浅析 CobaltStrike Beacon Staging Server 扫描

0x01 前言

对网络空间测绘数据的分析和发掘，是Quake团队一直以来的核心目标。

近期，我们留意到有国外安全研究人员在github上发布了一个Cobalt Strike Beacon的扫描工具，可以提取Beacon的配置信息。于是经过Quake团队小伙伴一致努力下，将此功能集成入Quake系统，经过一小段时间的扫描颇见成效。

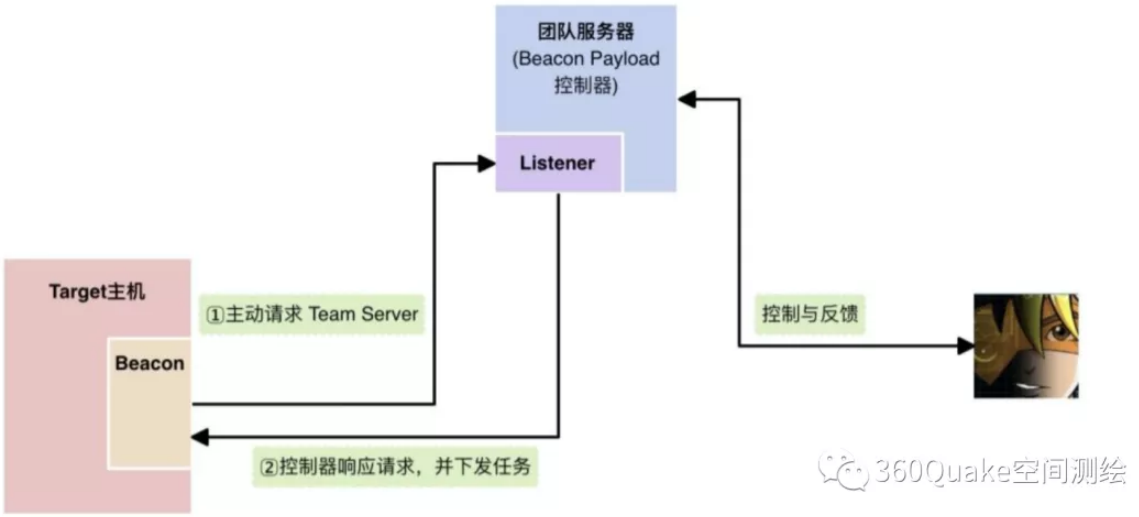
下面我们将详细介绍Beacon Staging Server扫描的原理。

0x02 Beacon是什么

从事渗透测试、红队攻防的小伙伴一定对这个概念并不陌生，我们这里直接使用Gcow安全团队文章里的一段介绍：

Beacon是Cobalt Strike运行在目标主机上的payload，Beacon在隐蔽信道上我们提供服务，用于长期控制受感染主机。

它的工作方式与Metasploit Framework Payload类似。在实际渗透过程中，我们可以将其**嵌入到可执行文件**、**添加到Word文档**或者通过**利用主机漏洞**来传递Beacon。



一图胜千言，本次我们通过主动测绘发现的就是团队服务器中的Beacon Listener。

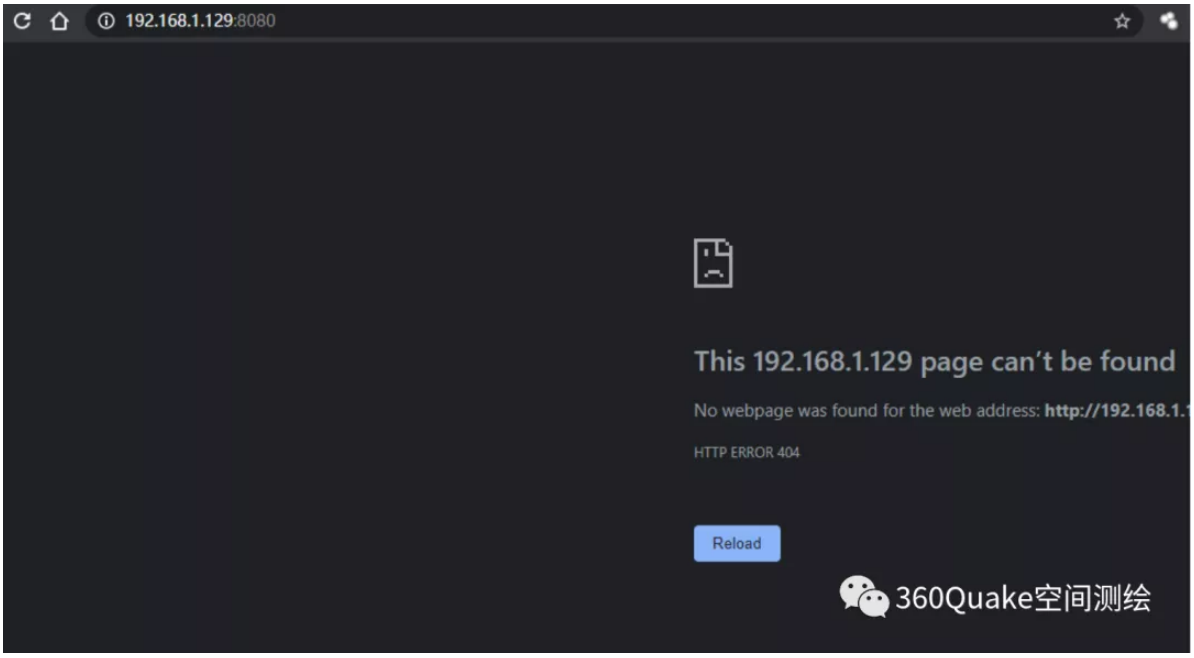
0x03 Beacon Staging Server

Beacon Staging Server的作用是为了防止Payload过大或者适应不同的攻击场景，可以分阶段进行payload投递。

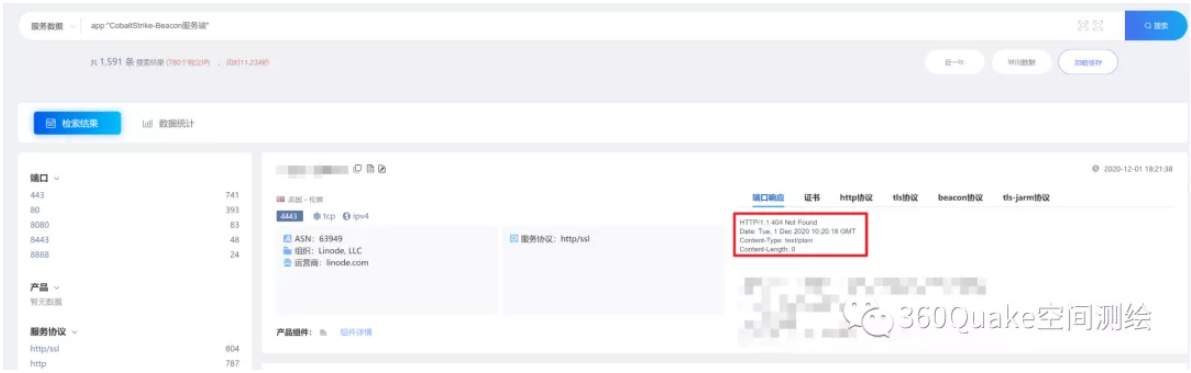
首先通过投递一个被称为stager的小巧的payload，然后去Beacon staging server下载体积较大更复杂的stage，并且访问stage的URL通过checksum8进行校验。

当存储着Beacon配置和payload的stage服务器暴露在公网上的时候，是可以通过主动测绘手段发现的。

不幸的是，默认情况下访问该服务是一个伪装的404页面。这也导致了各类扫描器、空间测绘系统、威胁情报平台等并不能基于页面response信息进行有效判断。

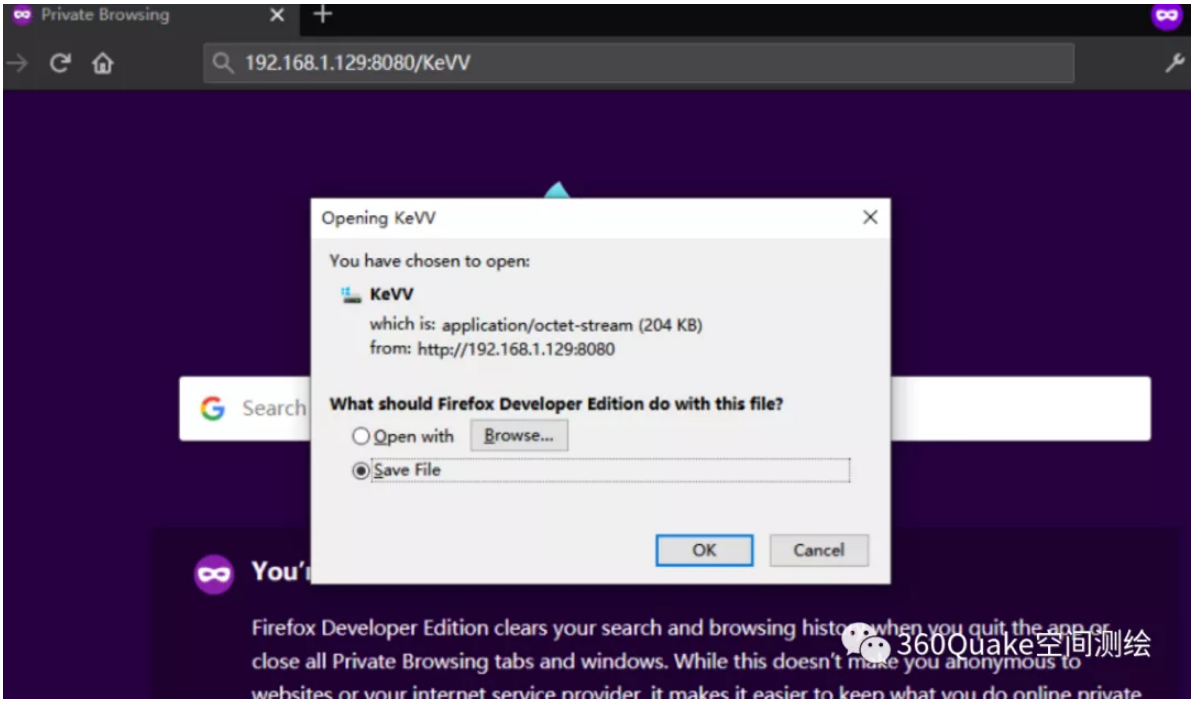


如果不经过专门的扫描识别，一个Beacon Staging Server应该只会返回下图红框内的信息。



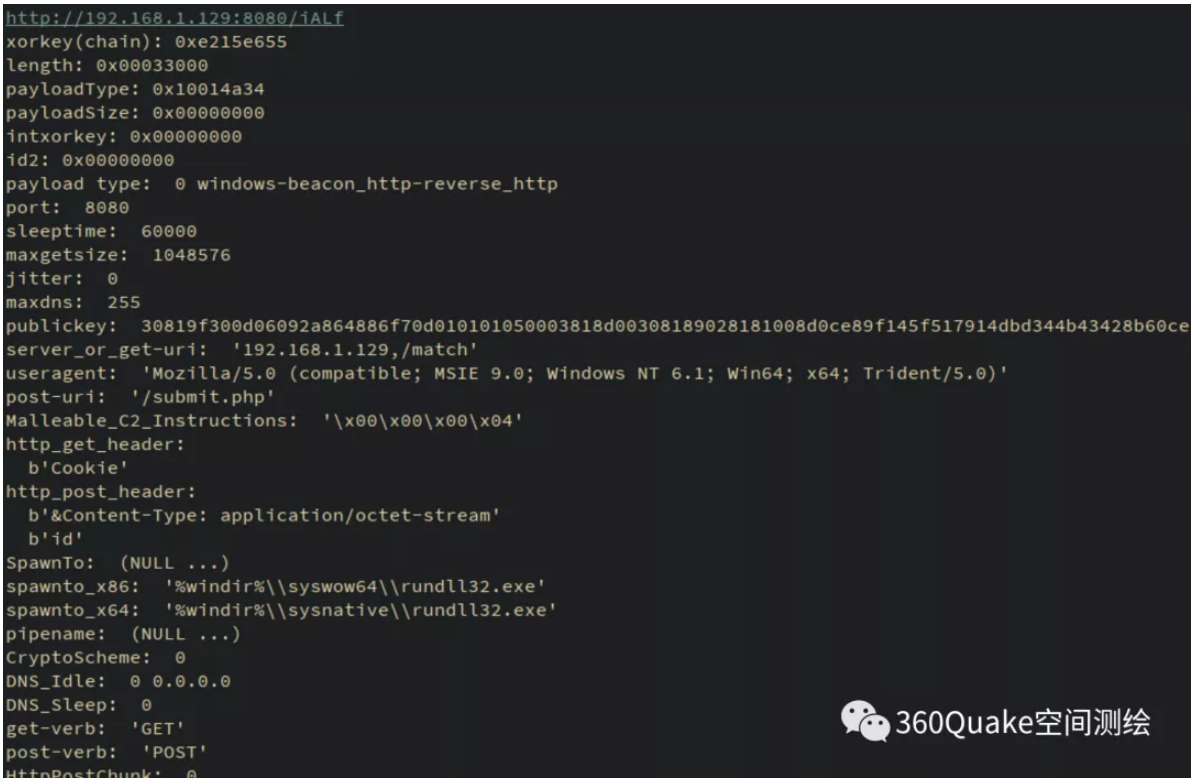
需要拿到具体的Stage，就必须知道URL的生成算法。这段算法来自于公开的NSE脚本，我们使用以下脚本进行校验码的生成，并且可以根据不同的输入生成32位或64位的payload的校验码。

通过拼接校验码到URL，我们便可以直接下载到Beacon的stage文件，而不是一个404页面。



0x04 解析Beacon配置

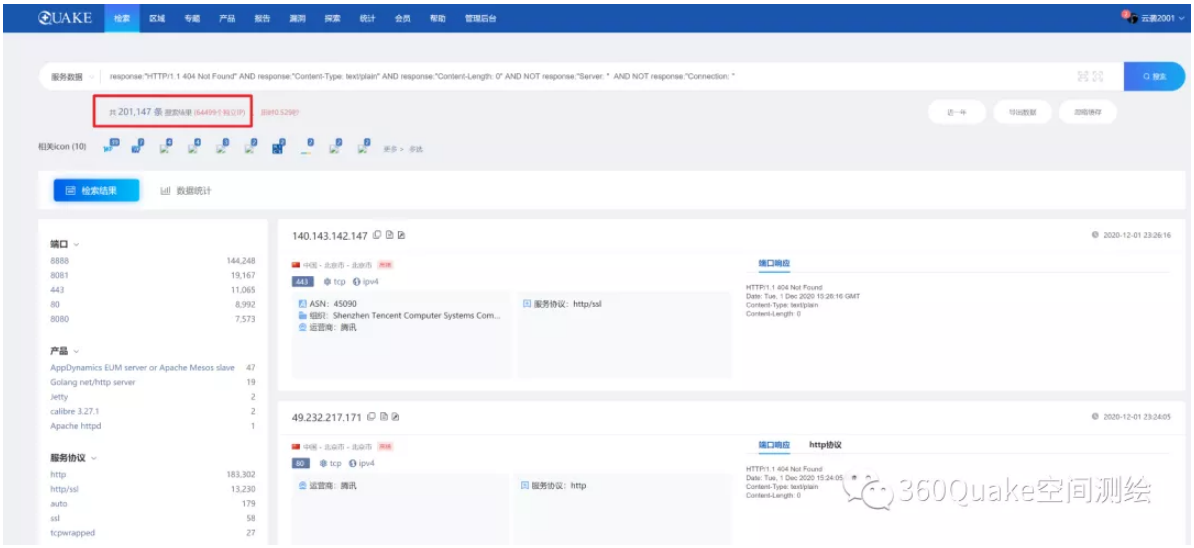
从Beacon staging server成功下载到stage后，我们需要对其进行解析。JPCERT在2018年发布了一个Volatility 插件cobaltstrikescan，用来解析Beacon的配置和payload。



0x05 Quake主动测绘

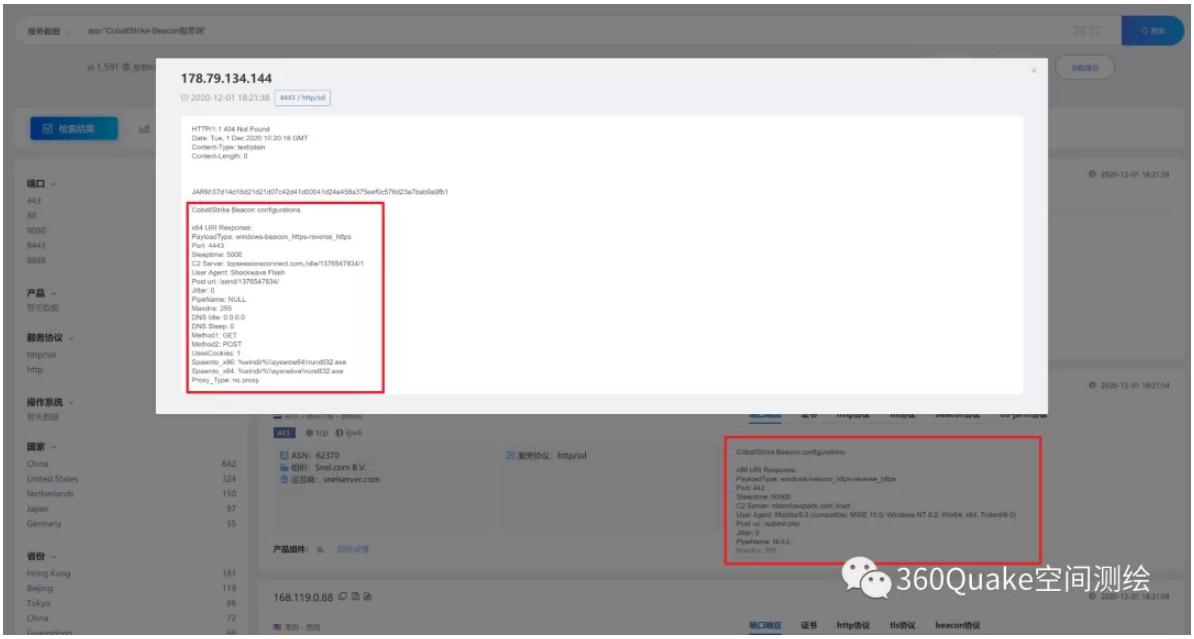
在明确了Beacon Staging Server的工作原理后，我们首先利用如下Quake搜索语法找出一批原始目标：

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: "



然后将上述结果中的IP进行针对性识别，最终我们将提取到的Beacon配置信息追加到了response端口相应之后：

可以使用Quake搜索语法直接进行查询：`app:"CobaltStrike-Beacon服务端"`



同时Quake对Beacon的配置也进行了深度解析，可以点击 beacon协议 查看：


```
{
  "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",
```

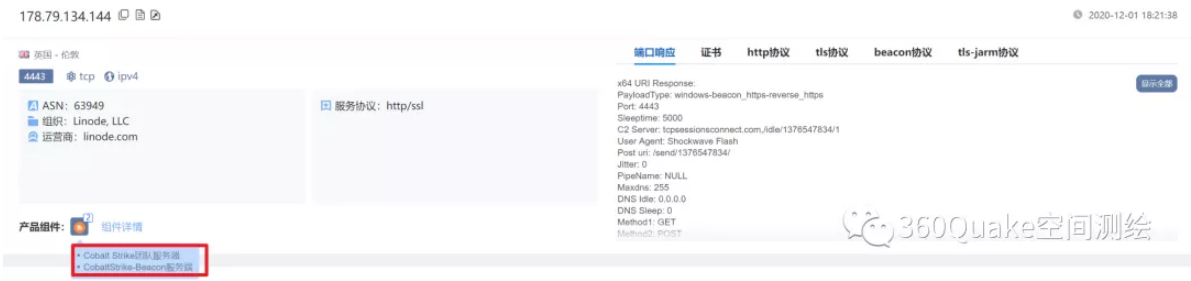
```
    "process_inject_stub": "F\\xa0úã\\x03äÒmaÿÆ£G\\xadïV",
    "publickey": "" 公钥
  },
  "x64": {
    "payloadtype": "",
    "port": "8080",
    "sleeptime": "60000",
    "c2_server": "1",
    "user_agent": "",
    "post_uri": "/submit.php",
    "jitter": "0",
    "pipename": "NULL",
    "maxdns": "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": ""
  }
}
```


至此，Quake系统已经支持了2个有关Cobalt Strike的产品指纹识别，分别是：

`app:"Cobalt Strike团队服务器"`

`app:"CobaltStrike-Beacon服务端"`

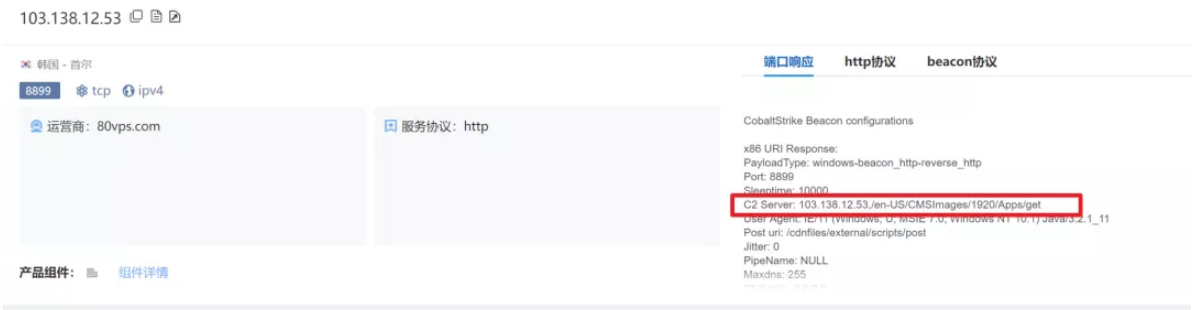
在Quake的检索结果页面上也会有标识：

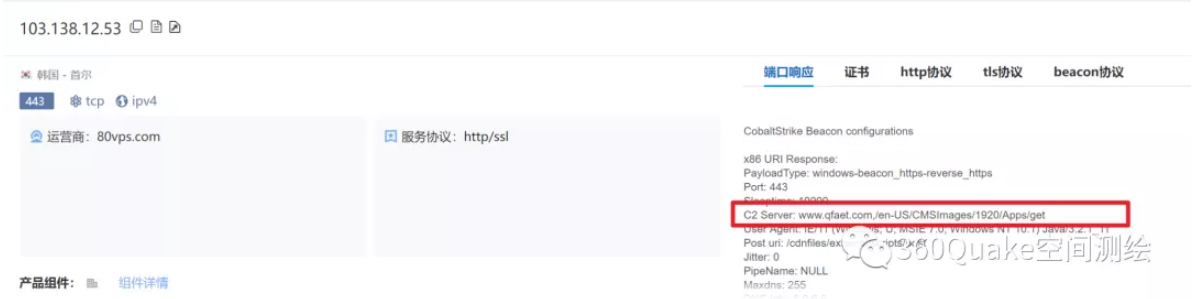


0x06 C2节点提取与分析

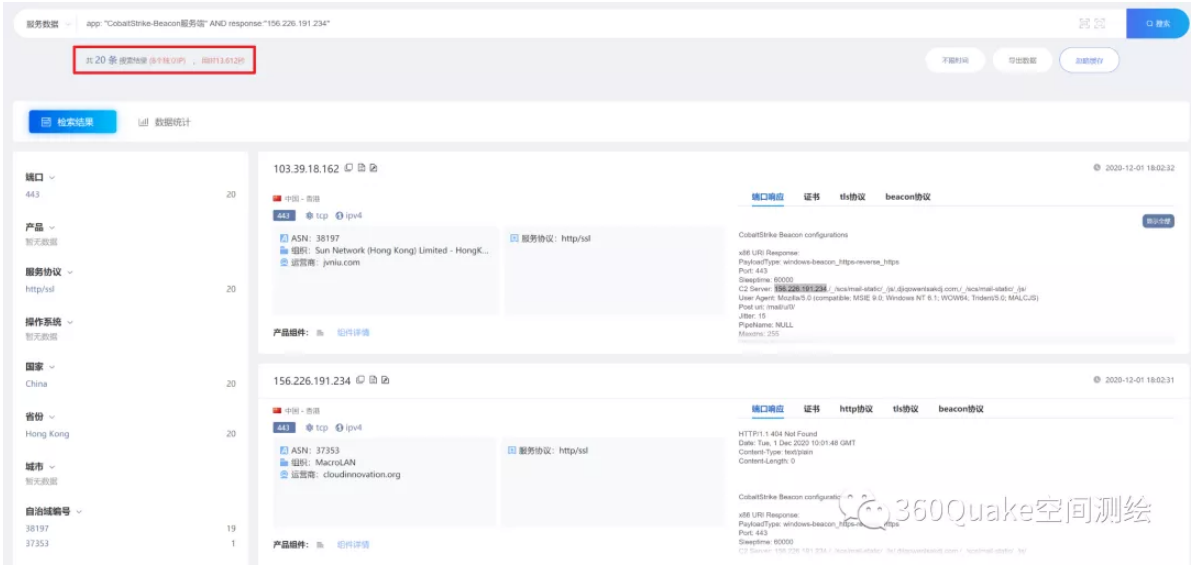
在能够正常解析Beacon的配置文件后，我们可以看出`c2_server`字段是C2服务器及其URL的地址，因此我们进行提取和分析后发现如下几个现像：

1. 绝大多数的C2地址就是Cobalt Strike其自身的IP，但是部分C2节点使用了域名进行连接；
2. 相同IP的不同端口，C2节点配置不同，例如`103.138.12[.]53`。可以利用该现像找到C2真实IP。同时也可能说明该Cobalt Strike配置了多个C2节点：





3. 存在多个不同的Cobalt Strike IP使用相同的C2地址现像。经过分析，可以判定这种情况是Cobalt Strike团队服务器有多个IP地址、或者有多个团队服务器：



4. 存在一个Cobalt Strike IP使用不同C2的现像，例如搜索 `app: "CobaltStrike-Beacon服务端" 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

5. 大多数C2节点使用的域名是新的IoC，在VirusTotal等平台中基本不会被判黑。

0x07 部分IoC

截至本文编辑完成时，我们将已经识别出Beacon配置中C2地址进行了提取分析：
共计777个CobaltStrike独立IP，781个 Beacon** C2地址（其中独立IP580个，独立域名201个)。**
部分IoC如下：

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

由于C2节点是攻击者手工配置的，并不能保证全部都是100%判黑的依据（例如C2是内网IP或者是白名单域名），请悉知。

如需获取全部IoC数据，请使用Quake系统 https://quake.360.cn 搜索：`app: "CobaltStrike-Beacon服务端"`下载。

相关监管部门、企事业单位可联系当地360政企安全销售人员获取。

0x08 结论

正如Quake在产品发布会和今年ISC空间测绘分论坛上所讲的：

网络空间测绘，始于资产，但不止于资产。

我们认为，主动测绘数据将会与终端行为样本数据、网络流量通信数据一样，是未来网络安全大数据&&威胁情报数据的重要源头。主动测绘数据和基于测绘数据分析后形成的知识将能够极大补充我们的视野，从而开拓出更多的攻击面和领域。
更多网络空间测绘领域研究内容，敬请期待~

0x09 参考链接

- 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