Cardinal RAT, Software S0348 | MITRE ATT&CK®

Archived: 2026-04-05 15:58:40 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Cardinal RAT is downloaded using HTTP over port 443.[1]

Enterprise T1560 .002 Archive Collected Data: Archive via Library

Cardinal RAT applies compression to C2 traffic using the ZLIB library.[1]

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

Cardinal RAT establishes Persistence by setting the `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load` Registry key to point to its executable.[1]

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

Cardinal RAT can execute commands.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Cardinal RAT decodes many of its artifacts and is decrypted (AES-128) after being downloaded.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Cardinal RAT uses a secret key with a series of XOR and addition operations to encrypt C2 traffic.[1]

Enterprise T1008 Fallback Channels

Cardinal RAT can communicate over multiple C2 host and port combinations.[1]

Enterprise T1083 File and Directory Discovery

Cardinal RAT checks its current working directory upon execution and also contains watchdog functionality that ensures its executable is located in the correct path (else it will rewrite the payload).[1]

Enterprise T1070 .004 Indicator Removal: File Deletion

Cardinal RAT can uninstall itself, including deleting its executable.[1]

Enterprise T1105 Ingress Tool Transfer

Cardinal RAT can download and execute additional payloads.[1]

Enterprise T1056 .001 Input Capture: Keylogging

Cardinal RAT can log keystrokes.[1]

Enterprise T1112 Modify Registry

Cardinal RAT sets `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load` to point to its executable.[1]

Enterprise T1027 .004 Obfuscated Files or Information: Compile After Delivery

Cardinal RAT and its watchdog component are compiled and executed after being delivered to victims as embedded, uncompiled source code.[1]

.013 Obfuscated Files or Information: Encrypted/Encoded File

Cardinal RAT encodes many of its artifacts and is encrypted (AES-128) when downloaded.[1]

Enterprise T1057 Process Discovery

Cardinal RAT contains watchdog functionality that ensures its process is always running, else spawns a new instance.[1]

Enterprise T1055 Process Injection

Cardinal RAT injects into a newly spawned process created from a native Windows executable.[1]

Enterprise T1090 Proxy

Cardinal RAT can act as a reverse proxy.[1]

Enterprise T1012 Query Registry

Cardinal RAT contains watchdog functionality that periodically ensures `HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load` is set to point to its executable.[1]

Enterprise T1113 Screen Capture

Cardinal RAT can capture screenshots.[1]

Enterprise T1082 System Information Discovery

Cardinal RAT can collect the hostname, Microsoft Windows version, and processor architecture from a victim machine.[1]

Enterprise T1033 System Owner/User Discovery

Cardinal RAT can collect the username from a victim machine.[1]

Enterprise T1204 .002 User Execution: Malicious File

Cardinal RAT lures victims into executing malicious macros embedded within Microsoft Excel documents.[1]

Source: https://attack.mitre.org/software/S0348/