BLOG ARTICLE

Look how many cybercriminals love Cobalt Strike

MAY 19, 2021

Since its release in 2012, Cobalt Strike has been one of the most popular tools for penetration testers to use when simulating how known threat actor tools will look when targeting an organization's network. However, there is a downside to that popularity: the criminals love it, too. And if they are using it, it's definitely not to simulate any sort of attack.

Cobalt Strike has become a very common second-stage payload for many malware campaigns across many malware families. Access to this powerful and highly flexible tool has been limited by the product's developers, but leaked versions have long spread across the internet. Additionally, there are tons of tutorials, education videos and other public documentation that can help newcomers understand how to effectively use it, lowering the bar for entry in the cybercrime world.

The cybercrime underground's adoption of Cobalt Strike correlates with the rise in ransomware activity over the past few years, while also being tied to numerous other types of malware that either lead to ransomware attacks, data exfiltration, or both. Despite all of the cybercriminal activity that can be launched with this pen testing tool, it can be difficult to figure out who is actually controlling a malicious Cobalt Strike team server. Additionally, Cobalt Strike allows users to build "malleable" command and control, which allows for easy modifications of network signatures.

Despite the obfuscation techniques, Intel 471 has collected a wealth of information on how the cybercrime underground has refashioned this security tool to its advantage. The following takes a deeper look at which threat actor groups and malware families are dropping Cobalt Strike for post-exploitation.

Trickbot

It should come as no surprise that Trickbot is on this list. Public reports of Trickbot operators dropping Cobalt Strike go back to 2019 [1].

We recently observed Trickbot infections associated with a specific "gtag" — a tracking ID used by the malware's developers — directly dropping Cobalt Strike stagers that were code-signed by Sectigo.

Trickbot operators using the "**rob**" gtag pushed a variety of Cobalt Strike stagers (http, https, x86, x64) through Trickbot's download-and-execute capabilities (command 43). Each Cobalt Strike variant was fetched from the very same server (http[:]//107.173.49.118) and tried to connect to https[:]//olhnmn.com (http[:]//217.12.201.194) based on the preferred communication protocol. We noticed that the Malleable-C2 profile was based off this public profile on Github:

`https://github.com/threatexpress/malleable-c2/blob/master/jquery-c2.3.11.profile`

Other researchers have also written about Cobalt Strike activity originating from TrickBot infections. Walmart Global Tech [2] has published details from a ransomware operation involving Cobalt Strike leveraged by a group utilizing the Trickbot banking trojan. The watermark — a distinct number attached to the make and model of Cobalt Strike — observed in the payload is **1359593325**.

Another security researcher has detailed in his blog [3] the phases that originated with an Emotet infection, a subsequent Trickbot install, plus the use of a series of plot-exploitation tools and frameworks that eventually took advantage of Cobalt Strike.

As an example, Cobalt Strike was loaded in an advanced stage of the operation detailed in the blog post above. Our events registering Cobalt Strike as a download & execute were recorded right after Trickbot issued the modules that the malware fetches when initiating an infection. That may be an indicator that different threat groups may be using the same tool, but leveraged different TTPs.

As a reference, the following table gathers the Cobalt Strike hashes collected by our tracking that were originated with Trickbot "**rob"** gtag:

SAMPLE NAME	SHA256
crypt_run2.exe	246c91ac7955ba97cc3c1aaf7b35a1798b72d7a3f82dca445e2e40

crypt_run1.exe	c4b4eb963c91fb4e82b0fbe510c35212d1f59850de82b04b0916ffd0cf5ef2af
https_444_x86.exe	d67baca49193bd23451cca76ff7a08f79262bf17fb1d8eb7adaf7296dca77ad6
https_444_x64.exe	12dd3add463863ab1f294f2038e5832ff5e0adf2a3ca28e42202a0705c6f3cec
http_444_x86.exe	7c76a27f3f9af16b5f7872e4bb459f0d4860d295d60e5f88fdc0eec16972e093
http_444_x64.exe	28c3f5bcedbea2c97d5baa8c12353d6c79ba0cb94512f322487dc166b54fdb27

The Cobalt Strike watermark that Intel 471 discovered from Trickbot payloads is **305419896**.

Other sources have also reported Cobalt Strike activity originating from the **rob** Trickbot infections. In May 2021, The DFIR report [4] blogged their observations when discovering Cobalt Strike activity after an intrusion that started with Trickbot.

Even though the same gtag is behind both Cobalt Strike deployments, the configuration extracted from the beacons completely differs from those observed in the DFIR Report article. This may suggest multiple threat actors are performing post-infection activity that leads to ransomware and data exfiltration. It could also mean that the operators pay close attention to operational security and try to avoid re-using infrastructure or methodologies across different attacks.

Hancitor

The actors behind Hancitor use Cobalt Strike, but this hasn't always been the case. This threat actor group preferred to drop the Gozi ISFB trojan and Evil Pony credential harvester until mid-2019, when the group replaced Gozi ISFB with Cobalt Strike. This switch serves as a signal of when the group may have decided to pursue ransomware instead of account takeovers. As we will demonstrate later in this section, the Cobalt Strike deployments from Hancitor payloads are strikingly similar. This leads us to believe one threat-actor group is managing these particular Cobalt Strike team servers, as well as the infected machines.

The group setting up the Cobalt Strike team servers related to Hancitor prefer to host their CS beacons on hosts without a domain. The CS beacons will call home to the same set of IPs. Stagers are downloaded from infrastructure set up via Yalishanda bulletproof hosting service.

It's important to note that Hancitor only drops Cobalt Strike on machines that are connected to a Windows domain. When this condition isn't met, Hancitor may drop SendSafe (a spambot), the Onliner IMAP checker, or the Ficker information stealer.

Stager distribution URLs (where Hancitor fetches CS stagers):

```
http://tren0[.]ru/0504.bin

http://tren0[.]ru/0504s.bin

http://pipopetfiu[.]ru/0104.bin

http://s5iwc[.]ru/0804s.bin

http://pipopetfiu[.]ru/0104s.bin

http://clublifes[.]ru/2903.bin

http://45des29[.]ru/1504s.bin

http://bambinoska[.]ru/2104.bin

http://g1smurt[.]ru/2303s.bin

http://man70[.]ru/2204s.bin

http://masaddrino[.]ru/1904.bin

http://q17ar45[.]ru/3003s.bin

http://gru77[.]ru/2704.bin

http://derferper[.]ru/1204s.bin

http://pirijinko[.]ru/1703s.bin
```

http://67xfjk[.]ru/0704.bin

Stager download URLs (CS stagers fetch CS beacon from here):

http://185.172.129[.]132:80/jDEi

http://192.95.16[.]245:80/OMkU

http://37.1.211[.]126:80/tV9Y

http://45.136.113[.]10:80/fk5V

http://45.138.27[.]44:80/w9aK

http://45.176.188[.]137:80/pFq5

http://66.165.240[.]211:80/l9Jm

http://74.121.191[.]2:80/wXY4

http://74.50.60[.]96:80/9Wic

http://80.92.205[.]9:80/CbKl

http://82.117.252[.]78:80/zGi2

Beacon C2 URLs (Beacons check in here):

https://74.50.60[.]96/cx

http://192.95.16[.]245/activity

https://45.176.188[.]137/ptj

https://45.136.113[.]10/dpixel

http://80.92.205[.]9/cx

https://80.92.205[.]9/updates.rss

```
https://173.199.115[.]116/cm

http://185.172.129[.]132/j.ad

https://80.92.205[.]9/__utm.gif
```

The public RSA key used by Hancitor team's Cobalt Strike beacons doesn't change often. The key we observe in recent samples is:

```
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnOM3nXx+7HBhkbDd+AwFrFisSunK999w2tM
0uTpuuEiBalcJhcL+QgQWtf6S7zPp5hjImG+2YcPl18geU4f5JlSPXHwilbK4DFb/ePWyKFjhr
A7emVRqhM21QMlo1ANsn14rY/RO2pzuft8P7TXoIjjI/B2GGVuzYNZX6X4I2EwIDAQABAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==
```

Qbot

While it has been around since 2007, the banking trojan Qbot (or Qakbot) is still being used by cybercriminals. Not only do the core components receive major updates every few months, but due to its modular design, the developers are able to push a variety of plug-ins to enhance the bot's capabilities. One of these plug-ins equips the bot with the tools to join the CobaltStrike trend.

Our Qbot tracking has registered attempts to load these CobaltStrike loader binaries. The controller instruction here differs from other families as the CobaltStrike loader is shipped to Qbot bots as a plug-in. The download plug-in directive reveals the internal name given to the plug-in DLL by Qbot developers: **plugin_cobalt_power3.**

An example of a **plugin_cobalt_power3** collected from Qbot is available in the table below.

SHA256	Controller
cd406baf24626545dc66102b593fdf70b1922d9497e95a92b1a2e5db277603e0	https://saferem[.]com

Skip to content

The configuration extracted from the Qbot-related Cobalt Strike beacon doesn't show any links to any other groups that we are aware of. Additionally, the CobaltStrike watermark from the beacon is **1580103814**.

When comparing this activity to samples reported by other researchers, we observed different public malleable-C2 profiles used, but commonalities in hosting infrastructure.

SystemBC

SystemBC is malware leveraging socket secure internet protocol (SOCKS5) to hide malicious traffic and to evade detection. It includes download and execute functionalities and supports self-updates. Cybersecurity firm Proofpoint published an extensive report in August 2019 about this malware family [5].

SystemBC is often observed as one part of an extensive infection chain. Some targeted ransomware operators seem to use it to maintain a secondary backdoor channel into a breached network. We observed SystemBC dropping Cobalt Strike during mid-to-late 2020 and early 2021. Let's see an overall summary of the SystemBC activity that leads to Cobalt Strike being dropped:

SystemBC controller	tcp[:]//80.85.84.79:4001
Activity period	Nov. 15, 2020 - Nov. 27, 2020
Nov 15	It downloaded a Cobalt Strike Beacon from: `http[:]//activedirectorysearch.com:8000/beac_prx8.exe` Hash: `d5f3ba52e0b71e8367636d60b13722b184cc764be4af0226429fe2a656c6653c`

	Watermark: 305419896
Nov 24	It downloaded Cobalt Strike Beacon from: http[:]//activedirectorysearch.com:8000/beac_prx8.exe Hash: 5e5e25a926e27bdd67ffcbace103dc5d0e0cdcf2f04c9fb17d92e3bb1a85086c Controller: https[:]//activedirectorysearch.com/api/beta/Users(Watermark: <unknown>
Nov 27	It tried to download an unknown sample from: https[:]//activedirectorysearch.com/crypt_socks.exe The sample was not found.

This SystemBC controller was only active during that short period of time and only downloaded those samples. We cannot link this IP to any known actor or infrastructure. Also, the controller configured in those Cobalt Strike samples does not appear in any other sample we have in our collection.

The domain is still active and the server is up, but there is no trace to Cobalt Strike resources. The IP, 212.47.228[.]134, which is the one hosting 'activedirectorysearch[.]com' responds with a 'bad gateway' message, which means that it was an nginx reverse proxy and the endpoint is not connected anymore. This IP is linked to several pieces of malware and has hosted a lot of malicious activity. By looking at all traces in VirusTotal, we can see multiple domains and resources with traces to phishing attacks, APK deployment, and more malicious activities.

System BC controller	tcp[:]//172.105.253.97:4001
Activity period	Nov. 29, 2020 - Dec. 15, 2020

Nov. 29 - Dec. 10	It downloaded a VBS script used for doing reconnaissance of Windows networks:
	`http[:]//172.105.253.97/systembc/exec.vbs`
	
	Hash:
	
	`e86d3fd7a2ff1bc75d750b661dfd3ab357b611028abfbbedd4653b930160d6d2`
	
	Summary: The script was an early stage reconnaissance tool aimed at adding a new user on the victim machine, making this user an administrator, enabling remote desktop capability and collecting network information about the infected machine. The tactics, techniques and procedures (TTPs) used by the operator or operators of the VBScript tool suggested they might be operating undisclosed ransomware and using the script at the initial compromise stage and to conduct reconnaissance in the system.
	
	Through the course of our research, we identified 18 entities in Canada, Germany, Ireland, Luxembourg, the U.K. and the U.S. where the script was deployed.

Dec. 10 - Dec. 11	It downloaded Cobalt Strike Beacon from: `http[:]//172.105.253.97/coba.exe` Hash:

	Controller:https://lsass.cloud/pixel Watermark: 0
Dec. 15	It tried to download an unknown sample from: http[:]//172.105.253.97/all_xxx.exe And also downloaded Cobalt Strike Loader from: http[:]//172.105.253.97/artif_pp.exe Hash: 6b3991d59e49312c4f6dc09ba900d4cff475598e6a190da340466313be48c4f3 Controller: https[:]//lsass.cloud:443/1kxH

The infrastructure used for this operation was shared between SystemBC and CobaltStrike. The IPs used in SystemBC and also for all CobaltStrike stages (beacon drop and controllers), including also the domain 'lsass.cloud' - which resolved to 172.105.34.105, hosted by Linode.

Something interesting to notice here is that there are also some Cobalt Strike stager

dropped by SystemBC. This demonstrates what other researchers have also found, that SystemBC is used as an alternative backdoor into breached networks.

```
Cobalt Strike stager:
575f230f54f769aa3a9ea3a5e76d64a8419501d16651fac0c0e2247f4a41e16e

Download URL:https[:]//lsass.cloud:443/2tsC

Cobalt Strike
Beacon:5259695c25fa6cc27334d3c9d16a307f1762ca0aa3b0cc3e153f271b2df4e6c4

Controller: "https[:]//lsass.cloud/api/beta/Users('
```

Using OSINT it's possible to find some more CobaltStrike samples sharing this domain:

```
https[:]//lsass.cloud/pixel

https[:]//lsass.cloud/g.pixel

https[:]//lsass.cloud/dpixel

https[:]//lsass.cloud/8Amv

https[:]//lsass.cloud:443/1kxH
```

Smokeloader

Cobalt Strike is most often selectively deployed on targets that meet a certain criteria. However, Intel 471 found an instance where Cobalt Strike was haphazardly deployed across a range of infected systems, alongside several other malware samples. This was most likely the work of a malware install service, where threat actors can buy "loads" (installs) in bulk.

The nexus of this activity was an actor that maintains large botnets made up of a modular loader known as Smokeloader, which was revealed in 2011 and exists in resident and non-resident versions. Despite its age, Smokeloader still is used in the wild and received several code updates from its author, **Smokeldr**. It includes a lot of features and accepts multiple modules. It is able to steal files, browser data and

The typical payloads distributed by this threat actor are various stealers and RATs. However, on one occasion, Intel 471 uncovered a Cobalt Strike stager.

The controller which delivered the download command was:

```
h[tt]p://dsdett[.]com/upload/
```

This Smokeloader controller was hosted by a bulletproof hoster known as CCweb (also known as Fluxxy). The CS stager was downloaded from:

```
h[tt]p://persoonlijknab[.]com/putty.exe
```

Cobalt Strike beacon was downloaded from:

```
h[tt]p://164.90.173[.]158:80/VYy4
```

and reported back to:

```
http://164.90.173[.]158/push
```

This Cobalt Strike control server was hosted at Digital Ocean, and was found with a watermark of **1359593325**.

What this shows us is even lower-tier cybercriminals that are buying installs, rather than setting up their own dedicated infection campaigns are using Cobalt Strike

Bazar

Bazar is a loader and backdoor pair that emerged in April 2020. Also known as Baza, the backdoor allows its operators to execute commands, exfiltrate files and download additional malware onto an infected system.

Incidents of the Bazar backdoor downloading and executing Cobalt Strike have been documented in other previous reports.

In late March 2021 Intel 471's automated tracking systems received commands to

the deployment of Cobalt Strike on hosts deemed of interest to the operators. As such, it is also a precursor to data exfiltration and deployment of ransomware performed by targeted ransomware operators.

```
@echo off

echo General Info:

systeminfo



echo.

echo My Username:

whoami



echo.

echo Network Neighbourghoud:

net view /all



echo.

echo Domain Neighbourghoud:

net view /all /domain



echo.

echo Domain Trust:

nltest /domain_trusts /all_trusts
```

```
echo.

echo Installed Programs:

reg query hklm\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /v
"DisplayName" /s



echo.

echo Installed Programs (wow64):

reg query
hklm\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall /v
"DisplayName" /s



echo.

echo Installed Programs (current user):

reg query hkcu\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /v
"DisplayName" /s



echo.

echo Installed Programs (current user, wow64):

reg query
hkcu\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall /v
"DisplayName" /s



echo.
```

```
echo Process List:

tasklist
```

In early 2021, Bazar campaigns were distributing a Cobalt Strike loader variant instead of the conventional Bazar loader. The samples were signed and fully undetectable by antivirus engines on platforms such as VirusTotal at the time of those campaigns. Below are some artifacts from samples of this variant:

```
Loader URLs:

hxxps://finderout[.]com:443/components/af.png

hxxps://lionpick[.]com:443/image-directory/profile.jpg

hxxps://hdhuge[.]com:443/files/remove.gif



Beacon URLs:

hxxps://finderout[.]com/mobile-ipad-home.css

hxxps://lionpick[.]com:443/media.css

hxxps://hdhuge[.]com:443/skin
```

Conclusion

Cobalt Strike is a powerful tool that's being leveraged by people that shouldn't be leveraging it at all: a growing number of cybercriminals. That said, not all deployments of Cobalt Strike are the same. As this blog has shown, some deployments demonstrate bad operational security by re-using infrastructure and not changing their malleable-C2 profiles. Additionally, some operators drop Cobalt

Cobalt Strike, while used by security practitioners to ultimately thwart cybercrime, is now a common tool in the arsenal of cybercriminals. For now, most threat actors are relying on open source methods for deployment and configuration, but we expect cybercriminals to begin to innovate and develop new tactics that defenders will have to adapt to. We expect these innovations particularly from those cybercriminal groups that are using the tool in targeted ransomware attacks.

For more on what Intel 471 has observed, download our white paper.

1. Dropping Anchor: From a TrickBot Infection to the Discovery of the Anchor Malware
https://www.cybereason.com/blog/dropping-anchor-from-a-trickbot-infection-to-the-discovery-of-the-anchor-malware
2. TrickBot Crews New CobaltStrike Loader
https://medium.com/walmartglobaltech/trickbot-crews-new-cobaltstrike-loader-32c72b78e81c
3. TRICKBOT - Analysis Part II
https://www.sneakymonkey.net/2019/10/29/trickbot-analysis-part-ii/
4. Trickbot Brief: Creds and Beacons
https://thedfirreport.com/2021/05/02/trickbot-brief-creds-and-beacons