria-body has the ability to duplicate a token from ntprint.exe.[1]

.002 Access Token Manipulation: Create Process with Token

Aria-body has the ability to execute a process using `runas`.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Aria-body has used HTTP in C2 communications.[1]

Enterprise T1010 Application Window Discovery

Aria-body has the ability to identify the titles of running windows on a compromised host.[1]

Enterprise T1560 Archive Collected Data

Aria-body has used ZIP to compress data gathered on a compromised host.[1]

Enterprise T1547 .001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder

Aria-body has established persistence via the Startup folder or Run Registry key.[1]

Enterprise T1025 Data from Removable Media

Aria-body has the ability to collect data from USB devices.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Aria-body has the ability to decrypt the loader configuration and payload DLL.[1]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

Aria-body has the ability to use a DGA for C2 communications.[1]

Enterprise T1083 File and Directory Discovery

Aria-body has the ability to gather metadata from a file and to search for file and directory names.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Aria-body has the ability to delete files and directories on compromised hosts.[1]

Enterprise T1105 Ingress Tool Transfer

Aria-body has the ability to download additional payloads from C2.[1]

Enterprise T1680 Local Storage Discovery

Aria-body has the ability to identify disk information on a compromised host.[1]

Enterprise T1106 Native API

Aria-body has the ability to launch files using `ShellExecute`.[1]

Enterprise T1095 Non-Application Layer Protocol

Aria-body has used TCP in C2 communications.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

Aria-body has used an encrypted configuration file for its loader.[1]

Enterprise T1057 Process Discovery

Aria-body has the ability to enumerate loaded modules for a process.[1].

Enterprise T1055 .001 Process Injection: Dynamic-link Library Injection

Aria-body has the ability to inject itself into another process such as rundll32.exe and dllhost.exe.[1]

Enterprise T1090 Proxy

Aria-body has the ability to use a reverse SOCKS proxy module.[1]

Enterprise T1113 Screen Capture

Aria-body has the ability to capture screenshots on compromised hosts.[1]

Enterprise T1082 System Information Discovery

Aria-body has the ability to identify the hostname, computer name, Windows version, processor speed, and machine GUID on a compromised host.[1]

Enterprise T1016 System Network Configuration Discovery

Aria-body has the ability to identify the location, public IP address, and domain name on a compromised host.[1]

Enterprise T1049 System Network Connections Discovery

Aria-body has the ability to gather TCP and UDP table status listings.[1]

Enterprise T1033 System Owner/User Discovery

Aria-body has the ability to identify the username on a compromised host.[1]
