Stats from Hunting Cobalt Strike Beacons

By svch0st

Published: 2021-05-06 · Archived: 2026-04-05 13:18:03 UTC

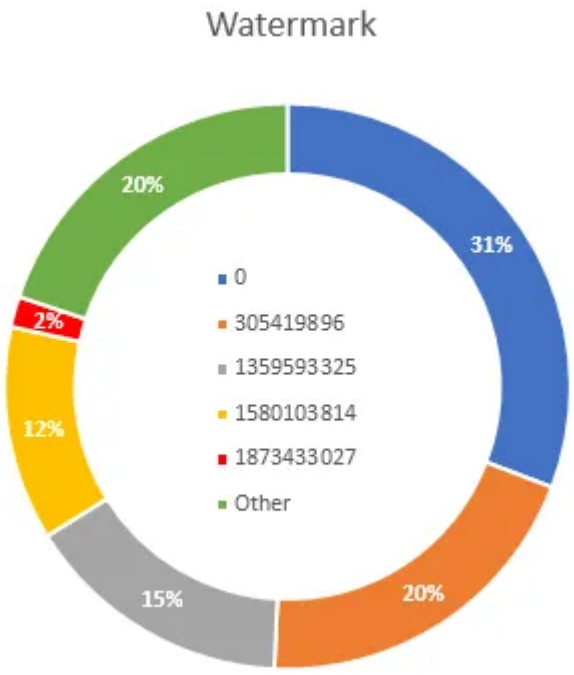
Some Statistics on Cobalt Strike Configs in April and May 2021

Collected from over 1000 configurations, here are some high-level statistics that demonstrate some of the common trends among one of the most popular tools in an adversary's arsenal. These configs were collected from live servers around early May 2021.

If you are interested in how the data was collected, scroll to the bottom of the article. ***Also if you just want the raw data here is a link.***

If you want to read more about how the configurations are structured in Cobalt Strike payloads his article is a good start:

Most common watermark



Unsurprisingly most common watermark was 0. The watermark of 0 is indicative of cracked versions for Cobalt Strike which are commonly used by threat actors in their campaigns. More interestingly is 305419896, 1359593325, and 1580103814, all had configuration counts above 100.

The watermark 305419896 has been associated with the Maze ransomware:

User Agents

Besides the standard user agents imitating web browsers, several configurations had the user agent of “Shockwave Flash”

Interesting URI

The more standard URIs of */submit.php* and */jquery-3.3.2.min.js* were the most common but this one stood out to me:

- /r/webdev/comments/95lyr/slow_loading_of_google

Most common process spawn targets

Get svch0st’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

The default values of rundll32.exe were the most common.

Row Labels	Count of ip
%windir%\sysnative\rundll32.exe	395
%windir%\syswow64\rundll32.exe	394
%windir%\syswow64\dllhost.exe	47
%windir%\sysnative\dllhost.exe	46
%windir%\sysnative\mstsc.exe	23
%windir%\syswow64\mstsc.exe	23
%windir%\syswow64\WUAUCLT.exe	23
%windir%\sysnative\WUAUCLT.exe	23
%windir%\sysnative\gpupdate.exe	19
%windir%\syswow64\wusa.exe	16
%windir%\sysnative\wusa.exe	16
%windir%\syswow64\gpupdate.exe	15
%windir%\syswow64\svchost.exe	13
%windir%\sysnative\svchost.exe	11
%windir%\syswow64\regsvr32.exe	8

Looking at the information, I was most interested in some of the more custom values such as:

- %windir%\syswow64\eventvwr.exe
- %windir%\syswow64\backgroundtaskhost.exe
- %windir%\system32\mobsync.exe
- %windir%\sysnative\adobe64.exe

How I collected the Data

I used 2 main queries to get as many C2 IPs as quickly as possible.

- RiskIQ prebuild component to search for Cobalt Strike (requires a free account) (~8k IPs)
- A search on JARM hashes that I had found in a recent case (~10k IPs):

```
JARMFuzzy: 07d14d16d21d21d07c42d41d00041d
```

If you want to learn more about JARM, which is developed by the Salesforce team, this is a great article:

This data contained many IPs that were burnt by the time of analysis; however, it still provided a decent enough dataset to get some results.

Retreiving the Configs

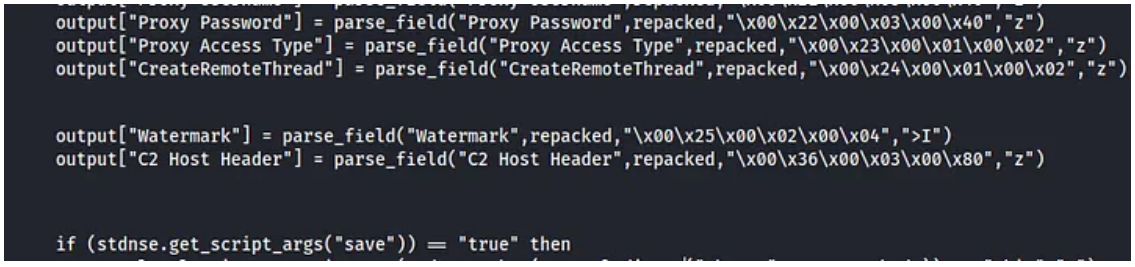
I had two ideas for harvesting configs; one would be downloading the binary payload from sources like Virustotal and MalwareBazaar and parsing them.

But if we know the IPs already, let's just ask the servers for the config?

There are a bunch of awesome tools that exist for extracting and parsing Cobalt beacon configs, but the one I used for this was a Nmap NSE script by Wade Hickey.

I had added some error exception handling and most importantly an extra line to pull out the beacon Watermark (or license number) which is very helpful for threat intelligence.

Press enter or click to view image in full size



See my fork here:

I then used the IP lists I had as input and ran the Nmap script.

```
nmap --script=grab_beacon_config.nse -p 80,443,8080 -iL jarmfuzzy.txt -oA jarmfuzzy -T4
```

The output of the script will look something like this:

```
|_grab_beacon_config: {"x86": {"uri_queried": "\/DxRN", "md5": "7118007ad133a9dcd59419beef0896a5", "
```

From there, it was an exercise of cleaning up the data into something useable and using Excel-fu to get some ugly pie graphs :)
