CHIMNEYSWEEP, Software S1149 | MITRE ATT&CK®

Archived: 2026-04-05 16:30:15 UTC

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

CHIMNEYSWEEP can make use of the Windows `SilentCleanup` scheduled task to execute its payload with elevated privileges.[1]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

CHIMNEYSWEEP can send `HTTP GET` requests to C2.[1]

Enterprise T1115 Clipboard Data

CHIMNEYSWEEP can capture content from the clipboard.[1]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

CHIMNEYSWEEP can invoke the PowerShell command `[Reflection.Assembly]::LoadFile(\"%s\")\n$i=\"\"\n$r=[%s]::%s(\"%s\",[ref] $i)\necho $r,$i\n` to execute secondary payloads.[1]

.005 Command and Scripting Interpreter: Visual Basic

CHIMNEYSWEEP has executed a script named cln.vbs on compromised hosts.[1]

Enterprise T1132 .002 Data Encoding: Non-Standard Encoding

CHIMNEYSWEEP can use a custom Base64 alphabet for encoding C2.[1]

Enterprise T1005 Data from Local System

CHIMNEYSWEEP can collect files from compromised hosts.[1]

Enterprise T1074 .001 Data Staged: Local Data Staging

CHIMNEYSWEEP can store captured screenshots to disk including to a covert store named `APPX.%x%x%x%x%x.tmp` where `%x` is a random value.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

CHIMNEYSWEEP can use an embedded RC4 key to decrypt Windows API function strings.[1]

Enterprise T1480 Execution Guardrails

CHIMNEYSWEEP can execute a task which leads to execution if it finds a process name containing "creensaver." [1]

Enterprise T1041 Exfiltration Over C2 Channel

CHIMNEYSWEEP can upload collected files to the command-and-control server.[1]

Enterprise T1083 File and Directory Discovery

CHIMNEYSWEEP has the ability to enumerate directories for files that match a set list.[1]

Enterprise T1070 .006 Indicator Removal: Timestomp

CHIMNEYSWEEP can time stomp its executable, previously dating it between 2010 to 2021.[1]

Enterprise T1105 Ingress Tool Transfer

CHIMNEYSWEEP can download additional files from C2.[1]

Enterprise T1056 .001 Input Capture: Keylogging

CHIMNEYSWEEP has the ability to support keylogging.[1]

Enterprise T1112 Modify Registry

CHIMNEYSWEEP can use the Windows Registry Environment key to change the `%windir%` variable to point to `c:\Windows` to enable payload execution.[1]

Enterprise T1106 Native API

CHIMNEYSWEEP can use Windows APIs including `LoadLibrary` and `GetProcAddress`.[1]

Enterprise T1027 Obfuscated Files or Information

CHIMNEYSWEEP can use a custom Base64 alphabet to encode an API decryption key.[1]

.001 Binary Padding

The CHIMNEYSWEEP installer has been padded with null bytes to inflate its size.[1]

.007 Dynamic API Resolution

CHIMNEYSWEEP can use `LoadLibrary` and `GetProcAddress` to resolve Windows API function strings at run time.[1]

.009 Embedded Payloads

CHIMNEYSWEEP can extract RC4 encrypted embedded payloads for privilege escalation.[1]

Enterprise T1120 Peripheral Device Discovery

CHIMNEYSWEEP can monitor for removable drives.[1]

Enterprise T1057 Process Discovery

CHIMNEYSWEEP can check if a process name contains "creensaver."[1]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

CHIMNEYSWEEP can use the Windows `SilentCleanup` scheduled task to enable payload execution.[1]

Enterprise T1113 Screen Capture

CHIMNEYSWEEP can capture screenshots on targeted systems using a timer and either upload them or store them to disk.[1]

Enterprise T1518 .001 Software Discovery: Security Software Discovery

CHIMNEYSWEEP is capable of checking whether a compromised device is running DeepFreeze by Faronics.[1]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

CHIMNEYSWEEP has been dropped by a self-extracting archive signed with a valid digital certificate.[1]

Enterprise T1218 .003 System Binary Proxy Execution: CMSTP

CHIMNEYSWEEP can use CMSTP.exe to install a malicious Microsoft Connection Manager Profile.[1]

Enterprise T1033 System Owner/User Discovery

CHIMNEYSWEEP has included the victim's computer name and username in C2 messages sent to actor-owned infrastructure.[1]

Enterprise T1529 System Shutdown/Reboot

CHIMNEYSWEEP can reboot or shutdown the targeted system or logoff the current user.[1]

Enterprise T1102 Web Service

CHIMNEYSWEEP has the ability to use use Telegram channels to return a list of commands to be executed, to download additional payloads, or to create a reverse shell.[1]
