Stats from Hunting Cobalt Strike Beacons

Some Statistics on Cobalt Strike Configs in April and May 2021

svch0st · Follow
4 min read · May 6, 2021

39

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:

Cobalt Strike Staging and Extracting Configuration Information

By default Cobalt Strike exposes its stager shellcode via a valid checksum8 request (the same request format used in...

Unsurprisingly most common watermark was 0. The watermark of 0 is in… by th…

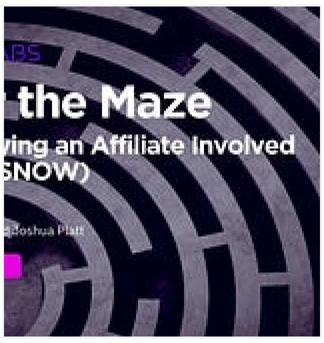
1359593325, and 1580103814, all had configuration counts above 100.

The watermark 305419896 has been associated with the Maze ransomware:

Enter the Maze: Demystifying an Affiliate Involved in Maze (SNOW) - SentinelLabs

By Jason Reaves and Joshua Platt Maze continues to be one of the most dangerous and actively developed ransomware…

labs.sentinelone.com



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

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

- %windir%\syswow64\backgroundtaskhost.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):

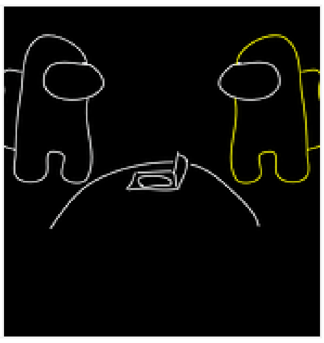
```
JARMFuzzy: 07d14d16d21d21d07c42d41d00041d
```

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

Easily Identify Malicious Servers on the Internet with JARM

JARM is an active Transport Layer Security server fingerprinting tool that provides the ability to identify and group...

engineering.salesforce.com



This data contained many IPs that were burnt by the time of analysis:

I had added some error exception handling and most importantly an extra lin

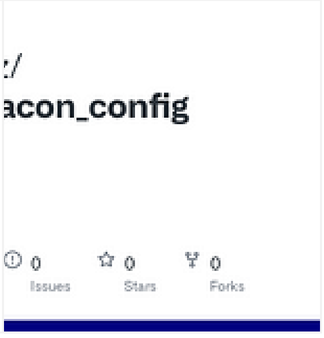
he

See my fork here:

svch0stz/grab_beacon_config

Contribute to svch0stz/grab_beacon_config development by creating an account on GitHub.

github.com



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": "\/DxPN", "md5":
```

```
"bf4ee9664fba51a1bbbdad13a598688914a48465fac3993c096c6d2cc0c2c021"
```

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

39

Written by svch0st

318 Followers

Follow

More from svch0st

Feb

See all from svch0st

Recommended from Medium

Alexander Nguyen in Level Up Coding

The resume that got a software engineer a $300,000 job at Google.

1-page. Well-formatted.

✦ Jun 1 25K 484

Mohammed Dief

How I managed to bypass Process Monitor detection for anti-...

Hey there, I hope this article finds you well and you're safe somewhere in the world,...

May 5 84 2

Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

Jun 18 1.6K 54

F. Perry Wilson, MD MSCE

How Old Is Your Body? Stand On One Leg and Find Out

According to new research, the time you can stand on one leg is the best marker of...

Oct 23 6.5K 152

See more recommendations