RCSession, Software S0662 | MITRE ATT&CK®

Archived: 2026-04-05 17:47:44 UTC

Enterprise T1548 .002 Abuse Elevation Control Mechanism: Bypass User Account Control

RCSession can bypass UAC to escalate privileges.[3]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

RCSession can use HTTP in C2 communications.[3][4]

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

RCSession has the ability to modify a Registry Run key to establish persistence.[3][4]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

RCSession can use `cmd.exe` for execution on compromised hosts.[3]

Enterprise T1005 Data from Local System

RCSession can collect data from a compromised host.[4][3]

Enterprise T1573 Encrypted Channel

RCSession can use an encrypted beacon to check in with C2.[1]

Enterprise T1574 .001 Hijack Execution Flow: DLL

RCSession can be installed via DLL side-loading.[1][3][4]

Enterprise T1070 .004 Indicator Removal: File Deletion

RCSession can remove files from a targeted system.[4]

Enterprise T1105 Ingress Tool Transfer

RCSession has the ability to drop additional files to an infected machine.[4]

Enterprise T1056 .001 Input Capture: Keylogging

RCSession has the ability to capture keystrokes on a compromised host.[3][4]

Enterprise T1036 Masquerading

RCSession has used a file named English.rtf to appear benign on victim hosts.[1][3]

Enterprise T1112 Modify Registry

RCSession can write its configuration file to the Registry.[3][4]

Enterprise T1106 Native API

RCSession can use WinSock API for communication including `WSASend` and `WSARecv`.[4]

Enterprise T1095 Non-Application Layer Protocol

RCSession has the ability to use TCP and UDP in C2 communications.[3][4]

Enterprise T1027 .011 Obfuscated Files or Information: Fileless Storage

RCSession can store its obfuscated configuration file in the Registry under `HKLM\SOFTWARE\Plus` or `HKCU\SOFTWARE\Plus`.[3][4]

.015 Obfuscated Files or Information: Compression

RCSession can compress and obfuscate its strings to evade detection on a compromised host.[3]

Enterprise T1057 Process Discovery

RCSession can identify processes based on PID.[4]

Enterprise T1055 .012 Process Injection: Process Hollowing

RCSession can launch itself from a hollowed svchost.exe process.[1][3][4]

Enterprise T1113 Screen Capture

RCSession can capture screenshots from a compromised host.[4]

Enterprise T1218 .007 System Binary Proxy Execution: Msiexec

RCSession has the ability to execute inside the msiexec.exe process.[4]

Enterprise T1082 System Information Discovery

RCSession can gather system information from a compromised host.[4]

Enterprise T1033 System Owner/User Discovery

RCSession can gather system owner information, including user and administrator privileges.[4]
