Cobalt Strike, Software S0154 | MITRE ATT&CK®

Archived: 2026-04-05 14:06:54 UTC

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

Cobalt Strike can use a number of known techniques to bypass Windows UAC.[1][2]

.003 Abuse Elevation Control Mechanism: Sudo and Sudo Caching

Cobalt Strike can use `sudo` to run a command.[2]

Enterprise T1134 .001 Access Token Manipulation: Token Impersonation/Theft

Cobalt Strike can steal access tokens from exiting processes.[1][2]

.003 Access Token Manipulation: Make and Impersonate Token

Cobalt Strike can make tokens from known credentials.[1]

.004 Access Token Manipulation: Parent PID Spoofing

Cobalt Strike can spawn processes with alternate PPIDs.[3][2]

Enterprise T1087 .002 Account Discovery: Domain Account

Cobalt Strike can determine if the user on an infected machine is in the admin or domain admin group.[4]

Enterprise T1071 .001 Application Layer Protocol: Web Protocols

Cobalt Strike can use a custom command and control protocol that can be encapsulated in HTTP or HTTPS. All protocols use their standard assigned ports.[1][5][2][6][7]

.002 Application Layer Protocol: File Transfer Protocols

Cobalt Strike can conduct peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.[1][5]

.004 Application Layer Protocol: DNS

Cobalt Strike can use a custom command and control protocol that can be encapsulated in DNS. All protocols use their standard assigned ports.[1][5][2]

Enterprise T1197 BITS Jobs

Cobalt Strike can download a hosted "beacon" payload using BITSAdmin.[8][5][2]

Enterprise T1185 Browser Session Hijacking

Cobalt Strike can perform browser pivoting and inject into a user's browser to inherit cookies, authenticated HTTP sessions, and client SSL certificates.[1][2]

Enterprise T1059 .001 Command and Scripting Interpreter: PowerShell

Cobalt Strike can execute a payload on a remote host with PowerShell. This technique does not write any data to disk.[1][4] Cobalt Strike can also use PowerSploit and other scripting frameworks to perform execution.[9][3][5][2]

.003 Command and Scripting Interpreter: Windows Command Shell

Cobalt Strike uses a command-line interface to interact with systems.[9][5][2][10]

.005 Command and Scripting Interpreter: Visual Basic

Cobalt Strike can use VBA to perform execution.[9][3][5]

.006 Command and Scripting Interpreter: Python

Cobalt Strike can use Python to perform execution.[9][3][5][2]

.007 Command and Scripting Interpreter: JavaScript

The Cobalt Strike System Profiler can use JavaScript to perform reconnaissance actions.[5]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

Cobalt Strike can install a new service.[9]

Enterprise T1132 .001 Data Encoding: Standard Encoding

Cobalt Strike can use Base64, URL-safe Base64, or NetBIOS encoding in its C2 traffic.[2]

Enterprise T1005 Data from Local System

Cobalt Strike can collect data from a local system.[9][2]

Enterprise T1001 .003 Data Obfuscation: Protocol or Service Impersonation

Cobalt Strike can leverage the HTTP protocol for C2 communication, while hiding the actual data in either an HTTP header, URI parameter, the transaction body, or appending it to the URI.[2]

Enterprise T1030 Data Transfer Size Limits

Cobalt Strike will break large data sets into smaller chunks for exfiltration.[1]

Enterprise T1140 Deobfuscate/Decode Files or Information

Cobalt Strike can deobfuscate shellcode using a rolling XOR and decrypt metadata from Beacon sessions.[5][2]

Enterprise T1573 .001 Encrypted Channel: Symmetric Cryptography

Cobalt Strike has the ability to use AES-256 symmetric encryption in CBC mode with HMAC-SHA-256 to encrypt task commands and XOR to encrypt shell code and configuration data.[5]

.002 Encrypted Channel: Asymmetric Cryptography

Cobalt Strike can use RSA asymmetric encryption with PKCS1 padding to encrypt data sent to the C2 server.[5]

Enterprise T1203 Exploitation for Client Execution

Cobalt Strike can exploit Oracle Java vulnerabilities for execution, including CVE-2011-3544, CVE-2013-2465, CVE-2012-4681, and CVE-2013-2460.[5][2]

Enterprise T1068 Exploitation for Privilege Escalation

Cobalt Strike can exploit vulnerabilities such as MS14-058.[9][2]

Enterprise T1083 File and Directory Discovery

Cobalt Strike can explore files on a compromised system.[2]

Enterprise T1564 .010 Hide Artifacts: Process Argument Spoofing

Cobalt Strike can use spoof arguments in spawned processes that execute beacon commands.[2]

Enterprise T1562 .001 Impair Defenses: Disable or Modify Tools

Cobalt Strike has the ability to use Smart Applet attacks to disable the Java SecurityManager sandbox.[5][2]

Enterprise T1070 .006 Indicator Removal: Timestomp

Cobalt Strike can timestomp any files or payloads placed on a target machine to help them blend in.[1][2]

Enterprise T1105 Ingress Tool Transfer

Cobalt Strike can deliver additional payloads to victim machines.[5][2]

Enterprise T1056 .001 Input Capture: Keylogging

Cobalt Strike can track key presses with a keylogger module.[1][11][2]

Enterprise T1112 Modify Registry

Cobalt Strike can modify Registry values within `HKEY_CURRENT_USER\Software\Microsoft\Office\\Excel\Security\AccessVBOM\` to enable the execution of additional code.[5]

Enterprise T1106 Native API

Cobalt Strike's Beacon payload is capable of running shell commands without `cmd.exe` and PowerShell commands without `powershell.exe` [1][5][2]

Enterprise T1046 Network Service Discovery

Cobalt Strike can perform port scans from an infected host.[1][5][2]

Enterprise T1135 Network Share Discovery

Cobalt Strike can query shared drives on the local system.[9]

Enterprise T1095 Non-Application Layer Protocol

Cobalt Strike can be configured to use TCP, ICMP, and UDP for C2 communications.[5][2]

Enterprise T1027 Obfuscated Files or Information

Cobalt Strike can hash functions to obfuscate calls to the Windows API and use a public/private key pair to encrypt Beacon session metadata.[5][2]

.005 Indicator Removal from Tools

Cobalt Strike includes a capability to modify the Beacon payload to eliminate known signatures or unpacking methods.[1][2]

Enterprise T1137 .001 Office Application Startup: Office Template Macros

Cobalt Strike has the ability to use an Excel Workbook to execute additional code by enabling Office to trust macros and execute code without user permission.[5]

Enterprise T1003 .001 OS Credential Dumping: LSASS Memory

Cobalt Strike can spawn a job to inject into LSASS memory and dump password hashes.[2]

.002 OS Credential Dumping: Security Account Manager

Cobalt Strike can recover hashed passwords.[1]

Enterprise T1069 .001 Permission Groups Discovery: Local Groups

Cobalt Strike can use `net localgroup` to list local groups on a system.[2]

.002 Permission Groups Discovery: Domain Groups

Cobalt Strike can identify targets by querying account groups on a domain contoller.[2]

Enterprise T1057 Process Discovery

Cobalt Strike's Beacon payload can collect information on process details.[1][5][2]

Enterprise T1055 Process Injection

Cobalt Strike can inject a variety of payloads into processes dynamically chosen by the adversary.[1][2][12]

.001 Dynamic-link Library Injection

Cobalt Strike has the ability to load DLLs via reflective injection.[5][2]

.012 Process Hollowing

Cobalt Strike can use process hollowing for execution.[9][2]

Enterprise T1572 Protocol Tunneling

Cobalt Strike uses a custom command and control protocol that is encapsulated in HTTP, HTTPS, or DNS. In addition, it conducts peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.[1][2]

Enterprise T1090 .001 Proxy: Internal Proxy

Cobalt Strike can be configured to have commands relayed over a peer-to-peer network of infected hosts. This can be used to limit the number of egress points, or provide access to a host without direct internet access.[1][2]

.004 Proxy: Domain Fronting

Cobalt Strike has the ability to accept a value for HTTP Host Header to enable domain fronting.[2]

Enterprise T1012 Query Registry

Cobalt Strike can query `HKEY_CURRENT_USER\Software\Microsoft\Office\\Excel\Security\AccessVBOM\` to determine if the security setting for restricting default programmatic access is enabled.[5][2]

Enterprise T1620 Reflective Code Loading

Cobalt Strike's `execute-assembly` command can run a .NET executable within the memory of a sacrificial process by loading the CLR.[2]

Enterprise T1021 .001 Remote Services: Remote Desktop Protocol

Cobalt Strike can start a VNC-based remote desktop server and tunnel the connection through the already established C2 channel.[1][13]

.002 Remote Services: SMB/Windows Admin Shares

Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement.[9][10]

.003 Remote Services: Distributed Component Object Model

Cobalt Strike can deliver Beacon payloads for lateral movement by leveraging remote COM execution.[14]

.004 Remote Services: SSH

Cobalt Strike can SSH to a remote service.[9][2]

.006 Remote Services: Windows Remote Management

Cobalt Strike can use `WinRM` to execute a payload on a remote host.[1][2]

Enterprise T1018 Remote System Discovery

Cobalt Strike uses the native Windows Network Enumeration APIs to interrogate and discover targets in a Windows Active Directory network.[1][5][2]

Enterprise T1029 Scheduled Transfer

Cobalt Strike can set its Beacon payload to reach out to the C2 server on an arbitrary and random interval.[1]

Enterprise T1113 Screen Capture

Cobalt Strike's Beacon payload is capable of capturing screenshots.[1][11][2]

Enterprise T1518 Software Discovery

The Cobalt Strike System Profiler can discover applications through the browser and identify the version of Java the target has.[2]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

Cobalt Strike can use self signed Java applets to execute signed applet attacks.[5][2]

Enterprise T1218 .011 System Binary Proxy Execution: Rundll32

Cobalt Strike can use `rundll32.exe` to load DLL from the command line.[2][12][10]

Enterprise T1016 System Network Configuration Discovery

Cobalt Strike can determine the NetBios name and the IP addresses of targets machines including domain controllers.[4][2]

Enterprise T1049 System Network Connections Discovery

Cobalt Strike can produce a sessions report from compromised hosts.[5]

Enterprise T1007 System Service Discovery

Cobalt Strike can enumerate services on compromised hosts.[2]

Enterprise T1569 .002 System Services: Service Execution

Cobalt Strike can use PsExec to execute a payload on a remote host. It can also use Service Control Manager to start new services.[1][9][2]

Enterprise T1550 .002 Use Alternate Authentication Material: Pass the Hash

Cobalt Strike can perform pass the hash.[9]

Enterprise T1078 .002 Valid Accounts: Domain Accounts

Cobalt Strike can use known credentials to run commands and spawn processes as a domain user account.[1][3][2]

.003 Valid Accounts: Local Accounts

Cobalt Strike can use known credentials to run commands and spawn processes as a local user account.[1][3]

Enterprise T1047 Windows Management Instrumentation

Cobalt Strike can use WMI to deliver a payload to a remote host.[1][2][12]
