KGH_SPY, Software S0526 | MITRE ATT&CK®

Archived: 2026-04-05 18:15:10 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

KGH_SPY can send data to C2 with HTTP POST requests.[1]

Enterprise T1037 .001 Boot or Logon Initialization Scripts: Logon Script (Windows)

KGH_SPY has the ability to set the `HKCU\Environment\UserInitMprLogonScript` Registry key to execute logon scripts.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

KGH_SPY can execute PowerShell commands on the victim's machine.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

KGH_SPY has the ability to set a Registry key to run a cmd.exe command.[1]

Enterprise T1555 Credentials from Password Stores

KGH_SPY can collect credentials from WINSCP.[1]

.003 Credentials from Web Browsers

KGH_SPY has the ability to steal data from the Chrome, Edge, Firefox, Thunderbird, and Opera browsers.[1]

.004 Windows Credential Manager

KGH_SPY can collect credentials from the Windows Credential Manager.[1]

Enterprise T1005 Data from Local System

KGH_SPY can send a file containing victim system information to C2.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

KGH_SPY can save collected system information to a file named "info" before exfiltration.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

KGH_SPY can decrypt encrypted strings and write them to a newly created folder.[1]

Enterprise T1114 .001 Email Collection: Local Email Collection

KGH_SPY can harvest data from mail clients.[1]

Enterprise T1041 Exfiltration Over C2 Channel

KGH_SPY can exfiltrate collected information from the host to the C2 server.[1]

Enterprise T1083 File and Directory Discovery

KGH_SPY can enumerate files and directories on a compromised host.[1]

Enterprise T1105 Ingress Tool Transfer

KGH_SPY has the ability to download and execute code from remote servers.[1]

Enterprise T1056 .001 Input Capture: Keylogging

KGH_SPY can perform keylogging by polling the `GetAsyncKeyState()` function.[1]

Enterprise T1680 Local Storage Discovery

KGH_SPY can collect drive information from a compromised host.[1]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

KGH_SPY has masqueraded as a legitimate Windows tool.[1]

Enterprise T1027 .013 Obfuscated Files or Information: Encrypted/Encoded File

KGH_SPY has used encrypted strings in its installer.[1]

Enterprise T1518 Software Discovery

KGH_SPY can collect information on installed applications.[1]

Enterprise T1204 .002 User Execution: Malicious File

KGH_SPY has been spread through Word documents containing malicious macros.[1]
