DarkWatchman, Software S0673 | MITRE ATT&CK®

Archived: 2026-04-05 12:34:40 UTC

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

DarkWatchman uses HTTPS for command and control.[1]

Enterprise T1010 Application Window Discovery

DarkWatchman reports window names along with keylogger information to provide application context.[1]

Enterprise T1217 Browser Information Discovery

DarkWatchman can retrieve browser history.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

DarkWatchman can execute PowerShell commands and has used PowerShell to execute a keylogger.[1]

.003 Command and Scripting Interpreter: Windows Command Shell

DarkWatchman can use `cmd.exe` to execute commands.[1]

.007 Command and Scripting Interpreter: JavaScript

DarkWatchman uses JavaScript to perform its core functionalities.[1]

Enterprise T1132 .001 Data Encoding: Standard Encoding

DarkWatchman encodes data using hexadecimal representation before sending it to the C2 server.[1]

Enterprise T1005 Data from Local System

DarkWatchman can collect files from a compromised host.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

DarkWatchman can stage local data in the Windows Registry.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

DarkWatchman has the ability to self-extract as a RAR archive.[1]

Enterprise T1568 .002 Dynamic Resolution: Domain Generation Algorithms

DarkWatchman has used a DGA to generate a domain name for C2.[1]

Enterprise T1573 .002 Encrypted Channel: Asymmetric Cryptography

DarkWatchman can use TLS to encrypt its C2 channel.[1]

Enterprise T1083 File and Directory Discovery

DarkWatchman has the ability to enumerate file and folder names.[1]

Enterprise T1070 Indicator Removal

DarkWatchman can uninstall malicious components from the Registry, stop processes, and clear the browser history.[1]

.004 File Deletion

DarkWatchman has been observed deleting its original launcher after installation.[1]

Enterprise T1490 Inhibit System Recovery

DarkWatchman can delete shadow volumes using `vssadmin.exe` .[1]

Enterprise T1056 .001 Input Capture: Keylogging

DarkWatchman can track key presses with a keylogger module.[1]

Enterprise T1036 Masquerading

DarkWatchman has used an icon mimicking a text file to mask a malicious executable.[1]

Enterprise T1112 Modify Registry

DarkWatchman can modify Registry values to store configuration strings, keylogger, and output of components.[1]

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

DarkWatchman has used the `csc.exe` tool to compile a C# executable.[1]

.010 Obfuscated Files or Information: Command Obfuscation

DarkWatchman has used Base64 to encode PowerShell commands.[1]

.011 Obfuscated Files or Information: Fileless Storage

DarkWatchman can store configuration strings, keylogger, and output of components in the Registry.[1]

.015 Obfuscated Files or Information: Compression

DarkWatchman has been delivered as compressed RAR payloads in ZIP files to victims.[1]

Enterprise T1120 Peripheral Device Discovery

DarkWatchman can list signed PnP drivers for smartcard readers.[1]

Enterprise T1566 .001 Phishing: Spearphishing Attachment

DarkWatchman has been delivered via spearphishing emails that contain a malicious zip file.[1]

Enterprise T1012 Query Registry

DarkWatchman can query the Registry to determine if it has already been installed on the system.[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

DarkWatchman has created a scheduled task for persistence.[1]

Enterprise T1129 Shared Modules

DarkWatchman can load DLLs.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

DarkWatchman can search for anti-virus products on the system.[1]

Enterprise T1082 System Information Discovery

DarkWatchman can collect the OS version, system architecture, and computer name.[1]

Enterprise T1614 System Location Discovery

DarkWatchman can identity the OS locale of a compromised host.[1]

Enterprise T1033 System Owner/User Discovery

DarkWatchman has collected the username from a victim machine.[1]

Enterprise T1124 System Time Discovery

DarkWatchman can collect time zone information and system `UPTIME`.[1]

Enterprise T1047 Windows Management Instrumentation

DarkWatchman can use WMI to execute commands.[1]
