关于 Cobalt Strike 检测方法与去特征的思考

作者：毁三观大人 Dm

校对：Flame

DeadEye 安全实验室出品，未经授权，禁止洗搞，如有洗搞，肯定搞你

人云亦云

关于检测 Cobalt Strike 的方法有很多，而网上有一些文章会告诉大家如何修改所谓的特征值，但是这些方法实际上存在一定的误导和盲区

一般发现 Cobalt Strike 服务器的途径有以下几种（简单分类，不准确，勿喷）

样本分析

中马回连

黑客连主控端

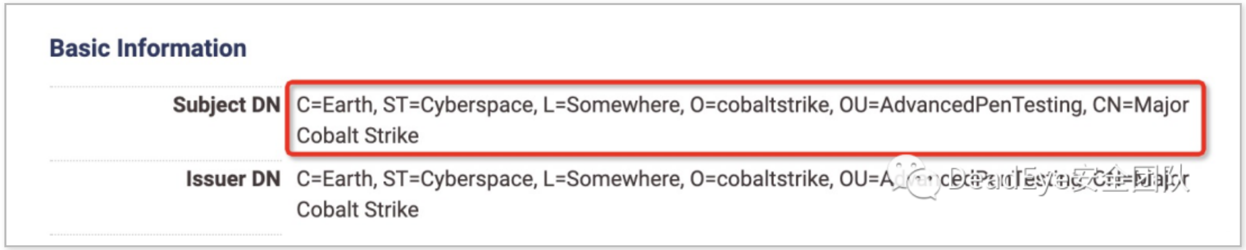
扫描发现

这里被使用的比较多的就是扫描发现，同时网上一些文章提到 Cobalt Strike 默认的 SSL/TLS 证书是固定的，所以一般都是使用这个证书作为特征值来发现 Cobalt Strike 服务器

所以，今天我们主要讨论这个默认 SSL/TLS 证书的问题

证书修改

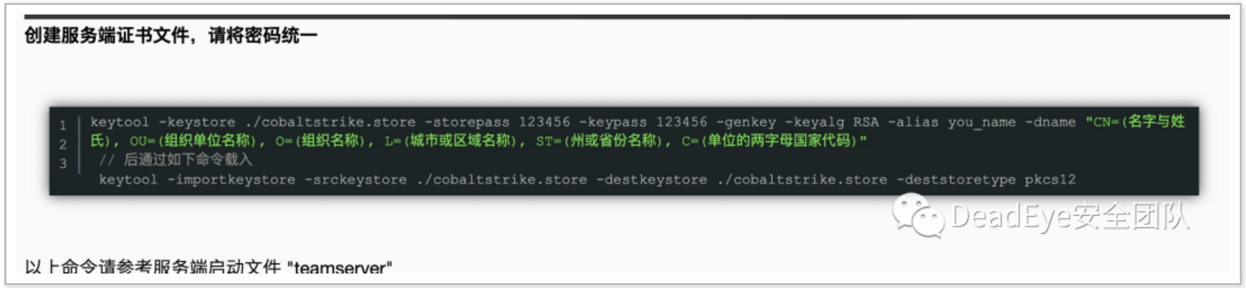
现在让我们提取这个证书的相关信息



Basic Information

Subject DN	C=Earth, ST=Cyberspace, L=Somewhere, O=cobaltstrike, OU=AdvancedPenTesting, CN=Major Cobalt Strike
Issuer DN	C=Earth, ST=Cyberspace, L=Somewhere, O=cobaltstrike, OU=AdvancedPenTesting, CN=Major Cobalt Strike

根据网上一些文章的修改方法，我们需要使用 keytool 修改证书信息，方法如下



创建服务端证书文件，请将密码统一

```
keytool -keystore ./cobaltstrike.store -storepass 123456 -keypass 123456 -genkey -keyalg RSA -alias you_name -dname "CN=(名字与姓氏), OU=(组织单位名称), O=(组织名称), L=(城市或区域名称), ST=(州或省份名称), C=(单位的两字母国家代码)"
 // 后通过如下命令载入
 keytool -importkeystore -srckeystore ./cobaltstrike.store -destkeystore ./cobaltstrike.store -deststoretype pkcs12
```

以上命令请参考服务端启动文件 "teamserver"

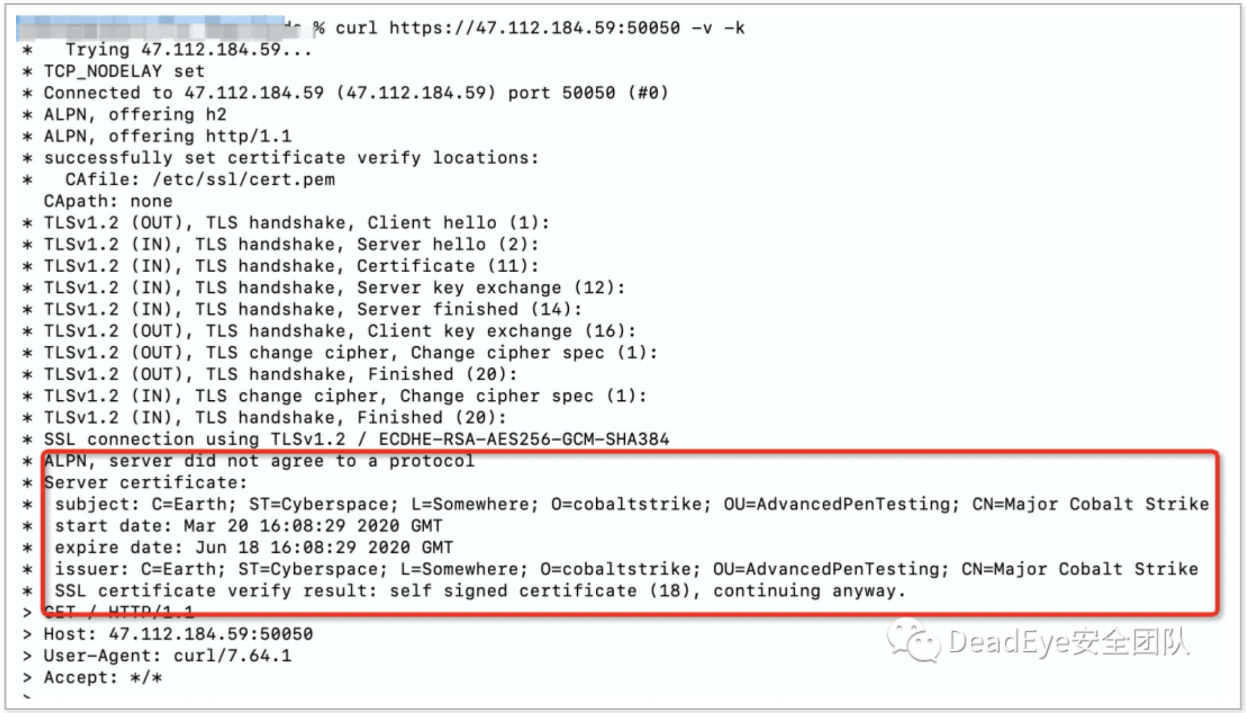
默认的证书具有很明显的特征，例如

```
O=cobaltstrike, OU=AdvancedPenTesting, CN=Major Cobalt Strike
```

我们拿这个信息去检索就可以发现许多 Cobalt Strike 服务器

但是这里忽略了一个问题，你到底修改的是什么证书，是主机上线的时候使用的吗?

这个证书是 teamserver 主控端使用的加密证书（默认端口 50050)



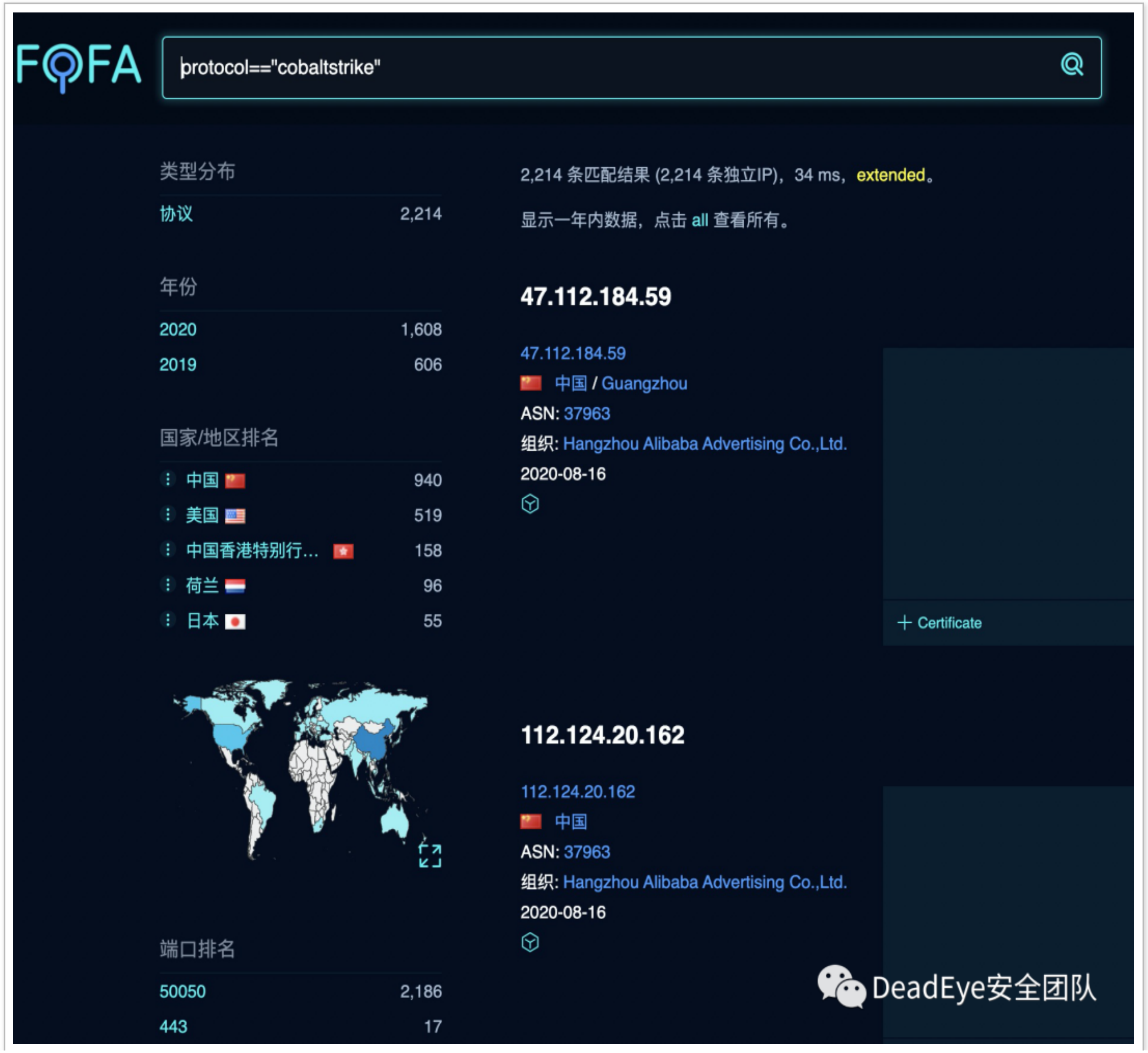
```
[redacted] % curl https://47.112.184.59:50050 -v -k
*   Trying 47.112.184.59...
* TCP_NODELAY set
* Connected to 47.112.184.59 (47.112.184.59) port 50050 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/cert.pem
  CApath: none
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server key exchange (12):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / ECDHE-RSA-AES256-GCM-SHA384
* ALPN, server did not agree to a protocol
* Server certificate:
*  subject: C=Earth; ST=Cyberspace; L=Somewhere; O=cobaltstrike; OU=AdvancedPenTesting; CN=Major Cobalt Strike
*  start date: Mar 20 16:08:29 2020 GMT
*  expire date: Jun 18 16:08:29 2020 GMT
*  issuer: C=Earth; ST=Cyberspace; L=Somewhere; O=cobaltstrike; OU=AdvancedPenTesting; CN=Major Cobalt Strike
*  SSL certificate verify result: self signed certificate (18), continuing anyway.
> GET / HTTP/1.1
> Host: 47.112.184.59:50050
> User-Agent: curl/7.64.1
> Accept: */*
>
```

修改这个证书以后 teamserver 服务器主控端的特征是没了

之前有一些人 hunting C2 服务器使用的就是这个规则

例如在 fofa.so 中，就有一条规则叫

```
protocol=="cobaltstrike"
```



protocol=="cobaltstrike"

类型分布

协议	2,214

年份

2020	1,608
2019	606

国家/地区排名

中国	940
美国	519
中国香港特别行...	158
荷兰	96
日本	55

端口排名

50050	2,186
443	17

2,214 条匹配结果 (2,214 条独立IP)，34 ms，extended。

显示一年内数据，点击 all 查看所有。

47.112.184.59

47.112.184.59
中国 / Guangzhou
ASN: 37963
组织: Hangzhou Alibaba Advertising Co.,Ltd.
2020-08-16

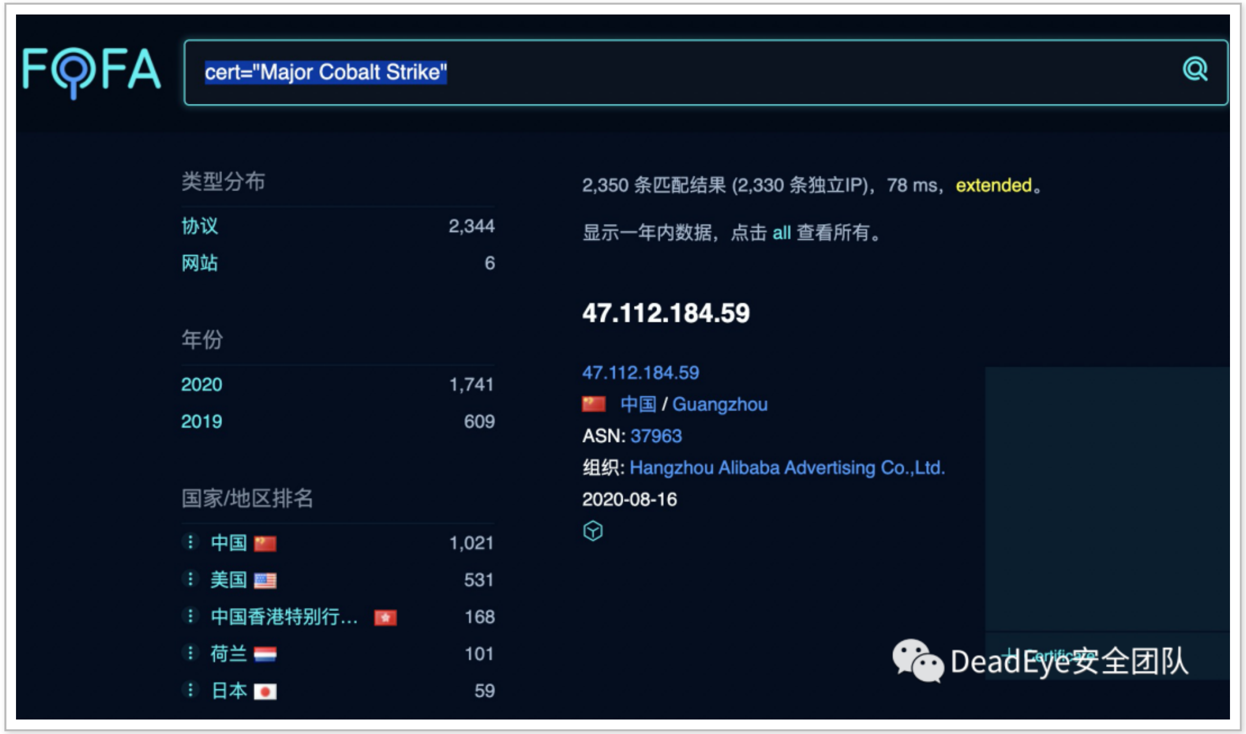
112.124.20.162

112.124.20.162
中国
ASN: 37963
组织: Hangzhou Alibaba Advertising Co.,Ltd.
2020-08-16

当然，我们也可以使用

```
cert="Major Cobalt Strike"
```

直接搜索



cert="Major Cobalt Strike"

类型分布

协议	2,344
网站	6

年份

2020	1,741
2019	609

国家/地区排名

中国	1,021
美国	531
中国香港特别行...	168
荷兰	101
日本	59

2,350 条匹配结果 (2,330 条独立IP)，78 ms，extended。

显示一年内数据，点击 all 查看所有。

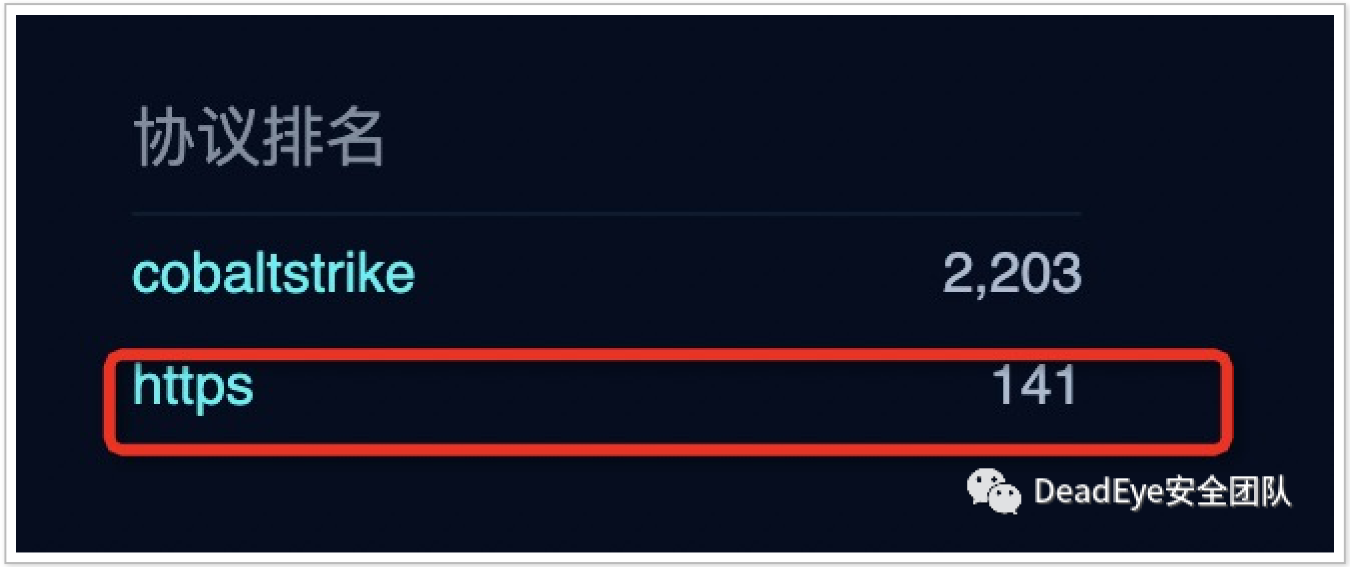
47.112.184.59

47.112.184.59
中国 / Guangzhou
ASN: 37963
组织: Hangzhou Alibaba Advertising Co.,Ltd.
2020-08-16

这里需要注意，使用

```
cert="Major Cobalt Strike"
```

搜索会发现有一些主机并没有被标注为 Cobalt Strike 服务器



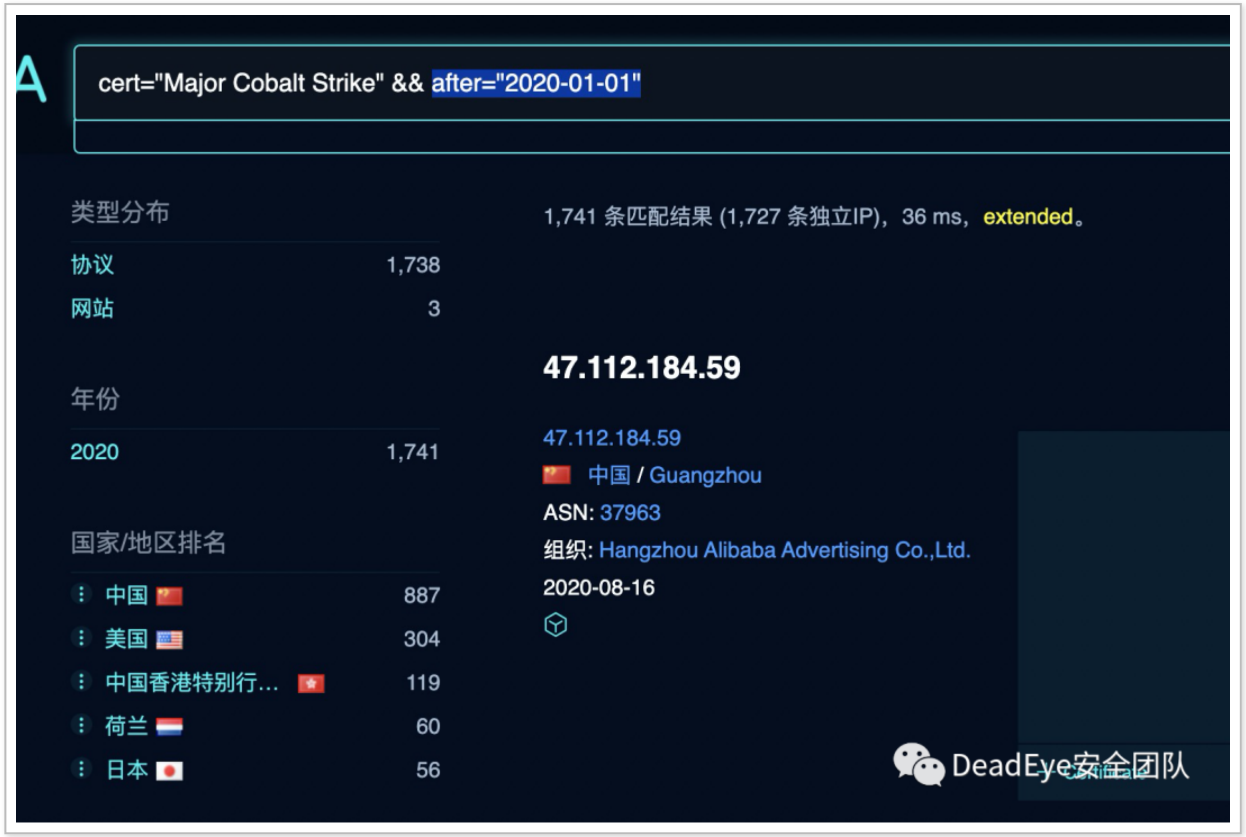
协议排名

cobaltstrike	2,203
https	141

（存在漏网之鱼

当然为了保证数据的时效性，我们在 fofa.so 搜索的时候最好加上

```
after="2020-01-01"
```



cert="Major Cobalt Strike" && after="2020-01-01"

类型分布

协议	1,738
网站	3

年份

2020	1,741

国家/地区排名

中国	887
美国	304
中国香港特别行...	119
荷兰	60
日本	56

1,741 条匹配结果 (1,727 条独立IP)，36 ms，extended。

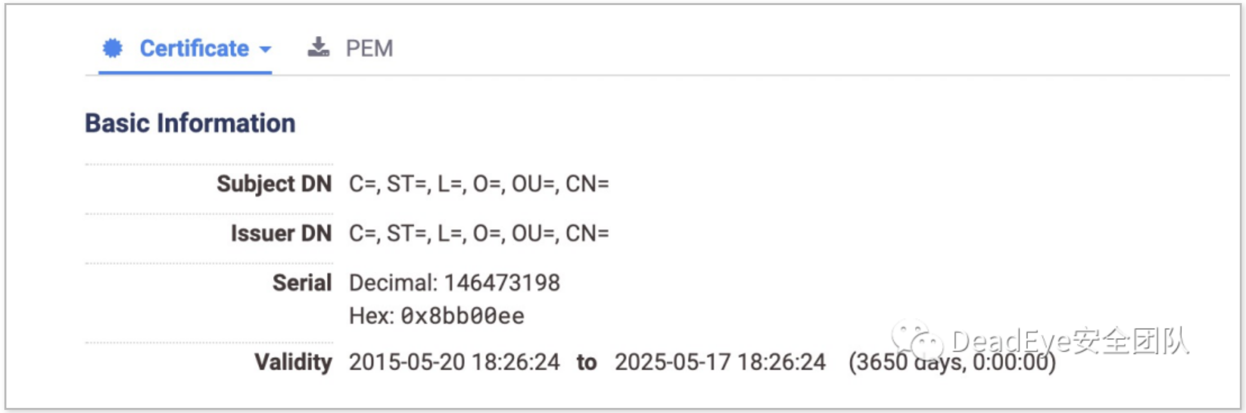
47.112.184.59

47.112.184.59
中国 / Guangzhou
ASN: 37963
组织: Hangzhou Alibaba Advertising Co.,Ltd.
2020-08-16

重要的分割线！！！！注意！！！！

但是！https 上线使用的证书，并不是上边我们修改的那一个，并且这个证书也是默认的...

证书信息如下图：



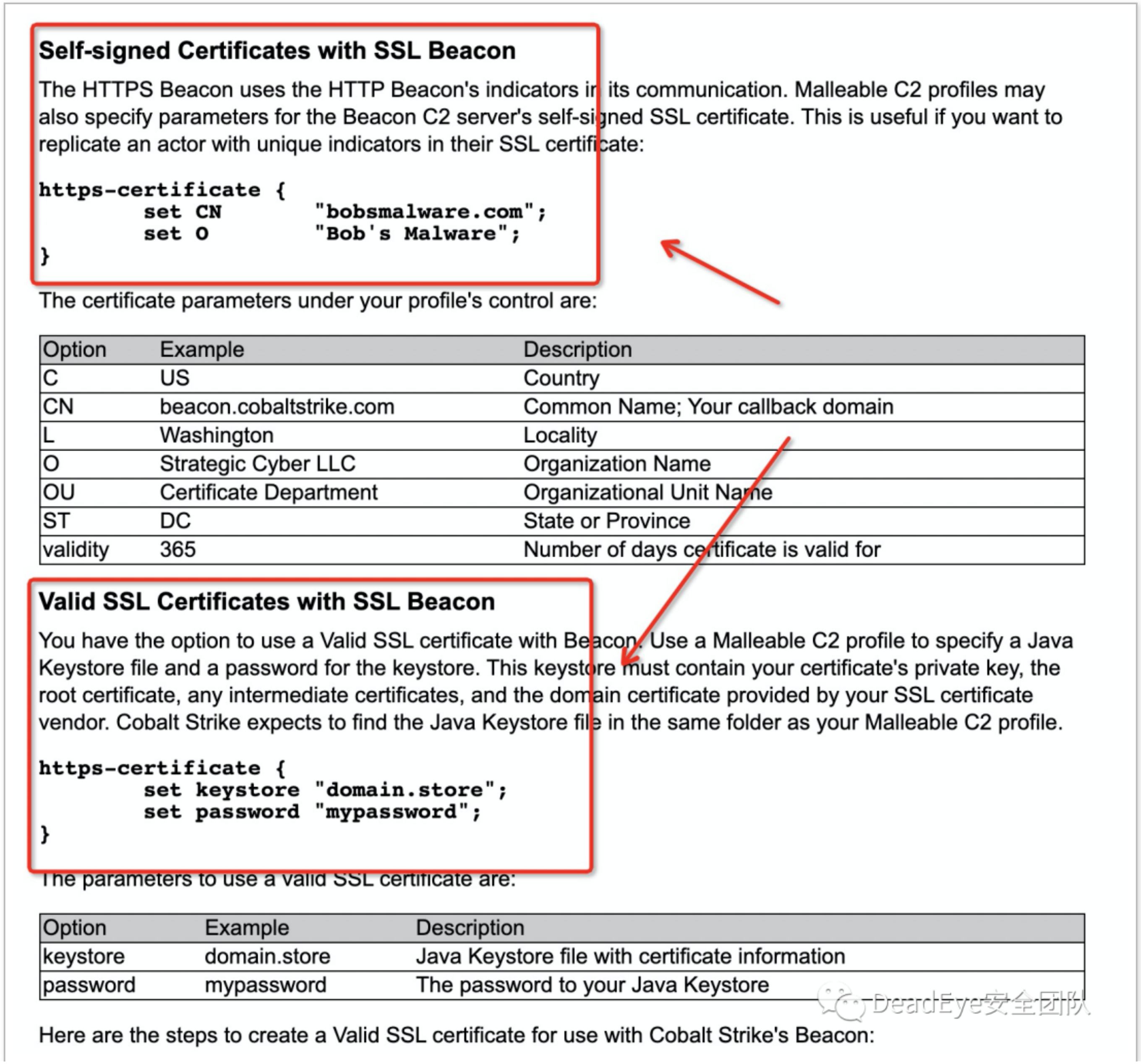
Basic Information

Subject DN	C=, ST=, L=, O=, OU=, CN=
Issuer DN	C=, ST=, L=, O=, OU=, CN=
Serial	Decimal: 146473198 Hex: 0x8bb00ee
Validity	2015-05-20 18:26:24 **to** 2025-05-17 18:26:24 (3650 days, 0:00:00)

如果想要修改这个证书，需要修改 Malleable C2 profile

查看官方文档

https://www.cobaltstrike.com/help-malleable-c2



Self-signed Certificates with SSL Beacon

The HTTPS Beacon uses the HTTP Beacon's indicators in its communication. Malleable C2 profiles may also specify parameters for the Beacon C2 server's self-signed SSL certificate. This is useful if you want to replicate an actor with unique indicators in their SSL certificate:

```
https-certificate {
        set CN       "bobsmalware.com";
        set O        "Bob's Malware";
}
```

The certificate parameters under your profile's control are:

Option	Example	Description
C	US	Country
CN	beacon.cobaltstrike.com	Common Name; Your callback domain
L	Washington	Locality
O	Strategic Cyber LLC	Organization Name
OU	Certificate Department	Organizational Unit Name
ST	DC	State or Province
validity	365	Number of days certificate is valid for

Valid SSL Certificates with SSL Beacon

You have the option to use a Valid SSL certificate with Beacon. Use a Malleable C2 profile to specify a Java Keystore file and a password for the keystore. This keystore must contain your certificate's private key, the root certificate, any intermediate certificates, and the domain certificate provided by your SSL certificate vendor. Cobalt Strike expects to find the Java Keystore file in the same folder as your Malleable C2 profile.

```
https-certificate {
        set keystore "domain.store";
        set password "mypassword";
}
```

The parameters to use a valid SSL certificate are:

Option	Example	Description
keystore	domain.store	Java Keystore file with certificate information
password	mypassword	The password to your Java Keystore

Here are the steps to create a Valid SSL certificate for use with Cobalt Strike's Beacon:

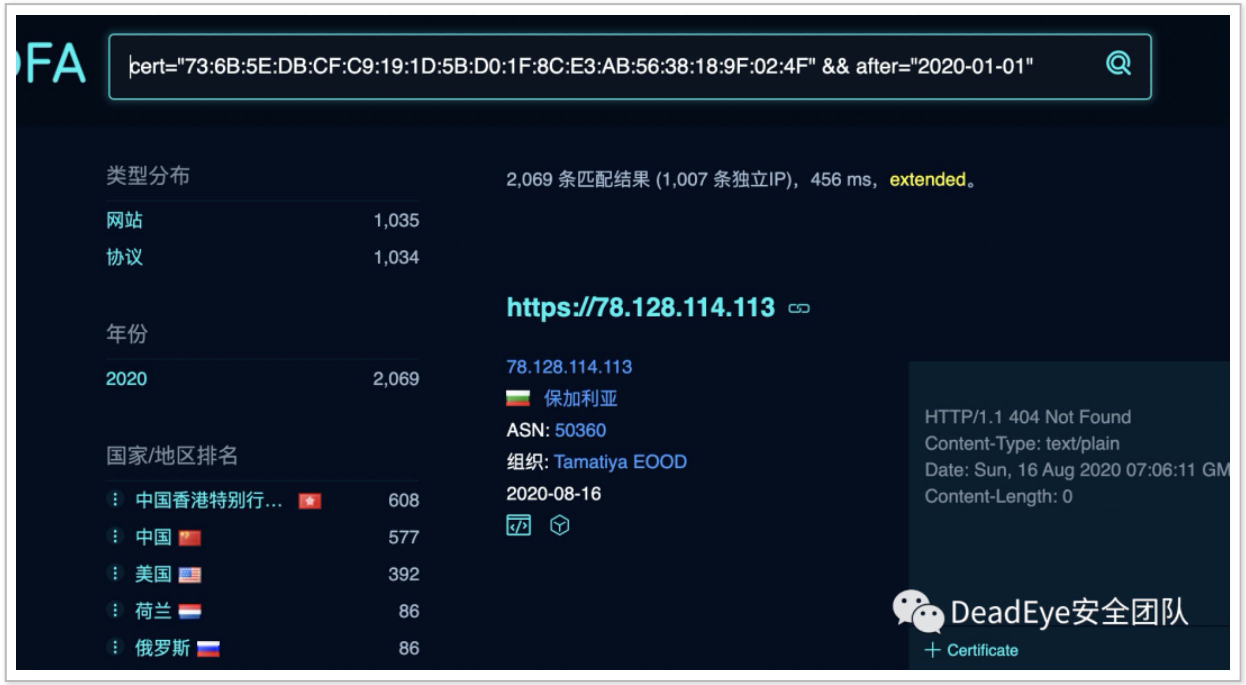
其中 Self-signed Certificates with SSL Beacon 和 Valid SSL Certificates with SSL Beacon 是用来修改 https 上线使用的证书的，Self-signed Certificates with SSL Beacon 根据字母意

思理解，就是自己设定的自签名证书，还有如果使用了 Valid SSL Certificates with SSL Beacon，我们在之前通过 keytool 设置的证书也可以用的上，但是这里应该让我们使用的是真实的证书，不管是偷来的还是买来的，用就完了

Let's Hunt!

使用 fofa.so 搜索相关证书信息

```
cert="73:6B:5E:DB:CF:C9:19:1D:5B:D0:1F:8C:E3:AB:56:38:18:9F:02:4F" && after="2020-01-01"
```



cert="73:6B:5E:DB:CF:C9:19:1D:5B:D0:1F:8C:E3:AB:56:38:18:9F:02:4F" && after="2020-01-01"

类型分布

网站	1,035
协议	1,034

年份

2020	2,069

国家/地区排名

中国香港特别行...	608
中国	577
美国	392
荷兰	86
俄罗斯	86

2,069 条匹配结果 (1,007 条独立IP)，456 ms，extended。

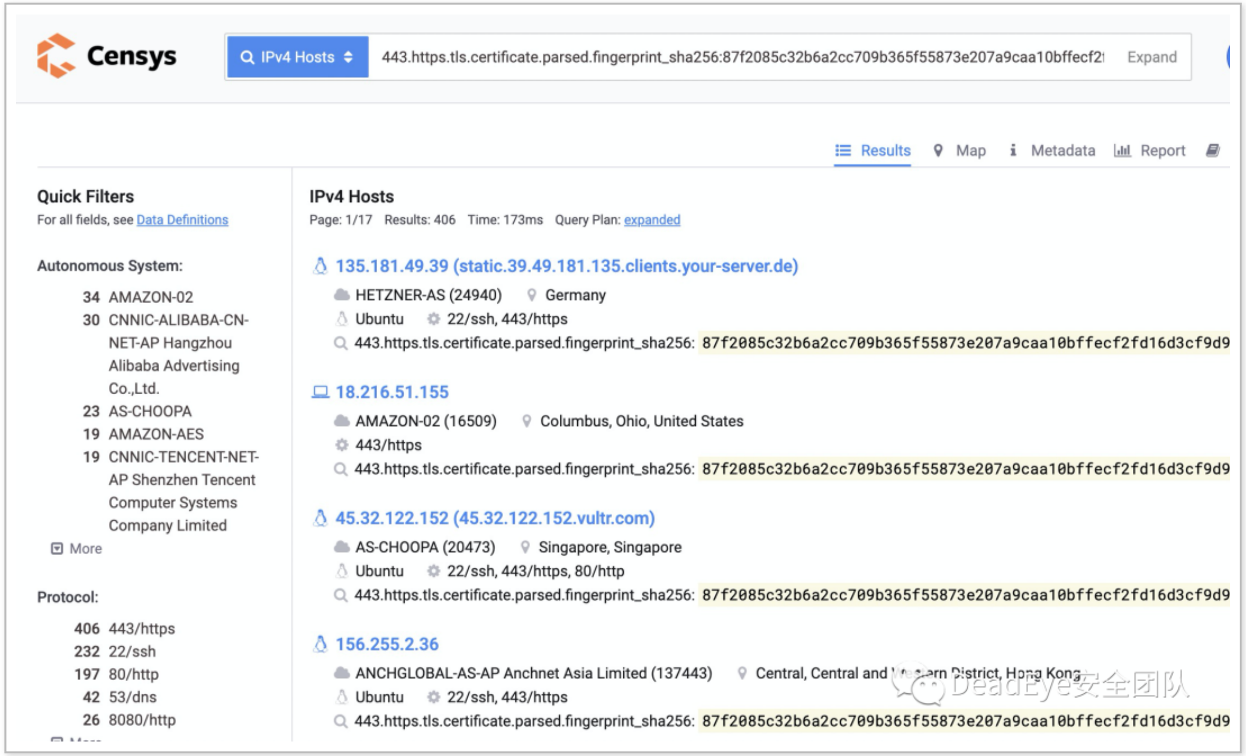
https://78.128.114.113

78.128.114.113
保加利亚
ASN: 50360
组织: Tamatiya EOOD
2020-08-16

```
HTTP/1.1 404 Not Found
Content-Type: text/plain
Date: Sun, 16 Aug 2020 07:06:11 GM
Content-Length: 0
```

使用 censys.io 搜索相关信息

```
443.https.tls.certificate.parsed.fingerprint_sha256:87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2fd16d3cf9d94d390c
```



443.https.tls.certificate.parsed.fingerprint_sha256:87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2

Quick Filters
For all fields, see Data Definitions

Autonomous System:

34	AMAZON-02
30	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd.
23	AS-CHOOPA
19	AMAZON-AES
19	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited

More

Protocol:

406	443/https
232	22/ssh
197	80/http
42	53/dns
26	8080/http

IPv4 Hosts
Page: 1/17 Results: 406 Time: 173ms Query Plan: expanded

135.181.49.39 (static.39.49.181.135.clients.your-server.de)
HETZNER-AS (24940) Germany
Ubuntu 22/ssh, 443/https
443.https.tls.certificate.parsed.fingerprint_sha256: 87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2fd16d3cf9d9

18.216.51.155
AMAZON-02 (16509) Columbus, Ohio, United States
443/https
443.https.tls.certificate.parsed.fingerprint_sha256: 87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2fd16d3cf9d9

45.32.122.152 (45.32.122.152.vultr.com)
AS-CHOOPA (20473) Singapore, Singapore
Ubuntu 22/ssh, 443/https, 80/http
443.https.tls.certificate.parsed.fingerprint_sha256: 87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2fd16d3cf9d9

156.255.2.36
ANCHGLOBAL-AS-AP Anchnet Asia Limited (137443) Central, Central and Western District, Hong Kong
Ubuntu 22/ssh, 443/https
443.https.tls.certificate.parsed.fingerprint_sha256: 87f2085c32b6a2cc709b365f55873e207a9caa10bffecf2fd16d3cf9d9

这里我们可以发现一些有趣的现象，例如有些服务器的 50050 端口也开了，teamserver 主控端的证书确实也是修改了，这证明攻击者还是会看一下文章学习如何去特征，但不幸的是只修改了一个

仅仅是扫描 ip 就能拿到所有证书吗？不能，我们也需要扫描域名，还有就是 https 也不一定只开在 443 端口上

据我们了解，好多人搭建 C2 服务器的方法都比较原始，比如在某云搭建 C2 服务器，不会使用 slb/elb 转发请求，不会使用 security group 控制访问，不会使用一些高明的隐藏 C2 的方法。

并且烂大街的 Domain fronting、CDN 上线、高信誉服务等等也不会使用，就是上线梭哈一把刷..... 真的是给蓝队兄弟们一条生路

等等，到这就完了吗?

检测加密流量

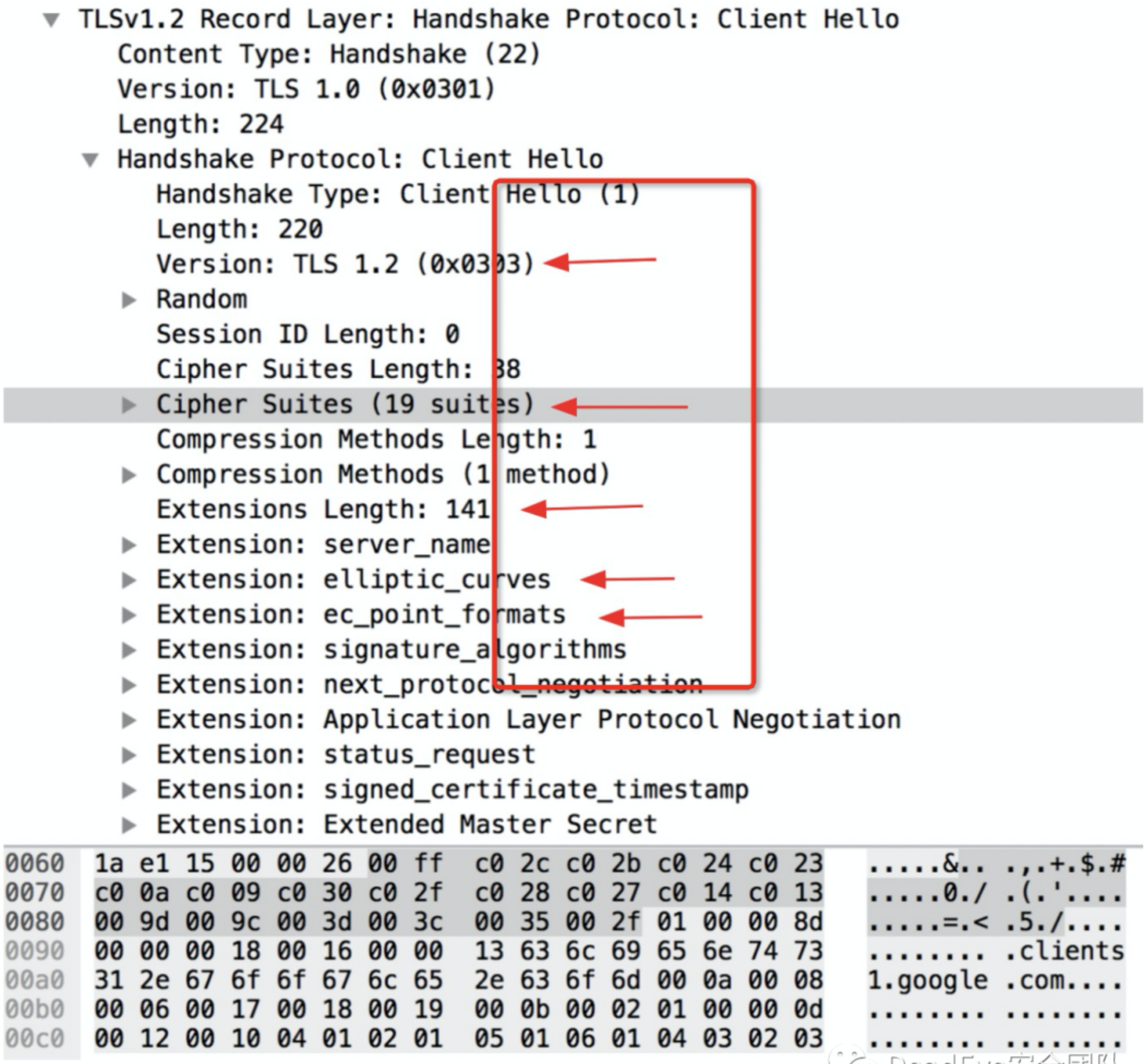
如果这些信息都修改了我们该怎么办那?

实际上还是有方法去检测的

我们可以参考 https://github.com/salesforce/ja3 这个项目

简单科普一下 JA3

JA3 方法用于收集 Client Hello 数据包中以下字段的十进制字节值：版本、可接受的密码、扩展列表、椭圆曲线密码和椭圆曲线密码格式。然后，它将这些值串联在一起，使用 “,” 来分隔各个字段，同时，使用 “-” 来分隔各个字段中的各个值。



```
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 224
  ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 220
      Version: TLS 1.2 (0x0303)
    ▶ Random
      Session ID Length: 0
      Cipher Suites Length: 38
    ▶ Cipher Suites (19 suites)
      Compression Methods Length: 1
    ▶ Compression Methods (1 method)
      Extensions Length: 141
    ▶ Extension: server_name
    ▶ Extension: elliptic_curves
    ▶ Extension: ec_point_formats
    ▶ Extension: signature_algorithms
    ▶ Extension: next_protocol_negotiation
    ▶ Extension: Application Layer Protocol Negotiation
    ▶ Extension: status_request
    ▶ Extension: signed_certificate_timestamp
    ▶ Extension: Extended Master Secret
0060  1a e1 15 00 00 26 00 ff  c0 2c c0 2b c0 24 c0 23   .....&.. .,.+.$.#
0070  c0 0a c0 09 c0 30 c0 2f  c0 28 c0 27 c0 14 c0 13   .....0./ .(.'....
0080  00 9d 00 9c 00 3d 00 3c  00 35 00 2f 01 00 00 8d   .....=.< .5./....
0090  00 00 00 18 00 16 00 00  13 63 6c 69 65 6e 74 73   ........ .clients
00a0  31 2e 67 6f 6f 67 6c 65  2e 63 6f 6d 00 0a 00 08   1.google .com....
00b0  00 06 00 17 00 18 00 19  00 0b 00 02 01 00 00 0d   ........ ........
00c0  00 12 00 10 04 01 02 01  05 01 06 01 04 03 02 03   ........ ........
```

Example Client Hello packet as viewed in Wireshark

这里相当于把支持的 TLS 扩展信息，都收集起来当作一个特征值来用（除了客户端发起的，还有关于服务器的 JA3S）

这其实算一种降维打击，并且我们发现主流在线沙箱、主流 IDS 大都支持了 JA3/JA3S 指纹检测

因为本篇文章主要是讨论 Cobalt Strike 默认证书的问题，所以在这里就不过多介绍 JA3/JA3S 相关的信息了

IOCs:

2[.]56.212.165

3[.]106.130.137

3[.]11.62.87

3[.]121.32.171

3[.]128.154.6

3[.]129.110.164

3[.]129.19.175

3[.]130.5.32

3[.]130.75.203

3[.]135.199.11

3[.]16.137.85

3[.]218.141.232

3[.]22.141.197

3[.]22.195.74

3[.]234.252.217

3[.]234.255.7

3[.]236.183.143

3[.]25.149.16

3[.]25.162.235

3[.]25.177.162

3[.]25.180.21

3[.]80.164.184

3[.]95.136.233

3[.]95.159.27

5[.]149.253.199

5[.]180.99.65

5[.]188.206.219

5[.]39.216.203

5[.]39.217.115

5[.]39.221.60

5[.]45.64.36

5[.]8.18.50

8[.]210.152.83

8[.]210.52.10

13[.]124.92.145

13[.]211.161.113

13[.]211.170.37

13[.]211.180.107

13[.]229.222.207

13[.]236.208.125

13[.]54.198.47

13[.]59.192.233

13[.]91.4.128

18[.]130.144.147

18[.]130.155.157

18[.]163.206.98

18[.]163.46.190

18[.]166.31.113

18[.]215.167.27

18[.]216.51.155

18[.]217.19.176

18[.]217.54.127

18[.]224.234.85

23[.]101.204.40

23[.]106.215.179

23[.]248.162.142

23[.]254.202.217

23[.]254.228.89

23[.]254.229.35

23[.]254.230.60

23[.]82.185.91

23[.]82.185.96

23[.]83.248.105

27[.]102.118.181

27[.]102.118.187

27[.]102.118.190

31[.]14.40.230

31[.]210.91.217

31[.]220.43.160

31[.]44.184.125

31[.]44.184.131

31[.]44.184.48

31[.]44.184.49

31[.]44.184.50

31[.]44.184.51

31[.]44.184.53

31[.]44.184.55

34[.]204.3.10

34[.]209.40.26

34[.]212.83.227

34[.]221.2.201

34[.]224.157.70

34[.]230.68.206

34[.]238.192.43

34[.]67.180.214

34[.]80.144.150

34[.]84.39.173

34[.]87.76.219

34[.]92.237.246

34[.]92.57.181

34[.]94.33.19

34[.]96.129.197

34[.]96.245.66

34[.]97.55.204

35[.]164.172.115

35[.]176.207.20

35[.]201.164.132

35[.]203.173.196

35[.]225.244.45

35[.]234.156.244

35[.]235.89.222

35[.]241.125.159

36[.]133.35.7

39[.]100.119.37

39[.]100.233.99

39[.]100.65.99

39[.]100.72.108

39[.]101.174.86

39[.]101.207.137

39[.]101.207.158

39[.]102.37.102

39[.]102.40.225

39[.]102.52.75

39[.]104.162.182

39[.]105.106.14

39[.]105.202.243

39[.]105.229.27

39[.]105.23.21

39[.]105.24.37

39[.]105.55.133

39[.]105.59.107

39[.]105.69.107

39[.]106.107.82

39[.]106.144.55

39[.]106.205.34

39[.]106.21.92

39[.]106.219.95

39[.]106.223.146

39[.]106.81.105

39[.]106.85.139

39[.]106.9.248

39[.]107.101.223

39[.]107.111.157

39[.]107.221.136

39[.]107.231.0

39[.]107.59.30

39[.]107.99.0

39[.]108.181.99

39[.]108.185.207

39[.]108.195.174

39[.]108.236.227

39[.]108.5.55

39[.]108.95.18

39[.]96.1.24

39[.]96.10.181

39[.]96.12.238

39[.]96.13.114

39[.]96.63.97

39[.]97.126.8

39[.]97.187.94

39[.]97.188.94

39[.]97.232.51

39[.]98.157.103

39[.]98.171.162

39[.]98.203.19

40[.]122.106.213

40[.]127.129.199

40[.]70.64.23

40[.]73.6.221

42[.]159.86.108

43[.]224.35.134

43[.]225.30.90

43[.]226.148.151

43[.]226.153.250

43[.]226.26.242

43[.]240.15.68

43[.]242.201.199

43[.]246.208.208

43[.]246.208.225

43[.]246.208.240

43[.]248.124.189

45[.]10.20.166

45[.]11.180.108

45[.]11.180.220

45[.]11.79.20

45[.]113.2.107

45[.]114.10.17

45[.]124.64.53

45[.]134.168.146

45[.]137.10.116

45[.]138.172.81

45[.]138.209.75

45[.]142.124.196

45[.]145.185.68

45[.]153.241.16

45[.]192.118.162

45[.]192.118.163

45[.]192.118.164

45[.]192.118.165

45[.]192.118.166

45[.]248.85.20

45[.]32.116.138

45[.]32.122.112

45[.]32.122.152

45[.]32.32.186

45[.]32.62.198

45[.]32.78.66

45[.]61.136.32

45[.]61.136.46

45[.]66.250.14

45[.]76.106.22

45[.]76.158.91

45[.]76.183.78

45[.]76.208.172

45[.]76.25.185

45[.]77.13.57

45[.]77.143.131

45[.]77.172.168

45[.]77.174.46

45[.]77.18.248

45[.]77.249.181

45[.]77.91.11

45[.]78.67.211

45[.]78.9.49

45[.]82.79.211

45[.]83.140.231

45[.]83.237.19

46[.]166.128.234

46[.]166.129.169

46[.]166.129.170

46[.]166.176.140

46[.]17.98.192

46[.]21.147.5

46[.]255.211.20

46[.]4.157.54

47[.]100.136.26

47[.]100.46.70

47[.]100.48.156

47[.]100.55.126

47[.]100.77.190

47[.]100.89.120

47[.]101.11.214

47[.]101.130.253

47[.]101.149.183

47[.]101.177.45

47[.]101.208.219

47[.]101.35.67

47[.]101.62.0

47[.]102.110.39

47[.]102.86.216

47[.]103.207.83

47[.]103.220.119

47[.]103.220.165

47[.]103.29.187

47[.]103.62.94

47[.]104.108.112

47[.]104.11.169

47[.]104.193.7

47[.]104.238.128

47[.]104.77.93

47[.]104.82.12

47[.]105.146.99

47[.]105.180.183

47[.]105.99.5

47[.]106.70.58

47[.]107.102.61

47[.]107.108.38

47[.]107.136.247

47[.]108.113.23

47[.]108.153.115

47[.]108.60.37

47[.]110.145.60

47[.]110.228.171

47[.]112.184.59

47[.]113.103.131

47[.]113.126.57

47[.]113.94.95

47[.]114.45.227

47[.]114.93.159

47[.]114.93.194

47[.]115.125.106

47[.]115.38.42

47[.]240.43.238

47[.]240.54.247

47[.]244.0.247

47[.]244.13.36

47[.]244.14.7

47[.]244.218.224

47[.]245.12.138

47[.]245.31.124

47[.]52.161.9

47[.]56.151.214

47[.]56.169.92

47[.]56.253.186

47[.]57.186.166

47[.]75.42.43

47[.]75.55.181

47[.]75.86.225

47[.]91.221.115

47[.]91.242.27

47[.]92.155.231

47[.]92.219.198

47[.]92.239.244

47[.]92.255.176

47[.]93.116.160

47[.]93.12.191

47[.]93.229.0

47[.]94.102.248

47[.]94.136.27

47[.]94.14.145

47[.]94.154.108

47[.]94.228.41

47[.]94.96.209

47[.]95.115.1

47[.]95.119.10

47[.]95.194.251

47[.]95.205.52

47[.]97.98.237

47[.]98.131.192

47[.]98.156.92

47[.]98.162.206

47[.]98.166.253

47[.]98.239.204

47[.]98.244.206

47[.]98.247.45

47[.]99.48.241

47[.]99.72.130

49[.]232.20.75

49[.]232.239.196

49[.]232.27.213

49[.]232.39.67

49[.]233.132.10

49[.]233.137.7

49[.]233.155.141

49[.]233.73.185

49[.]233.78.149

49[.]233.85.7

49[.]233.89.89

49[.]234.105.212

49[.]234.155.24

49[.]234.239.23

49[.]234.5.74

49[.]234.64.118

49[.]234.93.171

49[.]234.94.85

49[.]235.119.2

49[.]235.144.34

49[.]235.158.131

49[.]235.166.224

49[.]235.199.136

49[.]235.200.123

49[.]235.204.16

49[.]235.212.74

49[.]235.217.243

49[.]235.22.75

49[.]235.223.77

49[.]235.23.207

49[.]235.23.236

49[.]235.244.235

49[.]235.40.131

49[.]235.42.77

49[.]235.50.54

49[.]235.60.144

49[.]235.90.230

50[.]112.70.12

51[.]15.136.48

51[.]210.87.117

51[.]83.200.186

51[.]91.79.126

52[.]14.171.234

52[.]14.65.166

52[.]147.4.139

52[.]166.232.140

52[.]175.218.135

52[.]22.35.45

52[.]229.22.93

52[.]87.210.1

52[.]90.135.23

52[.]91.46.68

52[.]91.75.52

54[.]153.242.99

54[.]169.240.239

54[.]172.42.32

54[.]174.145.85

54[.]175.230.166

54[.]201.107.45

54[.]206.20.207

54[.]212.69.111

54[.]213.249.7

54[.]214.197.200

54[.]246.146.207

54[.]252.206.69

54[.]252.210.126

54[.]253.108.178

54[.]253.244.200

54[.]80.166.26

60[.]163.129.202

60[.]205.3.82

61[.]141.222.100

62[.]113.117.167

63[.]142.243.214

63[.]34.87.167

64[.]128.143.70

64[.]225.114.141

64[.]227.121.168

64[.]227.6.38

64[.]44.133.156

65[.]49.133.221

65[.]49.135.123

65[.]49.224.215

66[.]152.191.41

66[.]42.62.80

69[.]30.206.250

69[.]30.232.138

69[.]30.232.139

69[.]30.232.140

69[.]30.232.141

69[.]30.232.142

74[.]118.138.159

78[.]128.114.113

78[.]129.165.207

78[.]142.18.157

78[.]142.194.114

78[.]94.208.254

79[.]141.162.41

81[.]70.19.111

81[.]70.30.97

83[.]164.140.60

85[.]92.108.85

85[.]93.20.114

88[.]214.26.29

89[.]45.4.135

91[.]121.76.158

91[.]208.184.81

91[.]241.19.10

92[.]223.105.130

92[.]42.14.133

93[.]115.23.169

94[.]100.18.43

94[.]156.189.168

94[.]232.40.176

94[.]232.43.237

95[.]141.41.18

95[.]142.40.121

95[.]179.134.194

95[.]179.201.34

95[.]179.228.227

95[.]179.236.54

99[.]79.101.225

99[.]81.122.12

100[.]24.234.117

100[.]24.56.227

100[.]25.151.21

101[.]132.116.202

101[.]132.236.129

101[.]132.33.79

101[.]133.137.195

101[.]200.147.217

101[.]200.164.199

101[.]200.53.21

101[.]200.55.39

101[.]200.87.178

101[.]201.121.13

101[.]201.65.35

101[.]32.29.242

101[.]37.24.50

101[.]37.76.212

103[.]147.12.5

103[.]150.8.146

103[.]193.4.11

103[.]209.102.241

103[.]214.165.213

103[.]224.82.171

103[.]238.224.138

103[.]242.134.79

103[.]254.75.240

103[.]255.179.187

103[.]39.108.20

103[.]45.116.10

103[.]45.129.67

103[.]45.173.221

103[.]56.53.100

103[.]68.251.31

103[.]73.161.42

103[.]78.243.197

103[.]78.243.198

103[.]78.243.199

103[.]94.180.33

103[.]97.124.50

104[.]128.93.229

104[.]149.168.199

104[.]154.248.179

104[.]160.41.224

104[.]168.159.36

104[.]168.172.252

104[.]168.174.197

104[.]168.175.192

104[.]168.176.29

104[.]168.214.104

104[.]192.169.78

104[.]194.10.206

104[.]198.151.234

104[.]225.239.196

104[.]237.4.40

104[.]238.134.63

104[.]244.156.156

104[.]251.217.97

106[.]12.90.123

106[.]13.174.69

106[.]13.182.116

106[.]13.33.86

106[.]13.42.155

106[.]13.48.213

106[.]13.8.47

106[.]13.85.189

106[.]14.0.74

106[.]14.189.174

106[.]14.82.209

106[.]15.202.7

106[.]15.249.108

106[.]2.13.25

106[.]52.214.81

106[.]52.235.216

106[.]52.55.45

106[.]53.116.113

106[.]53.226.165

106[.]53.231.16

106[.]53.241.3

106[.]53.243.154

106[.]53.59.24

106[.]53.74.243

106[.]53.97.24

106[.]54.177.4

106[.]54.211.200

106[.]54.241.235

106[.]54.84.65

106[.]54.96.164

106[.]55.153.204

107[.]148.241.235

107[.]148.247.198

107[.]161.188.203

107[.]182.24.70

108[.]177.235.22

108[.]61.162.223

108[.]61.200.55

108[.]61.201.65

109[.]235.70.99

111[.]229.107.34

111[.]229.35.56

111[.]229.51.128

111[.]229.58.217

111[.]230.197.23

111[.]231.228.112

111[.]231.240.158

111[.]231.79.105

111[.]90.149.188

112[.]124.20.162

112[.]126.89.177

112[.]74.33.227

113[.]31.118.7

114[.]116.225.193

114[.]116.41.86

114[.]118.4.213

114[.]215.86.71

114[.]55.106.242

114[.]55.25.227

114[.]55.33.36

116[.]204.170.146

116[.]62.100.78

116[.]62.104.16

116[.]62.174.32

116[.]62.200.143

116[.]85.69.130

117[.]50.80.107

117[.]51.136.34

117[.]51.142.47

117[.]51.150.222

118[.]126.100.187

118[.]178.94.47

118[.]184.23.74

118[.]24.108.239

118[.]24.136.75

118[.]24.170.186

118[.]24.28.219

118[.]24.85.85

118[.]24.9.34

118[.]25.138.119

118[.]25.157.90

118[.]25.71.232

118[.]89.95.126

119[.]23.237.214

119[.]23.241.16

119[.]23.42.235

119[.]23.79.133

119[.]28.194.152

119[.]29.116.14

119[.]29.119.60

119[.]29.132.198

119[.]29.188.218

119[.]3.124.44

119[.]3.140.246

119[.]3.187.188

119[.]3.86.69

119[.]45.136.244

119[.]45.191.253

119[.]45.5.195

119[.]45.56.199

120[.]131.3.43

120[.]132.81.138

120[.]132.81.145

120[.]24.64.98

120[.]25.167.81

120[.]26.160.136

120[.]26.162.133

120[.]26.177.10

120[.]27.17.232

120[.]27.245.125

120[.]27.3.39

120[.]55.194.145

120[.]76.119.147

120[.]77.180.97

120[.]78.176.65

120[.]78.196.37

120[.]79.142.88

120[.]79.210.67

120[.]79.237.135

120[.]79.24.186

120[.]79.28.147

120[.]79.38.19

120[.]92.173.127

121[.]127.234.11

121[.]196.177.46

121[.]196.193.160

121[.]196.27.187

121[.]199.16.25

121[.]36.107.213

121[.]36.12.130

121[.]36.140.230

121[.]36.146.237

121[.]36.149.225

121[.]36.155.174

121[.]36.162.110

121[.]36.175.175

121[.]36.196.31

121[.]36.211.148

121[.]36.215.68

121[.]36.252.20

121[.]36.32.125

121[.]36.37.7

121[.]37.23.161

121[.]40.103.231

121[.]40.124.244

121[.]41.229.1

121[.]41.82.60

121[.]46.4.136

122[.]114.195.209

122[.]51.131.86

122[.]51.137.157

122[.]51.16.84

122[.]51.250.26

122[.]51.253.174

122[.]51.33.2

123[.]206.21.178

123[.]206.210.153

123[.]206.221.27

123[.]206.232.40

123[.]206.47.78

123[.]207.14.227

123[.]56.116.146

123[.]56.228.208

123[.]56.27.243

123[.]56.9.63

123[.]57.143.225

123[.]57.17.24

123[.]57.209.41

123[.]57.241.243

124[.]156.120.11

124[.]156.196.145

124[.]217.230.137

124[.]243.240.42

124[.]70.135.155

124[.]70.151.66

124[.]70.200.2

129[.]204.169.102

129[.]204.207.114

129[.]204.228.7

129[.]204.248.145

129[.]204.89.21

129[.]28.196.47

129[.]28.203.182

132[.]232.3.136

132[.]232.33.160

132[.]232.75.164

134[.]175.132.40

134[.]175.15.58

134[.]175.183.74

134[.]209.130.219

135[.]181.1.70

135[.]181.49.38

135[.]181.49.39

136[.]243.44.50

138[.]128.208.123

138[.]91.90.6

138[.]99.216.18

139[.]129.231.62

139[.]155.18.71

139[.]155.23.11

139[.]155.34.217

139[.]155.69.206

139[.]180.186.130

139[.]180.199.171

139[.]186.10.157

139[.]186.30.246

139[.]196.21.224

139[.]196.37.219

139[.]196.91.13

139[.]198.15.159

139[.]199.100.94

139[.]199.31.223

139[.]217.99.29

139[.]224.31.47

139[.]9.115.85

139[.]9.121.229

139[.]9.128.123

140[.]143.125.186

140[.]82.16.24

140[.]82.19.10

140[.]82.19.26

141[.]164.41.118

141[.]164.48.79

141[.]164.57.174

141[.]164.61.249

141[.]164.63.233

142[.]202.205.57

142[.]202.205.88

143[.]92.49.158

143[.]92.49.159

143[.]92.49.160

144[.]168.63.17

144[.]202.13.108

144[.]202.56.193

144[.]217.207.19

144[.]217.207.21

144[.]217.207.31

144[.]34.144.21

144[.]34.175.58

144[.]34.194.159

144[.]34.198.241

144[.]48.10.16

145[.]249.106.56

145[.]249.107.135

149[.]129.48.48

149[.]129.68.79

149[.]129.72.37

149[.]129.92.203

149[.]248.37.167

149[.]28.117.151

149[.]28.147.25

149[.]28.148.224

149[.]28.28.87

149[.]28.88.208

149[.]6.167.60

150[.]109.103.16

150[.]109.111.208

150[.]109.125.111

152[.]136.114.253

154[.]209.69.6

154[.]210.12.80

154[.]220.3.125

154[.]220.3.196

154[.]220.3.226

154[.]223.142.56

154[.]223.149.97

154[.]223.160.112

154[.]8.160.196

154[.]92.14.41

155[.]138.138.215

155[.]138.164.216

155[.]94.143.110

155[.]94.174.114

156[.]232.254.19

156[.]232.254.6

156[.]234.168.104

156[.]236.118.226

156[.]239.157.66

156[.]245.17.6

156[.]253.11.144

156[.]255.2.36

156[.]96.59.27

157[.]245.169.236

157[.]52.168.140

158[.]101.144.105

161[.]129.39.103

161[.]129.65.118

161[.]35.114.210

161[.]35.38.97

162[.]254.204.222

163[.]172.39.102

167[.]172.45.244

167[.]179.72.102

167[.]179.75.10

167[.]179.78.159

167[.]179.89.117

167[.]71.60.61

170[.]130.55.21

170[.]130.55.22

172[.]105.57.166

172[.]241.27.141

172[.]241.27.174

172[.]241.27.192

172[.]241.27.204

172[.]241.27.34

172[.]241.27.44

172[.]241.27.66

172[.]241.29.153

172[.]241.29.155

172[.]241.29.156

172[.]247.123.118

172[.]81.239.64

172[.]81.254.151

172[.]86.75.123

173[.]208.133.38

173[.]232.146.232

173[.]232.146.32

173[.]232.146.37

173[.]82.236.130

173[.]82.26.59

175[.]24.133.73

175[.]24.46.93

175[.]24.48.117

175[.]24.62.158

175[.]24.75.220

175[.]99.82.225

176[.]119.29.43

176[.]119.29.71

176[.]121.14.183

176[.]121.14.199

176[.]121.14.208

176[.]121.14.237

176[.]223.165.110

176[.]31.193.24

176[.]9.193.5

178[.]17.171.58

179[.]43.176.202

180[.]215.228.28

180[.]215.228.34

180[.]215.228.36

180[.]215.228.38

180[.]76.60.140

180[.]97.215.181

182[.]16.4.114

182[.]16.4.115

182[.]16.4.116

182[.]16.4.117

182[.]16.4.118

182[.]254.173.239

182[.]254.202.89

182[.]92.115.109

182[.]92.120.156

182[.]92.233.56

182[.]92.4.23

182[.]92.65.134

182[.]92.66.81

182[.]92.86.170

185[.]118.164.229

185[.]14.30.139

185[.]147.14.248

185[.]153.196.207

185[.]153.196.209

185[.]153.196.212

185[.]153.196.215

185[.]153.196.216

185[.]153.198.27

185[.]153.198.31

185[.]153.198.40

185[.]153.198.45

185[.]153.198.54

185[.]158.114.53

185[.]161.208.201

185[.]162.235.111

185[.]162.235.178

185[.]162.235.233

185[.]162.235.35

185[.]162.235.76

185[.]162.235.91

185[.]174.103.157

185[.]177.59.70

185[.]180.198.61

185[.]202.0.111

185[.]202.2.182

185[.]207.152.86

185[.]207.154.21

185[.]213.26.197

185[.]227.82.66

185[.]23.200.165

185[.]232.52.137

185[.]234.52.45

185[.]243.113.141

185[.]243.113.192

185[.]243.242.116

185[.]243.41.224

185[.]33.84.190

185[.]33.86.54

185[.]45.193.7

185[.]70.184.44

185[.]80.220.171

188[.]116.36.76

188[.]65.74.60

192[.]169.6.180

192[.]169.6.42

192[.]169.7.160

192[.]169.7.223

192[.]184.90.209

192[.]236.155.238

192[.]236.161.221

192[.]236.161.222

192[.]236.232.228

192[.]34.109.12

192[.]52.167.102

192[.]69.91.119

193[.]112.10.125

193[.]112.124.26

193[.]168.147.249

193[.]187.119.133

193[.]27.14.215

193[.]29.13.168

193[.]32.161.135

193[.]32.163.21

194[.]36.188.188

194[.]36.191.118

195[.]123.213.235

195[.]123.214.182

195[.]123.217.36

195[.]54.160.115

195[.]54.167.235

195[.]54.167.237

195[.]88.209.87

198[.]13.55.13

198[.]44.250.175

198[.]46.198.130

199[.]189.108.68

199[.]192.17.125

199[.]192.17.18

199[.]233.237.115

202[.]182.105.129

202[.]182.119.224

202[.]61.87.136

203[.]195.158.21

203[.]195.199.146

204[.]16.247.89

204[.]44.83.217

207[.]148.124.20

207[.]148.127.216

207[.]148.65.247

207[.]219.199.120

207[.]46.130.130

208[.]51.62.26

208[.]51.62.27

208[.]51.62.28

208[.]51.62.29

208[.]51.62.30

209[.]126.119.186

210[.]16.120.248

211[.]159.201.49

211[.]49.225.208

212[.]129.150.253

212[.]64.44.176

213[.]217.0.216

216[.]126.231.24

216[.]24.188.130

216[.]240.134.70

216[.]250.111.90

217[.]12.202.89

217[.]12.208.162

217[.]12.208.227

217[.]12.208.251

217[.]12.218.99

218[.]253.251.100

218[.]253.251.74

219[.]146.156.17

221[.]181.173.48

221[.]237.189.200

222[.]186.39.123

223[.]68.10.24

参考：

https://www.cnblogs.com/websecyw/p/12058948.html

https://bbs.pediy.com/thread-249837.htm

https://research.nccgroup.com/2020/06/15/striking-back-at-retired-cobalt-strike-a-look-at-a-legacy-vulnerability/

https://www.nccgroup.com/us/about-us/newsroom-and-events/blog/2019/february/identifying-cobalt-strike-team-servers-in-the-wild/

https://www.cobaltstrike.com/help-malleable-c2

https://github.com/salesforce/ja3

https://xz.aliyun.com/t/3889

https://engineering.salesforce.com/tls-fingerprinting-with-ja3-and-ja3s-247362855967