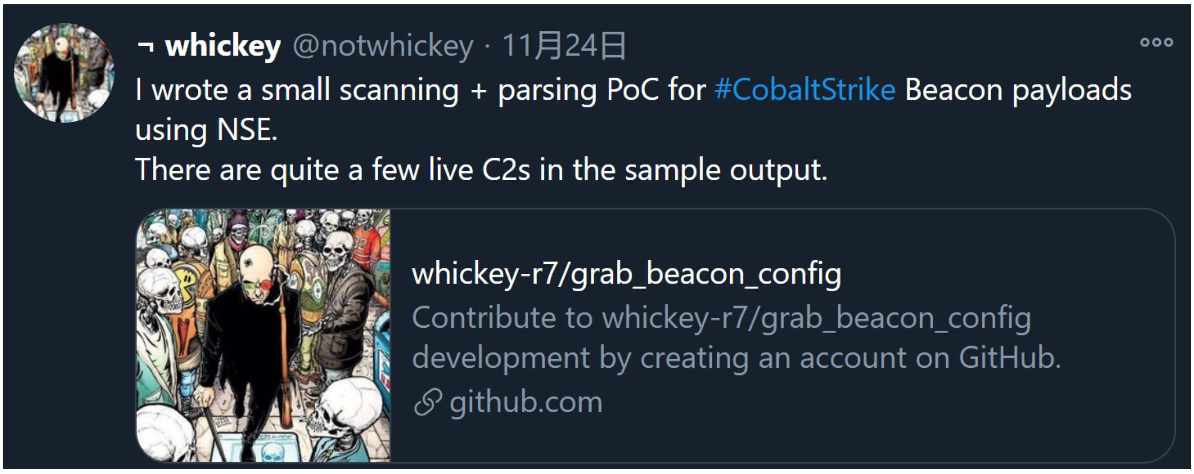
Hunting Beacons

0x01 Preface

Analysis and discovery of cyberspace mapping data has always been a core objective of the Quake team.

Recently, we noticed that some foreign security researchers have published a Cobalt Strike Beacon scanning tool on github, which can extract the configuration information of the Beacon. With the concerted efforts of our Quake teammates, this feature was integrated into the Quake system, and after a short period of time the scanning was quite effective.



¬ whickey @notwhickey · 11月24日

I wrote a small scanning + parsing PoC for #CobaltStrike Beacon payloads using NSE.
There are quite a few live C2s in the sample output.

whickey-r7/grab_beacon_config
Contribute to whickey-r7/grab_beacon_config development by creating an account on GitHub.
github.com

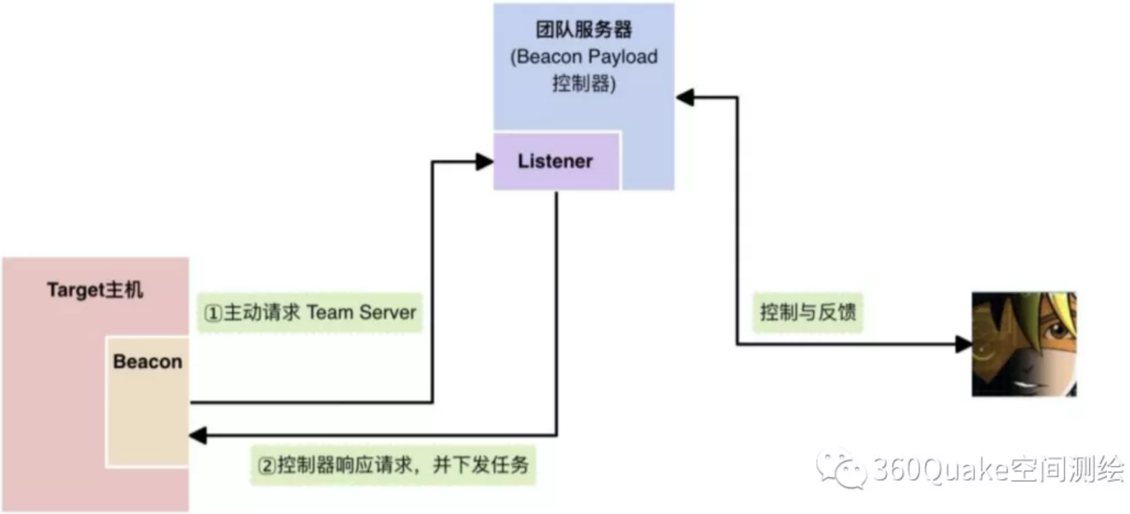
In the following we will explain in detail how Beacon Staging Server scanning works.

0x02 What is a Beacon?

Those of you who work in penetration testing, red team attack and defence will be familiar with this concept, but we'll just use here an introduction from an article by the Gcow security team.

Beacon is Cobalt Strike's payload running on the target host, Beacon is a service we provide on a covert channel for long-term control of infected hosts.

It works in a similar way to the Metasploit Framework Payload. During the actual infiltration process we can **embed it into an executable file**, **add it to a Word document** or deliver Beacon by **exploiting a host vulnerability**.



A picture is worth a thousand words, and in this case it was the Beacon Listener in the team server that we discovered through active mapping.

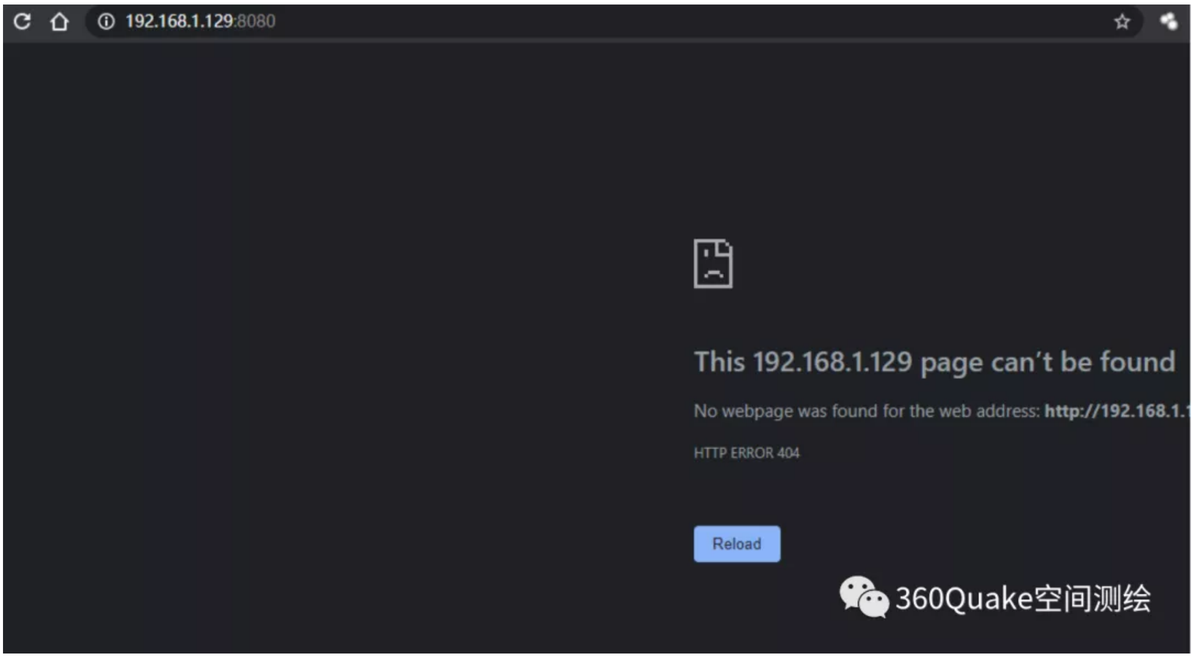
0x03 Beacon Staging Server

The purpose of the Beacon Staging Server is to prevent the payload from becoming too large or to adapt to different attack scenarios by delivering the payload in stages.

First by delivering a small payload called a stager, then by going to the Beacon staging server to download the larger and more complex stage, and the URL to access the stage is verified by checksum8.

When the staging server, which stores the Beacon configuration and payload, is exposed to the public web, it can be discovered by means of active mapping.

Unfortunately, access to the service is by default a disguised 404 page. This also results in various scanners, spatial mapping systems, threat intelligence platforms etc. not being able to make effective judgements based on page response information.

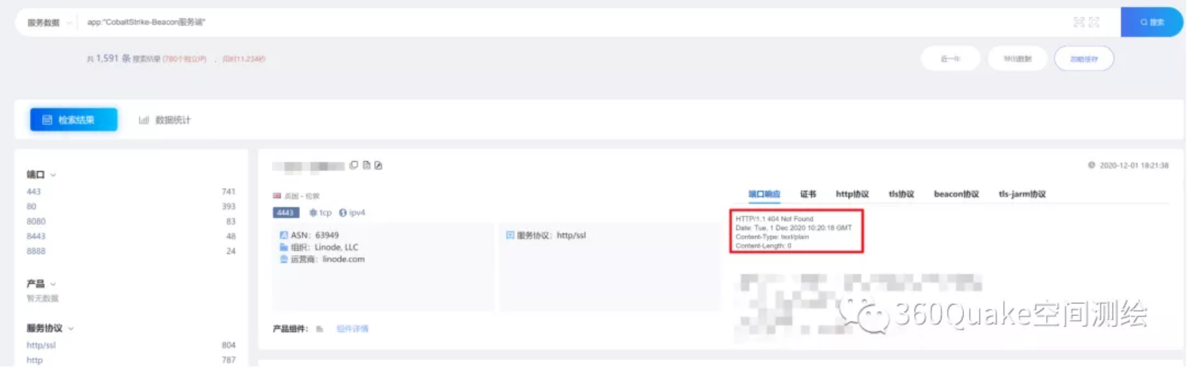


This 192.168.1.129 page can’t be found

No webpage was found for the web address: **http://192.168.1.1**

HTTP ERROR 404

If not specifically identified by a scan, a Beacon Staging Server should only return the information in the red box in the diagram below.



app:"CobaltStrike-Beacon服务端"

共 1,591 条

443 741
80 393
8080 83
8443 48
8888 24

暂无数据

http/ssl 804
http 787

2020-12-01 18:21:38

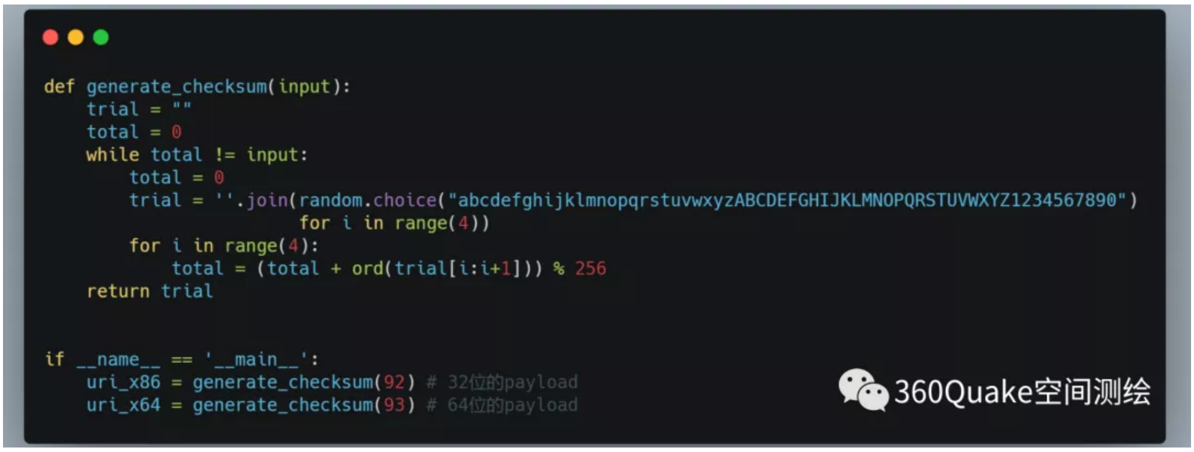
4443 tcp ipv4

ASN：63949
组织：Linode, LLC
运营商：linode.com

服务协议：http/ssl

```
HTTP/1.1 404 Not Found
Date: Tue, 1 Dec 2020 10:20:18 GMT
Content-Type: text/plain
Content-Length: 0
```

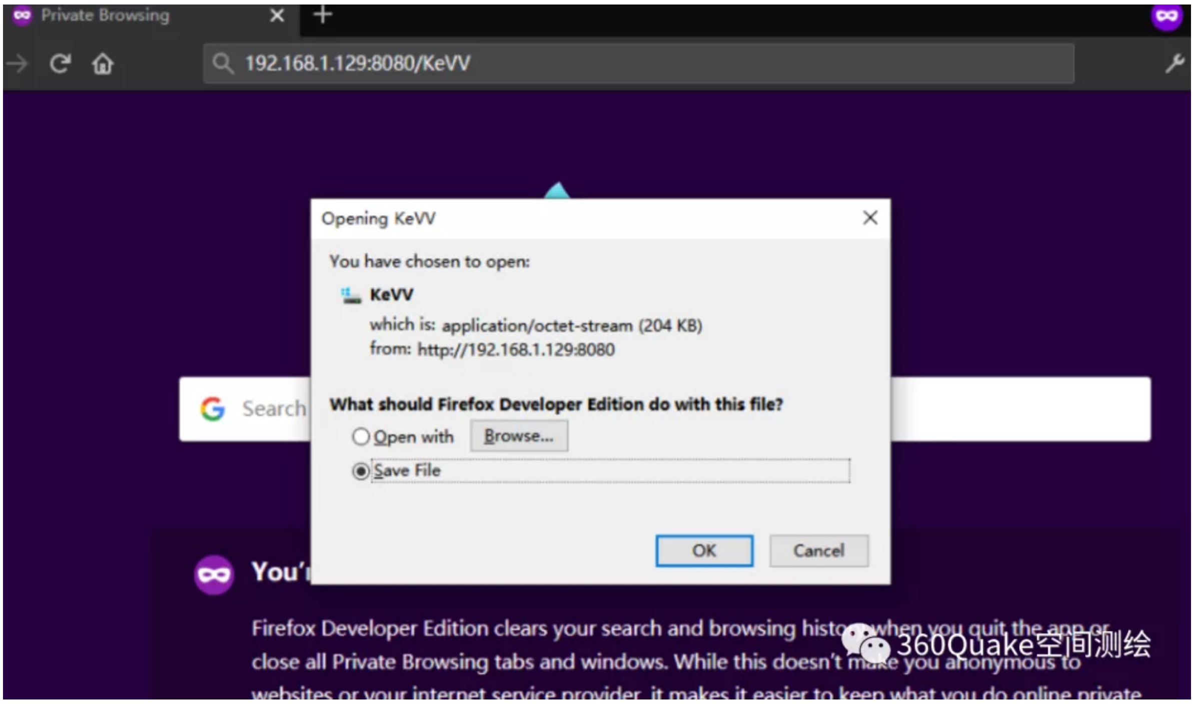
In order to get a specific Stage, it is necessary to know the URL generation algorithm. The algorithm is derived from publicly available NSE scripts, we use the following script for the generation of the check digits and can generate the check digits for a 32-bit or 64-bit payload depending on the input.



```python
def generate_checksum(input):
    trial = ""
    total = 0
    while total != input:
        total = 0
        trial = ''.join(random.choice("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890")
                        for i in range(4))
        for i in range(4):
            total = (total + ord(trial[i:i+1])) % 256
    return trial


if __name__ == '__main__':
    uri_x86 = generate_checksum(92) # 32位的payload
    uri_x64 = generate_checksum(93) # 64位的payload
```

By splicing the check digits to the URL, we can download directly to the Beacon's stage file, instead of a 404 page.



Opening KeVV

You have chosen to open:

KeVV

which is: application/octet-stream (204 KB)
from: http://192.168.1.129:8080

What should Firefox Developer Edition do with this file?

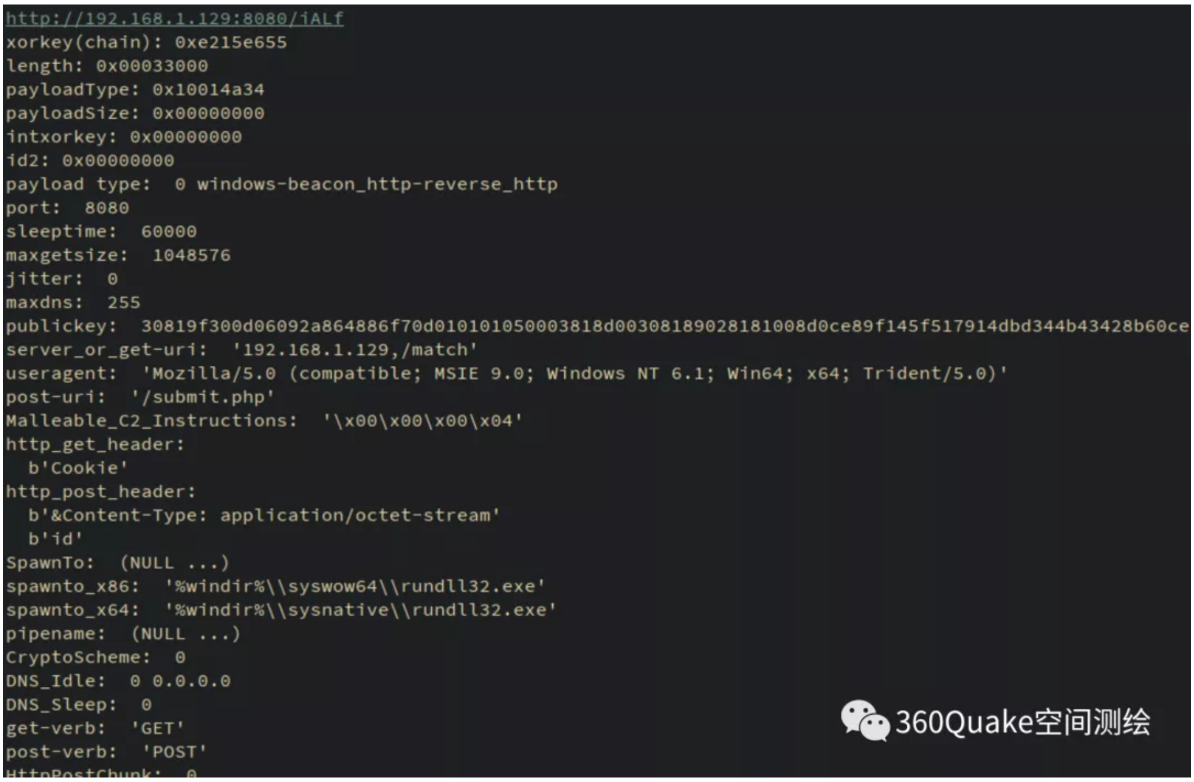
○ Open with Browse...
● Save File

OK Cancel

Firefox Developer Edition clears your search and browsing histo when you quit the app or close all Private Browsing tabs and windows. While this doesn't make you anonymous to websites or your internet service provider, it makes it easier to keep what you do online private

0x04 Resolving Beacon configurations

After a successful download from the Beacon staging server to the stage, we need to parse it, and JPCERT released a Volatility plugin cobaltstrikescan in 2018 to parse the Beacon configuration and payload.

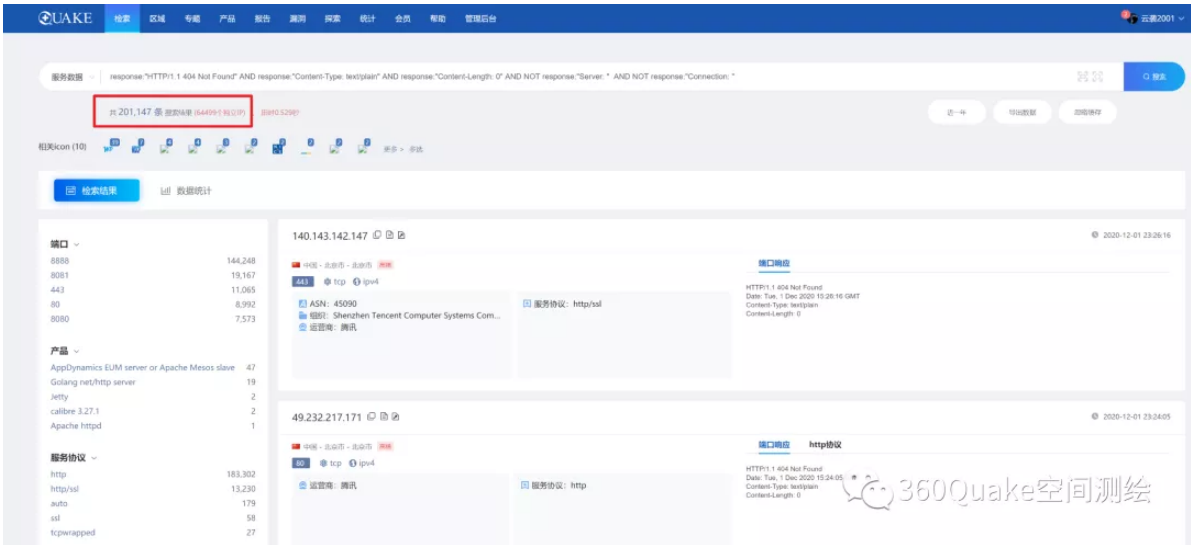


```
http://192.168.1.129:8080/iALf
xorkey(chain): 0xe215e655
length: 0x00033000
payloadType: 0x10014a34
payloadSize: 0x00000000
intxorkey: 0x00000000
id2: 0x00000000
payload type:  0 windows-beacon_http-reverse_http
port:  8080
sleeptime:  60000
maxgetsize:  1048576
jitter:  0
maxdns:  255
publickey:  30819f300d06092a864886f70d010101050003818d0030818902818100 8d0ce89f145f517914dbd344b43428b60ce
server_or_get-uri:  '192.168.1.129,/match'
useragent:  'Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)'
post-uri:  '/submit.php'
Malleable_C2_Instructions:  '\x00\x00\x00\x04'
http_get_header:
  b'Cookie'
http_post_header:
  b'&Content-Type: application/octet-stream'
  b'id'
SpawnTo:  (NULL ...)
spawnto_x86:  '%windir%\\syswow64\\rundll32.exe'
spawnto_x64:  '%windir%\\sysnative\\rundll32.exe'
pipename:  (NULL ...)
CryptoScheme:  0
DNS_Idle:  0 0.0.0.0
DNS_Sleep:  0
get-verb:  'GET'
post-verb:  'POST'
HttpPostChunk:  0
```

0x05 Quake Active Mapping

Having clarified how the Beacon Staging Server works, we first identified a group of original targets using the following Quake search syntax.

response:"HTTP/1.1 404 Not Found" AND response:"Content-Type: text/plain" AND response:"Content-Length: 0" AND NOT response:"Server: " AND NOT response:"Connection: "



response:"HTTP/1.1 404 Not Found" AND response:"Content-Type: text/plain" AND response:"Content-Length: 0" AND NOT response:"Server: " AND NOT response:"Connection: "

共 201,147 条 搜索结果 (64499个独立IP) 用时0.529秒

相关icon (10)

端口	
8888	144,248
8081	19,167
443	11,065
80	8,992
8080	7,573
产品	
AppDynamics EUM server or Apache Mesos slave	47
Golang net/http server	19
Jetty	2
calibre 3.27.1	2
Apache httpd	1
服务协议	
http	183,302
http/ssl	13,230
auto	179
ssl	58
tcpwrapped	27

140.143.142.147 — 2020-12-01 23:26:16
中国 - 北京市 - 北京市
443 tcp ipv4
ASN: 45090
组织: Shenzhen Tencent Computer Systems Com...
运营商: 腾讯
服务协议: http/ssl
端口响应

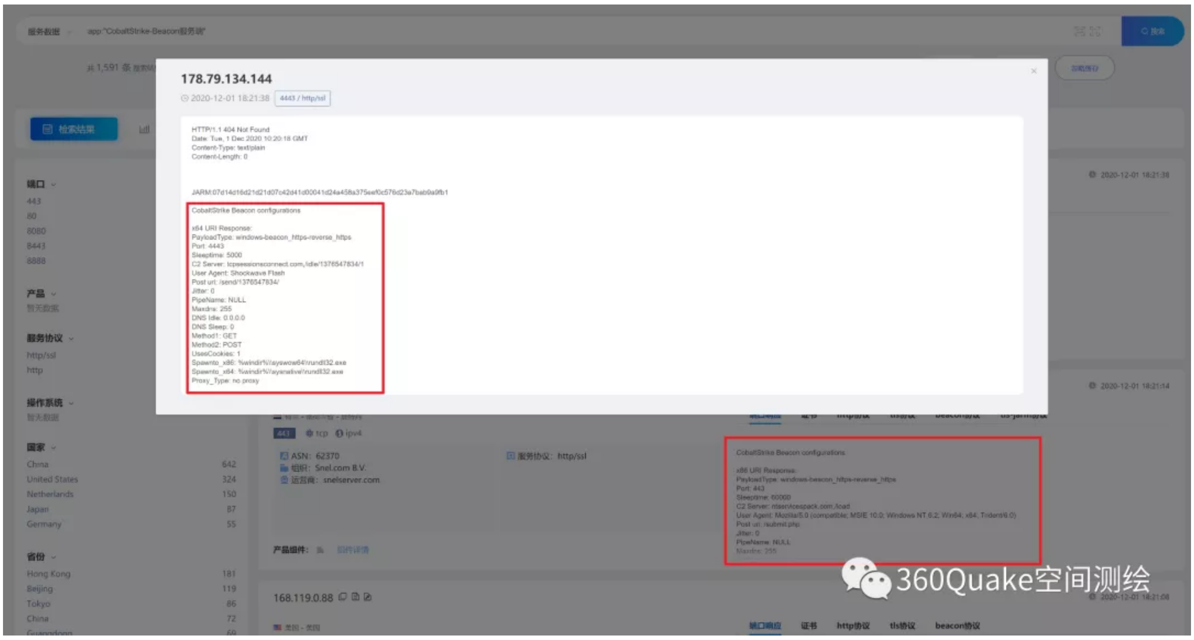
```
HTTP/1.1 404 Not Found
Date: Tue, 1 Dec 2020 15:26:16 GMT
Content-Type: text/plain
Content-Length: 0
```

49.232.217.171 — 2020-12-01 23:24:05
中国 - 北京市 - 北京市
80 tcp ipv4
运营商: 腾讯
服务协议: http
端口响应 http协议

```
HTTP/1.1 404 Not Found
Date: Tue, 1 Dec 2020 15:24:05
Content-Type: text/plain
Content-Length: 0
```

The IPs from the above results are then targeted and finally we append the extracted Beacon configuration information to the corresponding response port after.

Queries can be made directly using the Quake search syntax： `app:"CobaltStrike-Beacon"`



178.79.134.144

2020-12-01 18:21:38 4443 / http/ssl

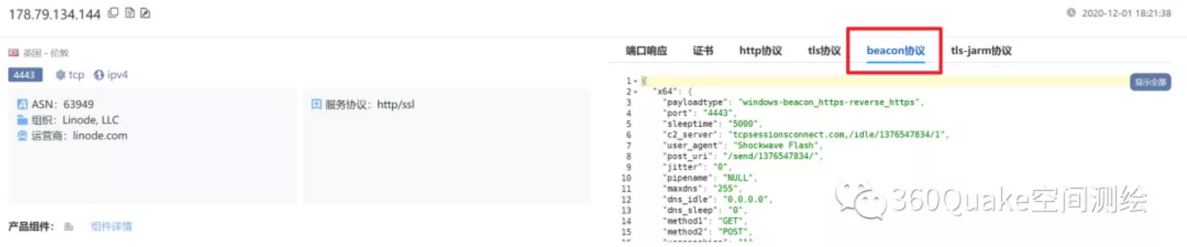
```
HTTP/1.1 404 Not Found
Date: Tue, 1 Dec 2020 10:20:18 GMT
Content-Type: text/plain
Content-Length: 0


JARM:07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1

CobaltStrike Beacon configurations

x64 URI Response:
PayloadType: windows-beacon_https-reverse_https
Port: 4443
Sleeptime: 5000
C2 Server: tcpsessionconnect.com,/idle/1376547834/1
User Agent: Shockwave Flash
Post uri: /send/1376547834/
Jitter: 0
PipeName: NULL
Maxdns: 255
DNS Idle: 0.0.0.0
DNS Sleep: 0
Method1: GET
Method2: POST
UsesCookies: 1
Spawnto_x86: %windir%\\syswow64\\rundll32.exe
Spawnto_x64: %windir%\\sysnative\\rundll32.exe
Proxy_Type: no proxy
```

Quake has also carried out an in-depth analysis of the Beacon configuration, which can be viewed by clicking on `beacon protocols'.



178.79.134.144

2020-12-01 18:21:38

英国 - 伦敦

4443 tcp ipv4

ASN: 63949
组织: Linode, LLC
运营商: linode.com

服务协议: http/ssl

产品组件: 组件详情

```
{
  "x64": {
    "payloadtype": "windows-beacon_https-reverse_https",
    "port": "4443",
    "sleeptime": "5000",
    "c2_server": "tcpsessionconnect.com,/idle/1376547834/1",
    "user_agent": "Shockwave Flash",
    "post_uri": "/send/1376547834/",
    "jitter": "0",
    "pipename": "NULL",
    "maxdns": "255",
    "dns_idle": "0.0.0.0",
    "dns_sleep": "0",
    "method1": "GET",
    "method2": "POST",
```

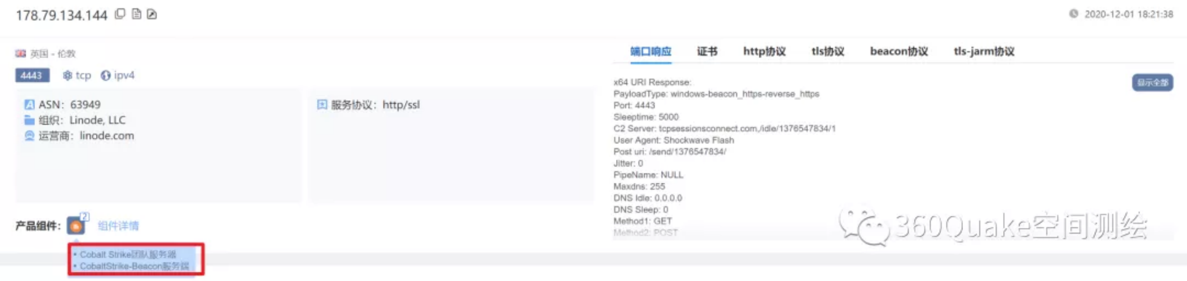
```
{
  "x86": {
    "payloadtype": "Beacon 类型",
    "port": "端口",
    "sleeptime": "60000", Beacon 默认心跳时间，每一分钟目标主机与teamserver通信一次。
    "c2_server": "C2 server",  C2服务器地址，以及URL路径
    "user_agent": "ua",
    "post_uri": "/submit.php",
    "jitter": "0", 针对睡眠时间的抖动率，随机睡眠。
    "pipename": "smb beacon之间的通信的管道名称" ,
    "maxdns": "255", 通过DNS上传数据时，主机名最大长度
    "dns_idle": "0.0.0.0",  表示改IP没有可用的任务,避免使用Bogon地址
    "dns_sleep": "0",每个单独的DNS请求前强制睡眠时间毫秒
    "method1": "GET",
    "method2": "POST",
    "usescookies": "1",
    "spawnto_x86": "x86默认打开并注入shellcode的进程",
    "spawnto_x64": "x64默认打开并注入shellcode的进程",
    "proxy_type": "IE settings", 代理类型
    // 进程注入选项
    "process_inject_start_rwx": "PAGE_EXECUTE_READWRITE",   使用RWX作为注入内容的初始权限。另一种是RW。
    "process_inject_use_rwx": "PAGE_EXECUTE_READWRITE",  使用RWX作为注入内容的最终权限。替代是RX。
    "process_inject_min_alloc": "0",    进程注入请求的最小内存
    "process_inject_transform_x86": "NULL", 转换成x86
    "process_inject_transform_x64": "NULL",转换成x64
    "process_inject_execute": "\\x01\\x02\\x03\\x04",
    "process_inject_allocation_method": "0",
    "process_inject_stub": "F\\xa0úã\\x03äÒmaÿÆ£G\\xadïV",
    "publickey": "" 公钥
  },
  "x64": {
    "payloadtype": "",
    "port": "8080",
    "sleeptime": "60000",
    "c2_server": "1",
    "user_agent": "",
    "post_uri": "/submit.php",
    "jitter": "0",
    "pipename": "NULL",
    "maxdns": "255",
    "dns_idle": "0.0.0.0",
    "dns_sleep": "0",
    "method1": "GET",
    "method2": "POST",
    "usescookies": "1",
    "spawnto_x86": "%windir%\\\\syswow64\\\\rundll32.exe",
    "spawnto_x64": "%windir%\\\\sysnative\\\\rundll32.exe",
    "proxy_type": "IE settings",
    "process_inject_start_rwx": "PAGE_EXECUTE_READWRITE",
    "process_inject_use_rwx": "PAGE_EXECUTE_READWRITE",
    "process_inject_min_alloc": "0",
    "process_inject_transform_x86": "NULL",
    "process_inject_transform_x64": "NULL",
    "process_inject_execute": "\\x01\\x02\\x03\\x04",
    "process_inject_allocation_method": "0",
    "process_inject_stub": "F\\xa0úã\\x03äÒmaÿÆ£G\\xadïV",
    "publickey": ""
  }
}
```

** Up to this point, the Quake system has supported 2 product fingerprints in relation to Cobalt Strike.

`app:"Cobalt Strik"`

`app:"CobaltStrike-Beacon"`

Quake's search results page will also be marked.



178.79.134.144

2020-12-01 18:21:38

英国 - 伦敦

4443 tcp ipv4

ASN：63949
组织：Linode, LLC
运营商：linode.com

服务协议：http/ssl

产品组件： 组件详情

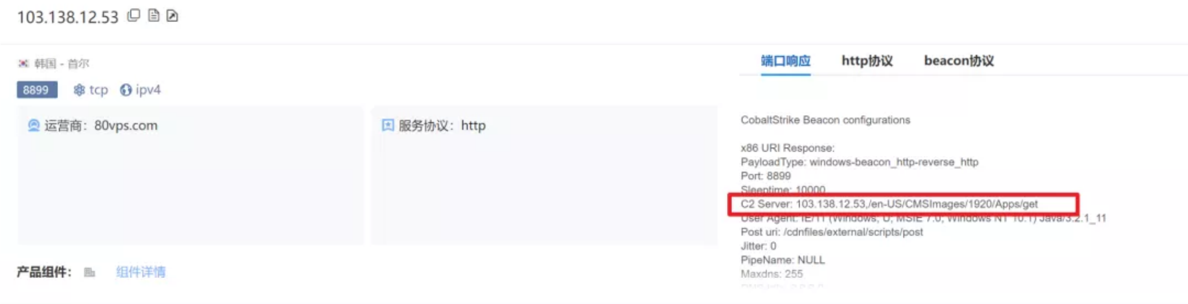
- Cobalt Strike团队服务器
- CobaltStrike-Beacon服务器

```
x64 URI Response:
PayloadType: windows-beacon_https-reverse_https
Port: 4443
Sleeptime: 5000
C2 Server: tcpsessionsconnect.com,/idle/1376547834/1
User Agent: Shockwave Flash
Post uri: /send/1376547834/
Jitter: 0
PipeName: NULL
Maxdns: 255
DNS Idle: 0.0.0.0
DNS Sleep: 0
Method1: GET
Method2: POST
```

0x06 C2 node extraction and analysis

After being able to parse Beacon's configuration file properly, we could see that the `c2_server` field is the address of the C2 server and its URL, so we extracted and analysed it and found the following.

1. the vast majority of C2 addresses are Cobalt Strike's own IP, but some C2 nodes are connected using domain names.
2. different ports with the same IP and different C2 node configurations, e.g. `103.138.12[...]53`. This image can be used to find the real C2 IP. it may also indicate that the Cobalt Strike has multiple C2 nodes configured.



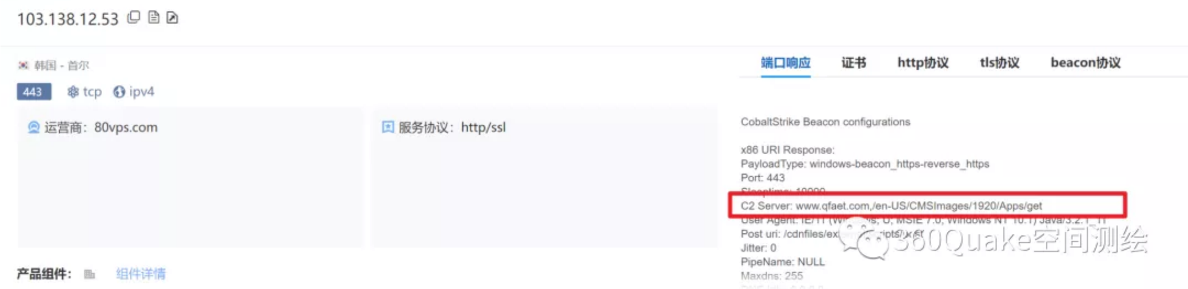
103.138.12.53

运营商：80vps.com

服务协议：http

```
CobaltStrike Beacon configurations

x86 URI Response:
PayloadType: windows-beacon_http-reverse_http
Port: 8899
Sleeptime: 10000
C2 Server: 103.138.12.53,/en-US/CMSImages/1920/Apps/get
User Agent: IE/11 (Windows; U; MSIE 7.0; Windows NT 10.1) Java/3.2.1_11
Post uri: /cdnfiles/external/scripts/post
Jitter: 0
PipeName: NULL
Maxdns: 255
```



103.138.12.53

运营商：80vps.com

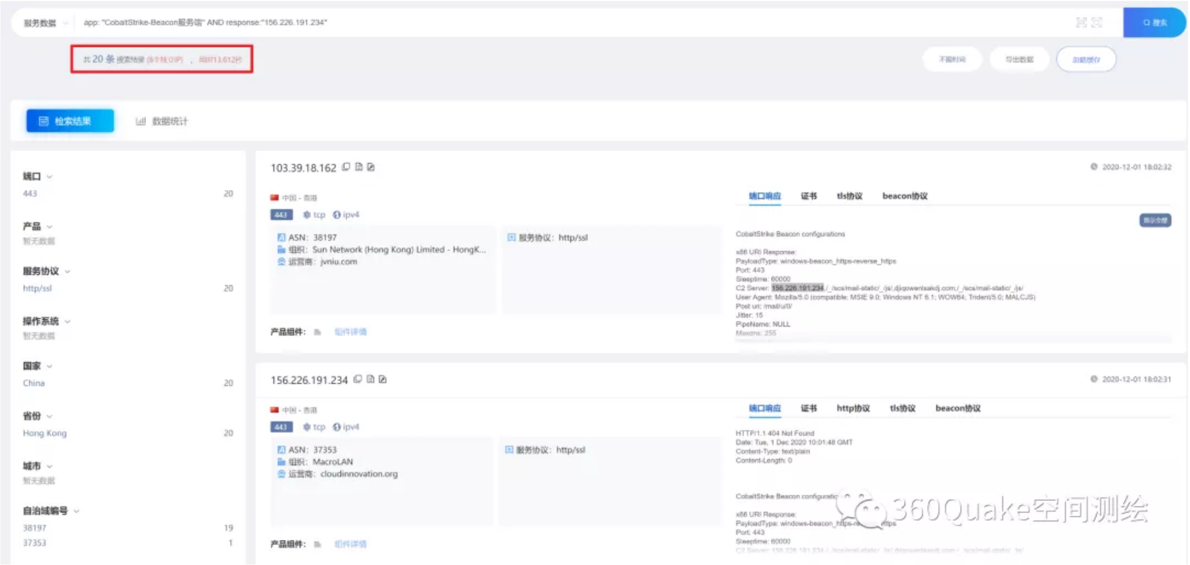
服务协议：http/ssl

```
CobaltStrike Beacon configurations

x86 URI Response:
PayloadType: windows-beacon_https-reverse_https
Port: 443
Sleeptime: 10000
C2 Server: www.qfaet.com,/en-US/CMSImages/1920/Apps/get
User Agent: IE/11 (Windows; U; MSIE 7.0; Windows NT 10.1) Java/3.2.1_11
Post uri: /cdnfiles/ex
Jitter: 0
PipeName: NULL
Maxdns: 255
```

360Quake空间测绘

3. the presence of several different Cobalt Strike IPs using the same C2 address. After analysis, it can be determined that the Cobalt Strike team server has multiple IP addresses or that there are multiple team servers.



app: "CobaltStrike-Beacon服务端" AND response:"156.226.191.234"

共 20 条

端口	
443	20
产品	
暂无数据	
服务协议	
http/ssl	20
操作系统	
暂无数据	
国家	
China	20
省份	
Hong Kong	20
城市	
暂无数据	
自治域编号	
38197	19
37353	1

103.39.18.162 2020-12-01 18:02:32

中国 - 香港 443 tcp ipv4

ASN：38197
组织：Sun Network (Hong Kong) Limited - HongK...
运营商：jvniu.com

服务协议：http/ssl

```
CobaltStrike Beacon configurations

x86 URI Response:
PayloadType: windows-beacon_https-reverse_https
Port: 443
Sleeptime: 60000
C2 Server: 156.226.191.234,/_/scs/mail-static/_/js/,djqowenlsakdj.com,/_/scs/mail-static/_/js/
User Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; MALCJS)
Post uri: /mail/u/0/
Jitter: 15
PipeName: NULL
Maxdns: 255
```

156.226.191.234 2020-12-01 18:02:31

中国 - 香港 443 tcp ipv4

ASN：37353
组织：MacroLAN
运营商：cloudinnovation.org

服务协议：http/ssl

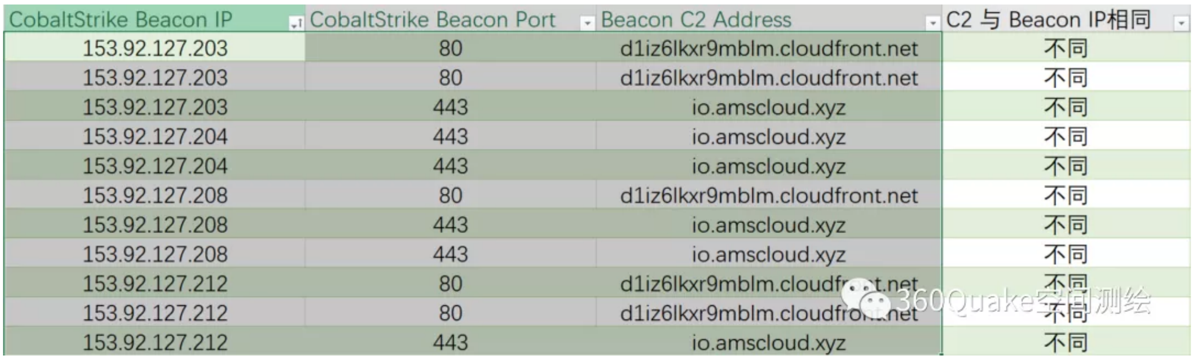
```
HTTP/1.1 404 Not Found
Date: Tue, 1 Dec 2020 10:01:48 GMT
Content-Type: text/plain
Content-Length: 0

CobaltStrike Beacon configuratio

x86 URI Response:
PayloadType: windows-beacon_https-re    ttps
Port: 443
Sleeptime: 60000
```

360Quake空间测绘

4. the existence of a Cobalt Strike IP using a different C2 image, e.g. search for `app: "CobaltStrike-Beacon" AND response: "153.92.127.212"`



CobaltStrike Beacon IP	CobaltStrike Beacon Port	Beacon C2 Address	C2 与 Beacon IP相同
153.92.127.203	80	d1iz6lkxr9mblm.cloudfront.net	不同
153.92.127.203	80	d1iz6lkxr9mblm.cloudfront.net	不同
153.92.127.203	443	io.amscloud.xyz	不同
153.92.127.204	443	io.amscloud.xyz	不同
153.92.127.204	443	io.amscloud.xyz	不同
153.92.127.208	80	d1iz6lkxr9mblm.cloudfront.net	不同
153.92.127.208	443	io.amscloud.xyz	不同
153.92.127.208	443	io.amscloud.xyz	不同
153.92.127.212	80	d1iz6lkxr9mblm.cloudfront.net	不同
153.92.127.212	80	d1iz6lkxr9mblm.cloudfront.net	不同
153.92.127.212	443	io.amscloud.xyz	不同

360Quake空间测绘

5. Most C2 nodes use domain names that are new IoC and are hardly ever judged black in platforms such as VirusTotal.

0x07 IoC

By the time this article was edited, we had identified the following C2 addresses in the Beacon configuration for extraction analysis.
Total of 777 CobaltStrike standalone IPs and 781 Beacon** C2 addresses (**580 standalone IPs and** 201 standalone domain names** of its**).
Some of the IoCs are as follows.

CobaltStrikeBeacon IP	CobaltStrikeBeacon Port	Beacon C2 Address
83.242.96.163	80	83.242.96.163
47.242.148.4	80	47.242.148.4
218.253.251.118	8443	218.253.251.118
5.34.181.12	5985	5.34.181.12
47.105.180.183	80	kinging.ysan.ml
185.244.149.152	443	yambanetsdev.net
23.224.41.132	80	23.224.41.132
46.148.26.246	443	199.217.117.184
185.150.117.50	443	185.150.117.50
49.234.94.85	8081	49.234.94.85
47.95.231.140	8080	47.95.231.140
176.121.14.249	80	176.121.14.249
144.217.207.21	443	52.188.209.63
185.212.47.171	443	skyler.shacknet.biz
114.118.5.108	443	114.118.5.108
39.100.224.129	8888	39.100.224.129
49.232.42.92	443	49.232.42.92
103.39.18.167	443	156.226.191.234
39.102.52.75	81	39.102.52.75
89.46.86.160	80	89.46.86.160
118.24.85.85	3306	118.24.85.85
47.95.119.10	8080	47.95.119.10
45.153.243.215	443	amajai-technologies.support
47.98.166.253	80	47.98.166.253
47.244.13.36	80	47.244.13.36
185.225.19.125	443	nguyenlieu.gratekey.com
192.144.234.207	80	192.144.234.207
51.195.35.0	8888	51.195.35.0
119.23.184.235	7777	119.23.184.235
152.32.252.47	8080	152.32.252.47

CobaltStrikeBeacon IP	CobaltStrikeBeacon Port	Beacon C2 Address
142.54.188.26	443	agturnfa.com
45.147.229.199	8080	45.147.229.199
106.55.153.204	443	106.55.153.204
49.233.155.141	7001	49.233.155.141
100.26.209.220	443	cdn.az.gov
103.73.97.119	443	103.73.97.119
114.116.33.191	8888	114.116.33.191
176.123.8.228	8000	176.123.8.228
153.92.127.204	443	io.amscloud.xyz
95.179.228.227	443	95.179.228.227
185.202.0.111	80	185.202.0.111
45.76.247.184	80	45.76.247.184
159.69.156.245	80	159.69.156.245
81.70.9.64	80	81.70.9.64
89.45.4.135	8080	89.45.4.135
185.52.3.205	443	185.52.3.205
49.232.217.171	80	49.232.217.171
78.128.113.14	443	78.128.113.14
88.99.89.152	80	88.99.89.152

Please note that as C2 nodes are manually configured by the attacker, there is no guarantee that all are 100% blacklisted (e.g. if C2 is an intranet IP or a whitelisted domain name).

0x08 Conclusion

As Quake said at the product launch and at this year's ISC Spatial Mapping sub-forum.

Cyberspace mapping starts with assets, but goes beyond them.

We believe that active mapping data will be an important source of future cyber security big data & threat intelligence data, along with sample endpoint behaviour data and network traffic communication data. Active mapping data and the knowledge generated from the analysis of mapping data will greatly complement our vision, opening up even more attack surfaces and areas.
Stay tuned for more research in the field of cyberspace mapping~!

0x09 Reference

- https://blog.cobaltstrike.com/2016/06/22/talk-to-your-children-about-payload-staging/

- https://research.nccgroup.com/2020/06/15/striking-back-at-retired-cobalt-strike-a-look-at-a-legacy-vulnerability
- https://github.com/rapid7/metasploit-framework/blob/7a6a124272b7c52177a540317c710f9a3ac925aa/lib/rex/payloads/meterpreter/uri_checksum.rb
- https://blogs.jpcert.or.jp/en/2018/08/volatility-plugin-for-detecting-cobalt-strike-beacon.html
- https://www.cobaltstrike.com/help-malleable-c2
- https://blog.cobaltstrike.com/2019/02/19/cobalt-strike-team-server-population-study/
- https://github.com/Sentinel-One/CobaltStrikeParser/blob/master/parse_beacon_config.py
- https://github.com/whickey-r7/grab_beacon_config/blob/main/grab_beacon_config.nse
- https://blog.cobaltstrike.com/2016/06/15/what-is-a-stageless-payload-artifact/
- http://blog.leanote.com/post/snowming/62ec1132a2c9