

Medium Q Search







Stats from Hunting Cobalt Strike Beacons

Some Statistics on Cobalt Strike Configs in April and May 2021

Medium





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

blog.securehat.co.uk



Most common watermark



Medium

Sign up to discover human stories that deepen your understanding of the world.

Free ✓ Distraction-free reading. No ads. ✓ Organize your knowledge with lists and highlights. ✓ Tell your story. Find your audience.

Membership
 ✓ Read member-only stories
 ✓ Support writers you read most
 ✓ Earn money for your writing
 ✓ Listen to audio narrations
 ✓ Read offline with the Medium app

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"

Medium

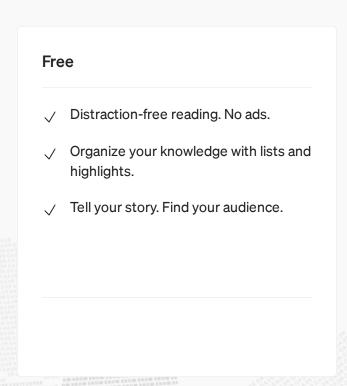
Sign up to discover human stories that deepen your understanding of the world.

Free ✓ Distraction-free reading. No ads. ✓ Organize your knowledge with lists and highlights. ✓ Tell your story. Find your audience.

/	Read member-only stories
/	Support writers you read most
/	Earn money for your writing
/	Listen to audio narrations
/	Read offline with the Medium app

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

Medium





• A search on JARM hashes that I had found in a recent case (~10k IPs):

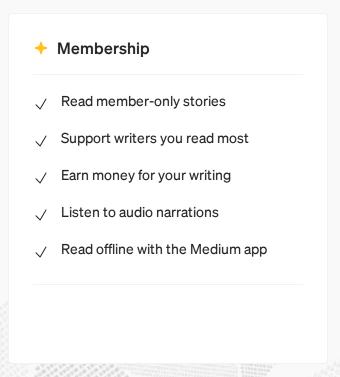
JARMFuzzy: 07d14d16d21d21d07c42d41d00041d

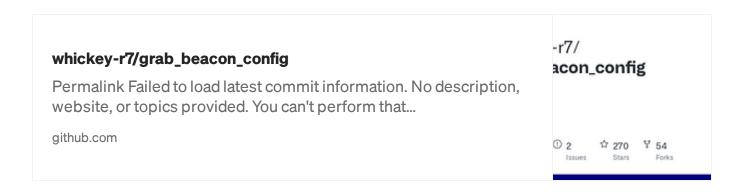
If you want to learn more about JARM, which is developed by the Salesforce team, this is a great article:

Medium

Sign up to discover human stories that deepen your understanding of the world.

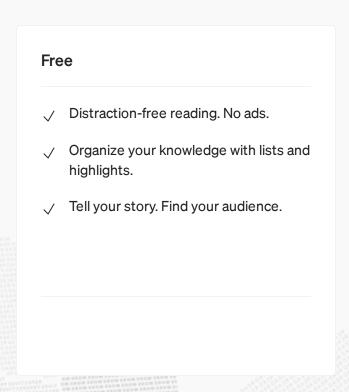
Free
 ✓ Distraction-free reading. No ads.
 ✓ Organize your knowledge with lists and highlights.
 ✓ Tell your story. Find your audience.

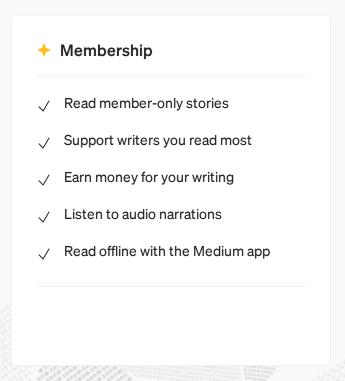




I had added some error exception handling and most importantly an extra line to pull out the beacon Watermark (or license number) which is very helpful for threat intelligence.

Medium





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

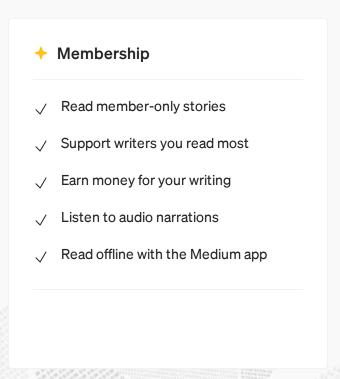
The output of the script will look something like this:

```
|_grab_beacon_config: {"x86": {"uri_queried": "\/DxRN", "md5":
"7118007ad133a9dcd59419beef0896a5", "config": {"Jitter": 0, "Spawn
To x64": "%windir%\\system32\\mobsync.exe", "Max DNS": 255, "C2
Server": "thefaithfulamerican.com,\/s\/ref=nb_sb_noss", "DNS
Sleep": 0. "HTTP Method Path 2":
```

Medium

Sign up to discover human stories that deepen your understanding of the world.

Free Distraction-free reading. No ads. Organize your knowledge with lists and highlights. Tell your story. Find your audience.



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



Medium

