Azorult, Software S0344 | MITRE ATT&CK®

Archived: 2026-04-05 15:39:29 UTC

Enterprise T1134 .002 Access Token Manipulation: Create Process with Token

Azorult can call WTSQueryUserToken and CreateProcessAsUser to start a new process with local system privileges.[1]

Enterprise T1555 .003 Credentials from Password Stores: Credentials from Web Browsers

Azorult can steal credentials from the victim's browser.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Azorult uses an XOR key to decrypt content and uses Base64 to decode the C2 address.[1][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Azorult can encrypt C2 traffic using XOR.[1][2]

Enterprise T1083 File and Directory Discovery

Azorult can recursively search for files in folders and collects files from the desktop with certain extensions.[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Azorult can delete files from victim machines.[1]

Enterprise T1105 Ingress Tool Transfer

Azorult can download and execute additional files. Azorult has also downloaded a ransomware payload called Hermes.[1][2]

Enterprise T1057 Process Discovery

Azorult can collect a list of running processes by calling CreateToolhelp32Snapshot.[1][2]

Enterprise T1055 .012 Process Injection: Process Hollowing

Azorult can decrypt the payload into memory, create a new suspended process of itself, then inject a decrypted payload to the new process and resume new process execution.[1]

Enterprise T1012 Query Registry

Azorult can check for installed software on the system under the Registry key `Software\Microsoft\Windows\CurrentVersion\Uninstall`.[1]

Enterprise T1113 Screen Capture

Azorult can capture screenshots of the victim's machines.[1]

Enterprise T1082 System Information Discovery

Azorult can collect the machine information, system architecture, the OS version, computer name, Windows product name, the number of CPU cores, video card information, and the system language.[1][2]

Enterprise T1016 System Network Configuration Discovery

Azorult can collect host IP information from the victim's machine.[1]

Enterprise T1033 System Owner/User Discovery

Azorult can collect the username from the victim's machine.[1]

Enterprise T1124 System Time Discovery

Azorult can collect the time zone information from the system.[1][2]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

Azorult can steal credentials in files belonging to common software such as Skype, Telegram, and Steam.[1]
