QuasarRAT, Software S0262 | MITRE ATT&CK®

Archived: 2026-04-05 13:54:51 UTC

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

QuasarRAT can generate a UAC pop-up Window to prompt the target user to run a command as the administrator. [5]

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

If the QuasarRAT client process does not have administrator privileges it will add a registry key to `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` for persistence.[1][5]

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

QuasarRAT can launch a remote shell to execute commands on the victim's machine.[1][5]

Enterprise T1555 Credentials from Password Stores

QuasarRAT can obtain passwords from common FTP clients.[1][2]

.003 Credentials from Web Browsers

QuasarRAT can obtain passwords from common web browsers.[1][2]

Enterprise T1005 Data from Local System

QuasarRAT can retrieve files from compromised client machines.[5]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

QuasarRAT uses AES with a hardcoded pre-shared key to encrypt network communication.[1][2][5]

Enterprise T1564 .001 Hide Artifacts: Hidden Files and Directories

QuasarRAT has the ability to set file attributes to "hidden" to hide files from the compromised user's view in Windows File Explorer.[5]

.003 Hide Artifacts: Hidden Window

QuasarRAT can hide process windows and make web requests invisible to the compromised user. Requests marked as invisible have been sent with user-agent string `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.75.14 (KHTML, like Gecko) Version/7.0.3 Safari/7046A194A` though QuasarRAT can only be run on Windows systems.[5]

Enterprise T1105 Ingress Tool Transfer

QuasarRAT can download files to the victim's machine and execute them.[1][2]

Enterprise T1056 .001 Input Capture: Keylogging

QuasarRAT has a built-in keylogger.[1][2]

Enterprise T1112 Modify Registry

QuasarRAT has a command to edit the Registry on the victim's machine.[1][5]

Enterprise T1095 Non-Application Layer Protocol

QuasarRAT can use TCP for C2 communication.[5]

Enterprise T1571 Non-Standard Port

QuasarRAT can use port 4782 on the compromised host for TCP callbacks.[5]

Enterprise T1090 Proxy

QuasarRAT can communicate over a reverse proxy using SOCKS5.[1][2]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

QuasarRAT has a module for performing remote desktop access.[1][2]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

QuasarRAT contains a .NET wrapper DLL for creating and managing scheduled tasks for maintaining persistence upon reboot.[2][5]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

A QuasarRAT .dll file is digitally signed by a certificate from AirVPN.[2]

Enterprise T1082 System Information Discovery

QuasarRAT can gather system information from the victim's machine including the OS type.[1]

Enterprise T1614 System Location Discovery

QuasarRAT can determine the country a victim host is located in.[5]

Enterprise T1016 System Network Configuration Discovery

QuasarRAT has the ability to enumerate the Wide Area Network (WAN) IP through requests to ip-api[.]com, freegeoip[.]net, or api[.]ipify[.]org observed with user-agent string `Mozilla/5.0 (Windows NT 6.3; rv:48.0) Gecko/20100101 Firefox/48.0`.[5]

Enterprise T1033 System Owner/User Discovery

QuasarRAT can enumerate the username and account type.[5]

Enterprise T1552 .001 Unsecured Credentials: Credentials In Files

QuasarRAT can obtain passwords from FTP clients.[1][2]

Enterprise T1125 Video Capture

QuasarRAT can perform webcam viewing.[1][2]
