

QUADAGENT, Software S0269 | MITRE ATT&CK®

Archived: 2026-04-05 17:14:08 UTC

Enterprise [T1071 .001 Application Layer Protocol: Web Protocols](#)

[QUADAGENT](#) uses HTTPS and HTTP for C2 communications. ^[1]

[.004 Application Layer Protocol: DNS](#)

[QUADAGENT](#) uses DNS for C2 communications. ^[1]

Enterprise [T1059 .001 Command and Scripting Interpreter: PowerShell](#)

[QUADAGENT](#) uses PowerShell scripts for execution. ^[1]

[.003 Command and Scripting Interpreter: Windows Command Shell](#)

[QUADAGENT](#) uses cmd.exe to execute scripts and commands on the victim's machine. ^[1]

[.005 Command and Scripting Interpreter: Visual Basic](#)

[QUADAGENT](#) uses VBScripts. ^[1]

Enterprise [T1132 .001 Data Encoding: Standard Encoding](#)

[QUADAGENT](#) encodes C2 communications with base64. ^[1]

Enterprise [T1140 Deobfuscate/Decode Files or Information](#)

[QUADAGENT](#) uses AES and a preshared key to decrypt the custom Base64 routine used to encode strings and scripts. ^[1]

Enterprise [T1008 Fallback Channels](#)

[QUADAGENT](#) uses multiple protocols (HTTPS, HTTP, DNS) for its C2 server as fallback channels if communication with one is unsuccessful. ^[1]

Enterprise [T1070 .004 Indicator Removal: File Deletion](#)

[QUADAGENT](#) has a command to delete its Registry key and scheduled task. ^[1]

Enterprise [T1036 .005 Masquerading: Match Legitimate Resource Name or Location](#)

[QUADAGENT](#) used the PowerShell filenames `Office365DCOMCheck.ps1` and `SystemDiskClean.ps1`. ^[1]

Enterprise [T1112 Modify Registry](#)

[QUADAGENT](#) modifies an HKCU Registry key to store a session identifier unique to the compromised system as well as a pre-shared key used for encrypting and decrypting C2 communications.^[1]

Enterprise [T1027 .010 Obfuscated Files or Information: Command Obfuscation](#)

[QUADAGENT](#) was likely obfuscated using `Invoke-Obfuscation`.^{[1][2]}

[.011 Obfuscated Files or Information: Fileless Storage](#)

[QUADAGENT](#) stores a session identifier unique to the compromised system as well as a pre-shared key used for encrypting and decrypting C2 communications within a Registry key (such as `HKCU\Office365DCOMCheck`) in the `HKCU` hive.^[1]

Enterprise [T1012 Query Registry](#)

[QUADAGENT](#) checks if a value exists within a Registry key in the HKCU hive whose name is the same as the scheduled task it has created.^[1]

Enterprise [T1053 .005 Scheduled Task/Job: Scheduled Task](#)

[QUADAGENT](#) creates a scheduled task to maintain persistence on the victim's machine.^[1]

Enterprise [T1016 System Network Configuration Discovery](#)

[QUADAGENT](#) gathers the current domain the victim system belongs to.^[1]

Enterprise [T1033 System Owner/User Discovery](#)

[QUADAGENT](#) gathers the victim username.^[1]

Source: <https://attack.mitre.org/software/S0269/>