ATT&CK sub-techniques have now been released! Take a tour, read the blog post or release notes, or see the previous version of the site.

SOFTWARE

- Overview
- 3PARA RAT
- 4H RAT
- ABK
- adbupd
- Adups
- ADVSTORESHELL
- Agent Smith
- Agent Tesla
- Agent.btz
- Allwinner
- Android/Chuli.A
- ANDROIDOS_ANSERVER.A
- AndroRAT
- Anubis
- Aria-body
- Arp
- ASPXSpy
- Astaroth
- at
- Attor
- AuditCred
- AutoIt backdoor
- Avenger
- Azorult
- BabyShark
- BackConfig
- Backdoor.Oldrea
- BACKSPACE
- BADCALL
- BADNEWS
- BadPatch
- Bandook
- Bankshot
- BBK
- BBSRAT
- BISCUIT

Home > Software > Cobalt Strike

Cobalt Strike

Cobalt Strike is a commercial, full-featured, penetration testing tool which bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system. [1]

In addition to its own capabilities, Cobalt Strike leverages the capabilities of other well-known tools such as Metasploit and Mimikatz. [1]

ID: S0154

Type: TOOL

Platforms: Windows

Contributors: Josh Abraham

Version: 1.3

Created: 14 December 2017

Last Modified: 23 June 2020

Version Permalink

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1548	.002	Abuse Elevation Control Mechanism: Bypass User Access Control	Cobalt Strike can use a number of known techniques to bypass Windows UAC.[1]
Enterprise	T1134	.001	Access Token Manipulation: Token Impersonation/Theft	Cobalt Strike can steal access tokens from exiting processes.[1]
		.004	Access Token Manipulation: Parent PID Spoofing	Cobalt Strike can spawn processes with alternate PPIDs.[3]
		.003	Access Token Manipulation: Make and Impersonate Token	Cobalt Strike can make tokens from known credentials.[1]
Enterprise	T1071		Application Layer Protocol	Cobalt Strike conducts peer-to-peer communication over Windows named pipes encapsulated in the SMB protocol. All protocols use their standard assigned ports.[1]
		.004	DNS	Cobalt Strike uses a custom command and control protocol that can encapsulated in DNS. All protocols use their standard assigned ports.[1]
		.001	Web Protocols	Cobalt Strike uses a custom command and control protocol that can be encapsulated in HTTP or HTTPS, or DNS. All protocols use their standard assigned ports.[1]

Bisonal
BITSAdmin
BLACKCOFFEE
BlackEnergy
BONDUPDATER
BOOSTWRITE
BOOTRASH
BrainTest
Brave Prince
Bread
Briba
BS2005
BUBBLEWRAP
build_downer
Bundlore
Cachedump
Cadelspy
CALENDAR
Calisto
CallMe
Cannon
Carbanak
Carbon
Cardinal RAT
CARROTBALL
CARROTBAT
Catchamas
CCBkdr
Cerberus
certutil
Chaos
Charger
ChChes
Cherry Picker
China Chopper
CHOPSTICK
CloudDuke
cmd
Cobalt Strike
Cobian RAT
CoinTicker
Comnie
ComRAT

Domain	ID		Name	Use
Enterprise	T1197		BITS Jobs	Cobalt Strike can download a hosted "beacon" payload using BITSAdmin.[4]
Enterprise	T1059	.003	Command and Scripting Interpreter: Windows Command Shell	Cobalt Strike uses a command-line interface to interact with systems.[2]
		.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] Cobalt Strike can also use PowerSploit and other scripting frameworks to perform execution.[2][3]
		.005	Command and Scripting Interpreter: Visual Basic	Cobalt Strike can use VBA to perform execution.[2][3]
		.006	Command and Scripting Interpreter: Python	Cobalt Strike can use Python to perform execution.[2][3]
Enterprise	T1543	.003	Create or Modify System Process: Windows Service	Cobalt Strike can install a new service.[2]
Enterprise	T1005		Data from Local System	Cobalt Strike can collect data from a local system.[2]
Enterprise	T1068		Exploitation for Privilege Escalation	Cobalt Strike can exploit vulnerabilities such as MS14-058.[2]
Enterprise	T1070	.006	Indicator Removal on Host: Timestomp	Cobalt Strike will timestomp any files or payloads placed on a target machine to help them blend in.[1]
Enterprise	T1056	.001	Input Capture: Keylogging	Cobalt Strike can track key presses with a keylogger module.[1]
Enterprise	T1185		Man in the Browser	Cobalt Strike can perform browser pivoting and inject into a user's browser to inherit cookies, authenticated HTTP sessions, and client SSL certificates.[1]
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]
Enterprise	T1046		Network Service Scanning	Cobalt Strike can perform port scans from an infected host.[1]
Enterprise	T1135		Network Share Discovery	Cobalt Strike can query shared drives on the local system.[2]
Enterprise	T1027	.005	Obfuscated Files or Information: Indicator Removal from Tools	Cobalt Strike includes a capability to modify the "beacon" payload to eliminate known signatures or unpacking methods.[1]
Enterprise	T1003	.002	OS Credential	Cobalt Strike can recover hashed

Concipit1248

CORALDECK

CORESHELL

Corona Updates

CosmicDuke

CozyCar

Crimson

CrossRAT

DarkComet

Daserf

DDKONG

DealersChoice

DEFENSOR ID

Dendroid

Denis

Derusbi

Dipsind

DOGCALL

Dok

down_new

Downdelph

DownPaper

DressCode

Dridex

DroidJack

dsquery

DualToy

Duqu

DustySky

Dvmap

Dyre

Ebury

Elise

ELMER

Emissary

Emotet

Empire

Epic

esentutl

EventBot

EvilBunny

EvilGrab

Domain	ID		Name	Use
Enterprise	T1003	.002	OS Credential Dumping: Security Account Manager	Cobalt Strike can recover hashed passwords.[1]
Enterprise	T1057		Process Discovery	Cobalt Strike's "beacon" payload can collect information on process details.[1]
Enterprise	T1055		Process Injection	Cobalt Strike can inject a variety of payloads into processes dynamically chosen by the adversary.[1]
		.012	Process Hollowing	Cobalt Strike can use process hollowing for execution.[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]
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]
Enterprise	T1021	.002	Remote Services: SMB/Windows Admin Shares	Cobalt Strike can use Window admin shares (C$ and ADMIN$) for lateral movement.[2]
		.006	Remote Services: Windows Remote Management	Cobalt Strike can use `WinRM` to execute a payload on a remote host.[1]
		.004	Remote Services: SSH	Cobalt Strike can SSH to a remote service.[2]
		.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]
		.003	Remote Services: Distributed Component Object Model	Cobalt Strike can deliver "beacon" payloads for lateral movement by leveraging remote COM execution.[5]
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]
Enterprise	T1029		Scheduled Transfer	Cobalt Strike can set its "beacon" payload to reach out to the C2 server on an arbitrary and random interval. In addition it will break large data sets into smaller chunks for exfiltration.[1]
Enterprise	T1113		Screen Capture	Cobalt Strike's "beacon" payload is capable

Exaramel for Linux
Exaramel for Windows
Exodus
Expand
FakeM
FALLCHILL
Felismus
FELIXROOT
Fgdump
Final1stspy
FinFisher
Flame
FLASHFLOOD
FlawedAmmyy
FlawedGrace
FlexiSpy
FLIPSIDE
Forfiles
FruitFly
FTP
Fysbis
Gazer
GeminiDuke
Get2
gh0st RAT
Ginp
GLOOXMAIL
Gold Dragon
GolfSpy
Gooligan
Goopy
GravityRAT
GreyEnergy
GRIFFON
gsecdump
Gustuff
H1N1
Hacking Team UEFI Rootkit
HALFBAKED
HAMMERTOSS
HAPPYWORK
HARDRAIN

of capturing screenshots.[1]

Domain	ID		Name	Use
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][2]
Enterprise	T1550	.002	Use Alternate Authentication Material: Pass the Hash	Cobalt Strike can perform pass the hash.[2]
Enterprise	T1078	.003	Valid Accounts: Local Accounts	Cobalt Strike can use known credentials to run commands and spawn processes as a local user account.[1][3]
		.002	Valid Accounts: Domain Accounts	Cobalt Strike can use known credentials to run commands and spawn processes as a domain user account.[1][3]
Enterprise	T1047		Windows Management Instrumentation	Cobalt Strike can use WMI to deliver a payload to a remote host.[1]

Groups That Use This Software

ID	Name	References
G0073	APT19	[6]
G0079	DarkHydrus	[7][8]
G0052	CopyKittens	[9]
G0050	APT32	[10][11][12][13]
G0080	Cobalt Group	[14][15][16][17] [18][19][20][21]
G0016	APT29	[22]
G0065	Leviathan	[23][24]
G0037	FIN6	[25]
G0096	APT41	[26]

References

1. Strategic Cyber LLC. (2017, March 14). Cobalt Strike Manual. Retrieved May 24, 2017.
2. Cobalt Strike. (2017, December 8). Tactics, Techniques, and Procedures. Retrieved December 20, 2017.
3. Mudge, R. (2017, May 23). Cobalt Strike 3.8 – Who's Your Daddy?. Retrieved June 4, 2019.
14. Svajcer, V. (2018, July 31). Multiple Cobalt Personality Disorder. Retrieved September 5, 2018.
15. Positive Technologies. (2017, August 16). Cobalt Strikes Back: An Evolving Multinational Threat to Finance. Retrieved September 5, 2018.
16. Matveeva, V. (2017, August 15). Secrets of Cobalt. Retrieved October 10, 2018.

Havij

HAWKBALL

hcdLoader

HDoor

Helminth

Hi-Zor

HiddenWasp

HIDEDRV

Hikit

HOMEFRY

HOPLIGHT

HotCroissant

HTRAN

HTTPBrowser

httpclient

HummingBad

HummingWhale

Hydraq

HyperBro

ifconfig

iKitten

Imminent Monitor

Impacket

InnaputRAT

INSOMNIA

InvisiMole

Invoke-PSImage

ipconfig

ISMInjector

Ixeshe

Janicab

JCry

JHUHUGIT

JPIN

jRAT

Judy

KARAE

Kasidet

Kazuar

KeyBoy

Keydnap

KEYMARBLE

4. Strategic Cyber, LLC. (n.d.). Scripted Web Delivery. Retrieved January 23, 2018.
5. Mudge, R. (2017, January 24). Scripting Matt Nelson's MMC20.Application Lateral Movement Technique. Retrieved November 21, 2017.
6. Ahl, I. (2017, June 06). Privileges and Credentials: Phished at the Request of Counsel. Retrieved May 17, 2018.
7. Falcone, R., et al. (2018, July 27). New Threat Actor Group DarkHydrus Targets Middle East Government. Retrieved August 2, 2018.
8. Unit 42. (2017, December 15). Unit 42 Playbook Viewer. Retrieved December 20, 2017.
9. ClearSky Cyber Security and Trend Micro. (2017, July). Operation Wilted Tulip: Exposing a cyber espionage apparatus. Retrieved August 21, 2017.
10. Carr, N.. (2017, May 14). Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations. Retrieved June 18, 2017.
11. Lassalle, D., et al. (2017, November 6). OceanLotus Blossoms: Mass Digital Surveillance and Attacks Targeting ASEAN, Asian Nations, the Media, Human Rights Groups, and Civil Society. Retrieved November 6, 2017.
12. Dahan, A. (2017, May 24). OPERATION COBALT KITTY: A LARGE-SCALE APT IN ASIA CARRIED OUT BY THE OCEANLOTUS GROUP. Retrieved November 5, 2018.
13. Dahan, A. (2017). Operation Cobalt Kitty. Retrieved December 27, 2018.
17. Mesa, M, et al. (2017, June 1). Microsoft Word Intruder Integrates CVE-2017-0199, Utilized by Cobalt Group to Target Financial Institutions. Retrieved October 10, 2018.
18. Klijnsma, Y.. (2017, November 28). Gaffe Reveals Full List of Targets in Spear Phishing Attack Using Cobalt Strike Against Financial Institutions. Retrieved October 10, 2018.
19. Klijnsma, Y.. (2018, January 16). First Activities of Cobalt Group in 2018: Spear Phishing Russian Banks. Retrieved October 10, 2018.
20. CrowdStrike. (2018, February 26). CrowdStrike 2018 Global Threat Report. Retrieved October 10, 2018.
21. Giagone, R., Bermejo, L., and Yarochkin, F. (2017, November 20). Cobalt Strikes Again: Spam Runs Use Macros and CVE-2017-8759 Exploit Against Russian Banks. Retrieved March 7, 2019.
22. Dunwoody, M., et al. (2018, November 19). Not So Cozy: An Uncomfortable Examination of a Suspected APT29 Phishing Campaign. Retrieved November 27, 2018.
23. Axel F, Pierre T. (2017, October 16). Leviathan: Espionage actor spearphishes maritime and defense targets. Retrieved February 15, 2018.
24. FireEye. (2018, March 16). Suspected Chinese Cyber Espionage Group (TEMP.Periscope) Targeting U.S. Engineering and Maritime Industries. Retrieved April 11, 2018.
25. McKeague, B. et al. (2019, April 5). Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware. Retrieved April 17, 2019.
26. Glyer, C, et al. (2020, March). This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits. Retrieved April 28, 2020.

KeyRaider

Kivars

Koadic

Komplex

KOMPROGO

KONNI

Kwampirs

LaZagne

LightNeuron

Linfo

Linux Rabbit

LockerGoga

LoJax

Lokibot

LoudMiner

LOWBALL

Lslsass

Lurid

Machete

MacSpy

MailSniper

Marcher

Matroyshka

MazarBOT

MAZE

MechaFlounder

meek

MESSAGETAP

Metamorfo

Micropsia

Mimikatz

MimiPenguin

Miner-C

MiniDuke

MirageFox

Mis-Type

Misdat

Mivast

MobileOrder

Monokle

MoonWind

More_eggs

Mosquito

MURKYTOP

Naid

NanHaiShu

NanoCore

NavRAT

nbtstat

NDiskMonitor

Nerex

Net

Net Crawler

NETEAGLE

netsh

netstat

NetTraveler

Netwalker

NETWIRE

Nidiran

njRAT

Nltest

NOKKI

NotCompatible

NotPetya

OBAD

OceanSalt

Octopus

Okrum

OLDBAIT

OldBoot

Olympic Destroyer

OnionDuke

OopsIE

Orz

OSInfo

OSX/Shlayer

OSX_OCEANLOTUS.D

OwaAuth

P2P ZeuS

Pallas

Pasam

Pass-The-Hash Toolkit

Pegasus for Android

Pegasus for iOS

PHOREAL

PinchDuke

Ping

Pisloader

PJApps

PLAINTEE

PLEAD

PlugX

pngdowner

PoetRAT

PoisonIvy

Pony

POORAIM

PoshC2

POSHSPY

Power Loader

PowerDuke

PowerShower

POWERSOURCE

PowerSploit

PowerStallion

POWERSTATS

POWERTON

POWRUNER

Prikormka

Proton

Proxysvc

PsExec

Psylo

Pteranodon

PUNCHBUGGY

PUNCHTRACK

Pupy

pwdump

QUADAGENT

QuasarRAT

Ragnar Locker

Ramsay

RARSTONE

RATANKBA

RawDisk

RawPOS

RCSAndroid

RDFSNIFFER

Reaver

RedDrop

RedLeaves

Reg

Regin

Remcos

Remexi

RemoteCMD

Remsec

Responder

Revenge RAT

RGDoor

Rifdoor

Riltok

RIPTIDE

Rising Sun

RobbinHood

ROCKBOOT

RogueRobin

ROKRAT

Rotexy

route

Rover

RTM

Ruler

RuMMS

RunningRAT

Ryuk

S-Type

Sakula

SamSam

schtasks

SDBot

SDelete

SeaDuke

Seasalt

SEASHARPEE

ServHelper

Shamoon

SHARPSTATS

ShiftyBug

ShimRat

ShimRatReporter

SHIPSHAPE

SHOTPUT

SHUTTERSPEED

SimBad

Skeleton Key

Skidmap

Skygofree

SLOWDRIFT

Smoke Loader

SNUGRIDE

Socksbot

SOUNDBITE

SPACESHIP

SpeakUp

spwebmember

SpyDealer

SpyNote RAT

sqlmap

SQLRat

SslMM

Starloader

Stealth Mango

StoneDrill

StreamEx

Sykipot

SynAck

Sys10

SYSCON

Systeminfo

T9000

Taidoor

TajMahal

Tangelo

Tasklist

TDTESS

TEXTMATE

TINYTYPHON

TinyZBot

- Tor
- Triada
- TrickBot
- TrickMo
- Trojan-SMS.AndroidOS.Agent.ao
- Trojan-SMS.AndroidOS.FakeInst.a
- Trojan-SMS.AndroidOS.OpFake.a
- Trojan.Karagany
- Trojan.Mebromi
- Truvasys
- TSCookie
- TURNEDUP
- Twitoor
- TYPEFRAME
- UACMe
- UBoatRAT
- Umbreon
- Unknown Logger
- UPPERCUT
- Uroburos
- Ursnif
- USBferry
- USBStealer
- Valak
- Vasport
- VBShower
- VERMIN
- ViceLeaker
- Volgmer
- WannaCry
- WEBC2
- Wiarp
- Windows Credential Editor
- WINDSHIELD
- WindTail
- WINERACK
- Winexe
- Wingbird
- WinMM
- Winnti for Linux

- Winnti for Linux
- Winnti for Windows
- Wiper
- WireLurker
- X-Agent for Android
- XAgentOSX
- Xbash
- Xbot
- xCmd
- XcodeGhost
- XLoader
- XTunnel
- YAHOYAH
- YiSpecter
- yty
- Zebrocy
- ZergHelper
- Zeroaccess
- ZeroT
- Zeus Panda
- ZLib
- zwShell
- ZxShell