Stealth Falcon, Group G0038 | MITRE ATT&CK®

Archived: 2026-04-05 15:33:32 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Stealth Falcon malware communicates with its C2 server via HTTPS.[1]

Enterprise T1059 Command and Scripting Interpreter

Stealth Falcon malware uses WMI to script data collection and command execution on the victim.[1]

.001 PowerShell

Stealth Falcon malware uses PowerShell commands to perform various functions, including gathering system information via WMI and executing commands from its C2 server.[1]

Enterprise T1555 Credentials from Password Stores

Stealth Falcon malware gathers passwords from multiple sources, including Windows Credential Vault and Outlook.[1]

.003 Credentials from Web Browsers

Stealth Falcon malware gathers passwords from multiple sources, including Internet Explorer, Firefox, and Chrome.[1]

.004 Windows Credential Manager

Stealth Falcon malware gathers passwords from the Windows Credential Vault.[1]

Enterprise T1005 Data from Local System

Stealth Falcon malware gathers data from the local victim system.[1]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Stealth Falcon malware encrypts C2 traffic using RC4 with a hard-coded key.[1]

Enterprise T1041 Exfiltration Over C2 Channel

After data is collected by Stealth Falcon malware, it is exfiltrated over the existing C2 channel.[1]

Enterprise T1057 Process Discovery

Stealth Falcon malware gathers a list of running processes.[1]

Enterprise T1012 Query Registry

Stealth Falcon malware attempts to determine the installed version of .NET by querying the Registry.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

Stealth Falcon malware creates a scheduled task entitled "IE Web Cache" to execute a malicious file hourly.[1]

Enterprise T1082 System Information Discovery

Stealth Falcon malware gathers system information via WMI, including the system directory, build number, serial number, version, manufacturer, model, and total physical memory.[1]

Enterprise T1016 System Network Configuration Discovery

Stealth Falcon malware gathers the Address Resolution Protocol (ARP) table from the victim.[1]

Enterprise T1033 System Owner/User Discovery

Stealth Falcon malware gathers the registered user and primary owner name via WMI.[1]

Enterprise T1047 Windows Management Instrumentation

Stealth Falcon malware gathers system information via Windows Management Instrumentation (WMI).[1]
