Improving network-based detection of in-the-wild Cobalt Strike C2 servers while reducing the risk of

In my own experience investigating large-scale incidents, I encountered Cobalt Strike in 20 of 25 big-game ransomware cases over the past 12 months, as well as in one APT campaign. This echoes findings from other researchers, such as Cisco Talos, which noted:

> *"Interestingly, 66 percent of all ransomware attacks this quarter involved red-teaming framework Cobalt Strike, suggesting that ransomware actors are increasingly relying on the tool as they abandon commodity trojans."*

Like many powerful tools, Cobalt Strike is frequently cracked and offered on

attackers. Its official video course is even available for free, further broadening its reach.

Given the widespread adoption of Cobalt Strike in cyberattacks, incident responders have developed specific workflows to analyze its beacons — whether on disk, in memory, or via network traffic. However, recent updates to the platform have introduced features that enable fileless execution, making detection more difficult. This poses a significant challenge to digital forensics and incident response (DFIR) teams, especially when dealing with incomplete data, missing event logs, or inconsistent network records.

the widespread 07…b1 JARM fingerprint, other fingerprints should not be disregarded:

- **07d14d16d21d21d07c07d14d07d21d9b2f5869a6985368a9dec764186a9175**
- **2ad2ad16d2ad2ad22c42d42d00042d58c7162162b6a603d3d90a2b76865b53**
- **07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1**

Using Shodan, I reduced the potential threat surface to several tens of thousands of IP addresses for each fingerprint. Despite this, the actual

2ad2ad16d2ad2ad22c42d42d00042d58c7162162b6a603d3d90a2b76865b53 (6,919 IPs)

fingerprints rely on TLS certificates, different implementations using the same certificate can yield different JARM results. Thus, searching for C2 servers based on serial numbers can complement JARM fingerprinting.

On May 3, 2021, I found 914 potential C2 servers using Shodan, based on this certificate serial number. Interestingly, there was less than 50% overlap between the JARM-identified servers and those identified through certificate serial numbers, demonstrating the value of combining detection methods.

Cobalt Strike C2 servers threat surface based on certificate serial number

```
Nmap scan report for 193.29.13.201
Host is up (0.014s latency).
PORT    STATE SERVICE
80/tcp  open  http
| cobalt:
| x86 URI Response:
| BeaconType: 0 (HTTP)
| Port: 80
| Polling: 60000
```

```
| Proxy_AccessType: 2 (Use IE settings)
443/tcp open  https
| cobalt:
| x86 URI Response:
| BeaconType: 8 (HTTPS)
| Port: 443
| Polling: 60000
| Jitter: 0
| C2 Server: 193.29.13.201,/g.pixel
| HTTP Method Path 2: /submit.php
```

This script allows organizations to scale their Cobalt Strike detection across thousands of IP addresses. While scanning the entire internet for Cobalt Strike C2 servers would be excessive for most organizations, focusing on a well-defined threat surface is far more manageable.

On May 3, 2021, by scanning the servers identified using JARM fingerprints and certificate serial numbers, I confirmed the presence of 474 active C2 servers.

Appendix A — Cobalt Strike C2 Servers List (3rd May 2021)

```
1.14.132.218,/kj.js
1.14.132.218,/ur.js
1.15.139.40,/activity
1.15.139.40,/push
1.15.139.40,/visit.js
1.15.175.22,/j.ad
1.15.230.57,/load
1.15.230.57,/match
10.10.16.2,/ga.js
10.248.1.135,/ga.js
100.24.56.227,/bing
```

```
109.201.142.17,/IE9CompatViewList.xml
109.201.142.17,/updates.rss
109.236.84.121,/IE9CompatViewList.xml
109.236.84.121,/load
109.236.84.121,/updates.rss
113.31.118.7,/g.pixel
113.31.118.7,/match
113.31.118.7,/pixel
113.31.118.7,/push
114.117.208.80,/geo/collect/v1
114.55.173.68,/g.pixel
114.55.173.68,/IE9CompatViewList.xml
115.159.143.241,/en_US/all.js
115.159.143.241,/ga.js
116.62.115.46,/dot.gif
116.62.115.46,/ptj
```

```
139.162.221.161,/jquery-3.3.1.min.js,192.46.221.58,/jquery-
3.3.1.min.js

139.196.153.6,/ptj
139.196.153.6,/updates.rss
139.60.161.99,/activity
139.60.161.99,/cx
139.60.161.99,/en_US/all.js
14.192.48.91,/dpixel
14.192.48.91,/ptj
144.34.187.147,/wp08/wp-includes/dtcla.php
145.249.106.104,/cm
145.249.106.104,/dpixel
145.249.106.104,/visit.js
145.249.107.35,/__utm.gif
145.249.107.35,/en_US/all.js
145.249.107.35,/IE9CompatViewList.xml
```

```
175.24.138.70,/dot.gif
176.105.252.144,/fwlink
176.111.174.66,/dot.gif
176.111.174.66,/updates.rss
176.121.14.113,/activity
176.121.14.113,/ca
176.121.14.113,/j.ad
18.163.120.26,/__utm.gif
18.163.120.26,/match
185.106.123.101,/fwlink
185.14.29.42,/jquery-3.3.1.min.js
185.153.199.164,/pixel
185.153.199.164,/visit.js
185.158.248.106,/activity
185.158.248.106,/en_US/all.js
185.158.248.106,/ga.js
```

```
202.182.101.162,/match
207.148.107.212,/load
207.148.65.247,/ptj
209.141.37.21,/ca
209.141.37.21,/dot.gif
209.141.37.21,/updates.rss
212.95.157.61,/push
212.95.157.61,/updates.rss
213.135.78.244,/hr.css
213.202.211.246,/metro91/admin/1/ppptp.jpg
213.217.0.216,/pixel
213.217.0.216,/push
213.217.0.216,/updates.rss
213.217.0.217,/__utm.gif
213.217.0.217,/cx
213.217.0.217,/match
```

```
39.97.216.224,/IE9CompatViewList.xml
42.192.119.64,/load
42.193.127.38,/owa/
42.193.220.214,/updates.rss
42.194.133.101,/en_US/all.js
42.194.133.101,/visit.js
45.137.10.148,/dpixel
45.138.209.73,/fwlink
45.144.3.120,/ca
45.145.36.210,/ga.js
45.146.164.199,/__utm.gif
45.146.164.199,/dpixel
45.146.165.143,/complete/search
45.199.160.117,/ca

45.32.136.204,/jquery-
```

```
47.56.219.26,/j.ad
47.57.125.197,/__utm.gif
47.57.125.197,/activity
47.57.125.197,/pixel
47.57.125.197,/ptj
47.90.202.152,/updates.rss
47.94.20.209,/admin
47.98.99.15,/visit.js
47.99.178.84,/cx
47.99.178.84,/ga.js
49.234.184.176,/en_US/all.js
49.234.184.176,/fwlink
49.234.93.169,/cx
49.234.93.169,/dpixel

49.235.217.243,/pixel,https://m1xg.tk,/pixel,https://m1xg.cf,/acti
vity
```

```
69.49.229.88,/ga.js
74.121.148.47,/image/
78.128.112.134,/match
78.128.112.215,/g.pixel
79.110.52.172,/activity
8.136.228.12,/groupcp
8.140.105.214,/ca
8.140.105.214,/cx
8.210.161.205,/ca
8.210.161.205,/IE9CompatViewList.xml
81.69.10.55,/g.pixel
81.70.155.208,/fwlink
85.208.110.108,/cm
88.198.165.127,/nd
94.103.94.203,/match
94.103.94.203,/visit.js
```

```
bigbrotheriswatchingyou.herokuapp.com,/IE9CompatViewList.xml
bigbrotheriswatchingyou.herokuapp.com,/pixel
bookcasegreeting632.roman-indigo.com,/viewerng/meta
braunballon.com,/jquery-3.3.1.min.js
buy9182.com,/RELEASES.js

cdn.lbwd.net,/s/ref=nb_sb_noss_1/596-20814129-5816322/field-
keywords=time

cdn.sogou-update.com,/copyright.css
cdn.sogou-update.com,/template.css
cdn.usbankcreditcards.com,/oscp/
charityhouseofbrooklin.com,/mobile-android

chmowd.xyz,/MicrosoftUpdate/ShellEx/KB242742/default.aspx,powssxct
aiwan.xyz,/MicrosoftUpdate/ShellEx/KB242742/default.aspx
```

```
fish.hellomrsone.com,/jquery-3.3.1.min.js
forteupdate.com,/activity
forteupdate.com,/IE9CompatViewList.xml
forteupdate.com,/match
fubukipr.xyz,/rs
fut1.net,/userid=
gonzofabriq.com,/jquery-3.3.1.min.js
grayballon.com,/jquery-3.3.1.min.js
greattxmsng-imgx.com,/ak.js
hars2t.com,/userid=
helle1.net,/userid=

help01.softether.net,/users/sign_in,work.cloud01.tk,/users/sign_in
,work.cloud20.tk,/users/sign_in,185.118.166.205,/users/sign_in
idxup.com,/us/ky/louisville/312-s-fourth-
st.html,dbhigh.com,/us/ky/louisville/312-s-fourth-st.html
```

```
pepesec2.azureedge.net,/s/ref=nb_sb_noss_1/089-89185991-
7448134/field-keywords=eye

pnwcontent-delivery.com,/pixel
pnwcontent-delivery.com,/updates.rss
presidentofschool14.com,/ab
private.medicaloptionsfinance.com,/real-world-investing/

qw.hashsystem.xyz,/RELEASE,as.hashsystem.xyz,/RELEASE,xz.hashsyste
m.xyz,/RELEASE

rabbitumed.com,/metro91/admin/1/ppptp.jpg
register.hr-tencent.com,/view/
repdot.com,/us/ky/louisville/312-s-fourth-st.html
resnote.com,/us/ky/louisville/312-s-fourth-
st.html,172.82.148.202,/us/ky/louisville/312-s-fourth-st.html
```

```
support.cloudways.com,/ocsp/a/

synergiedental.com,/safebrowsing/rd/CltOb12nLW1IbHehcmUtd2hUdmFzEBAY7-0KIOkUDC7h2

syscx.com,/dot.gif
syscx.com,/dpixel
tailgatethenation.com,/find.html

telemetry.wessonlabpartners.com,/jquery-3.3.1.min.js,admitting.healthfitconnection.com,/jquery-3.3.1.min.js,skilled_nursing.healthmanagementtoday.com,/jquery-3.3.1.min.js

tess2.net,/userid=
test.axibala.club,/cm
test.axibala.club,/g.pixel
```

```
www.unwomen.org,/jquery-3.3.1.min.js,www.prodibi.com,/jquery-3.3.1.min.js,www.oriental-residence.com,/jquery-3.3.1.min.js

www.weixim.ga,/__utm.gif
x-w-x.herokuapp.com,/jquery-3.3.1.min.js
zipflag.com,/us/ky/louisville/312-s-fourth-st.html
```

Incident Response | Forensics | Cybersecurity | Threat Intelligence | Hacking