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

By Sergiu Sechel, PhD

Published: 2024-10-02 · Archived: 2026-04-05 14:05:39 UTC

Press enter or click to view image in full size

Photo by Robynne Hu on Unsplash

Context

Cobalt Strike is a commercial post-exploitation platform designed for Windows-based environments. Its beacon (implant) can be delivered to a target in various ways, even without exploiting technical vulnerabilities (e.g., through malicious email attachments). The platform's functionality can be extended through plug-ins, and over the years, it has gained notoriety among both offensive security teams (red teamers) and cybercriminals. Since 2019, Cobalt Strike has been used in multiple high-profile ransomware attacks, advanced persistent threat (APT) campaigns, and espionage activities.

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 underground forums shortly after new versions are released. This accessibility has contributed to its growing use in cyberattacks.

Cracked Cobalt Strike 4.2 offered on an underground forum

Cobalt Strike detection methods

The industry is full of good tools, so what’s the fuss about Cobalt Strike?

Cobalt Strike’s appeal lies in its balance between advanced functionality and ease of use, making it attractive to both seasoned professionals and novice 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.

In some investigations, I’ve had to parse millions of network events and thousands of IP addresses in search of Cobalt Strike C2 servers because all other endpoint artifacts were unavailable. In this article, I’ll outline some network-based techniques for detecting Cobalt Strike C2 servers that blue teams, incident responders, and threat intelligence analysts can use for both active defense and proactive threat hunting.

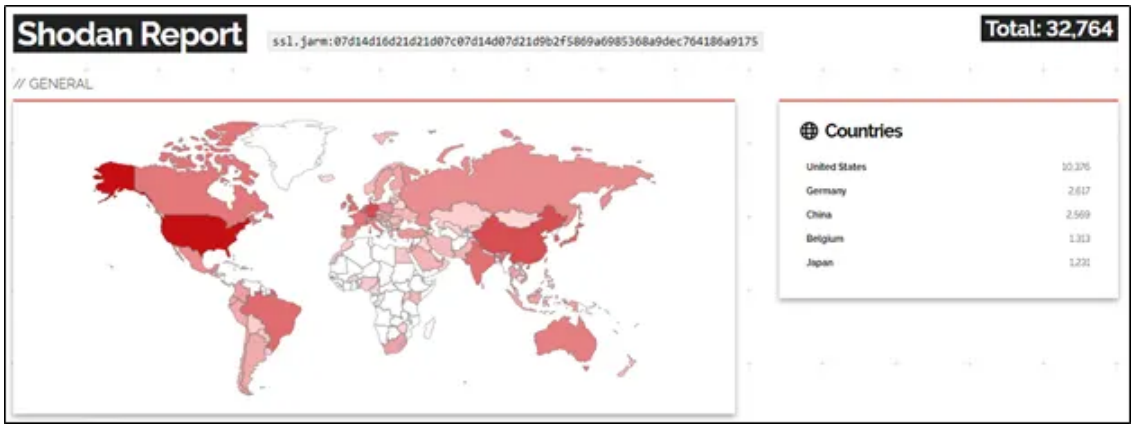
Cobalt Strike threat surface detection using JARM fingerprints

JARM fingerprints, developed by Salesforce Engineering, are an effective way to detect malicious C2 servers. They can help reduce the threat surface from billions of IP addresses to a more manageable subset before analyzing each C2 server individually.

In April 2021, I identified three distinct Cobalt Strike JARM fingerprints in C2 servers deployed globally. While much of the current research focuses on the widespread 07…b1 JARM fingerprint, other fingerprints should not be disregarded:

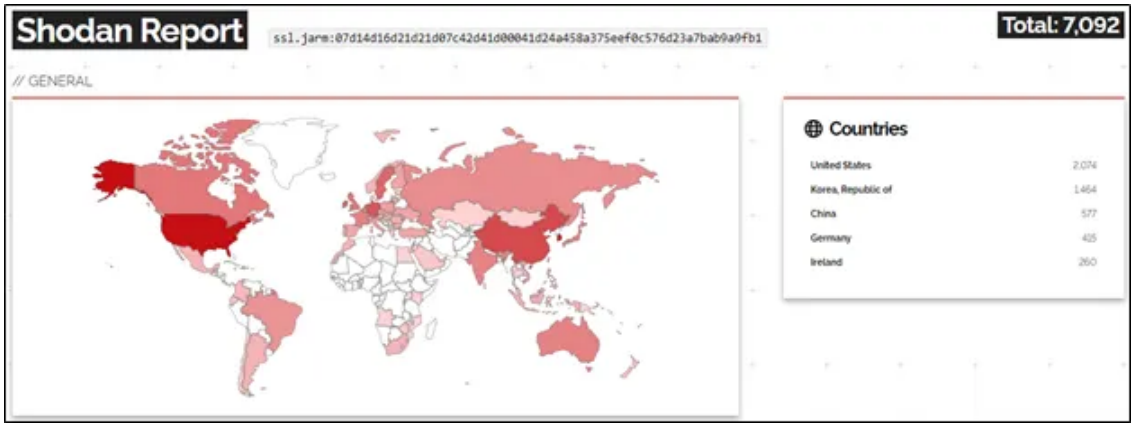
- **07d14d16d21d21d07c07d14d07d21d9b2f5869a6985368a9dec764186a9175**
- **2ad2ad16d2ad2ad22c42d42d00042d58c7162162b6a603d3d90a2b76865b53**
- **07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1**

Using Shodan, I reduced the potential threat surface to several tens of thousands of IP addresses for each fingerprint. Despite this, the actual number of active C2 servers I identified on May 3, 2021, was much smaller — only 474 servers.



07d14d16d21d21d07c07d14d07d21d9b2f5869a6985368a9dec764186a9175 (32,764 IPs)

2ad2ad16d2ad2ad22c42d42d00042d58c7162162b6a603d3d90a2b76865b53 (6,919 IPs)



07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1 (7,092 IPs)

The threat surface, based solely on the JARM fingerprints is large compared to the actual number of C2s I found active on 03 May 3, 2021. (474 active C2 servers)

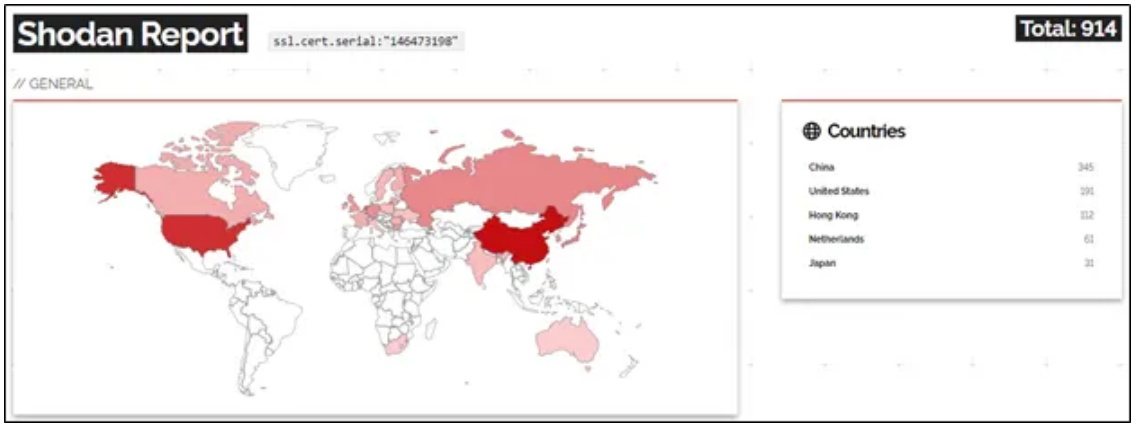
Cobalt Strike Detection Using Certificate Serial Numbers

Another method I've found effective involves identifying C2 servers by their certificate serial numbers. Many Cobalt Strike C2 servers in the wild use a generic certificate with the serial number **146473198**. While JARM 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.

```
Version: 3 (0x2)Serial Number: 146473198 (0x8bb00ee)Fingerprint Algorithm: sha256WithRSAEncryptionIs
```

On 3rd May 2021 I found 914 potential C2 servers, based on Shodan results.



Cobalt Strike C2 servers threat surface based on certificate serial number

Again, the threat surface is large compared to the actual number of C2s I found active 03 May 3, 2021 but to point out on interesting fact, there was less than 50% overlap between the JARM fingerprints population and the certificate-based detection.

Threat Surface Reduction by Payload Retrieval

While JARM and certificate-based detection methods provide a strong starting point, retrieving payloads from potential C2 servers further refines the threat surface. By actively interacting with Cobalt Strike C2 servers, it's possible to extract beacon configurations and confirm C2 activity.

I used the Nmap implementation of the payload retrieval technique (grab_beacon_config script) created by GitHub user "whickey-r7" to automate this process. This method efficiently retrieves beacon configurations from Cobalt Strike C2 servers, providing critical information such as the beacon type, polling intervals, and C2 server addresses.

Here's an example of a successful Nmap scan result:

```
Nmap scan report for 193.29.13.201Host is up (0.014s latency).PORT    STATE SERVICE80/tcp  open  htt
```

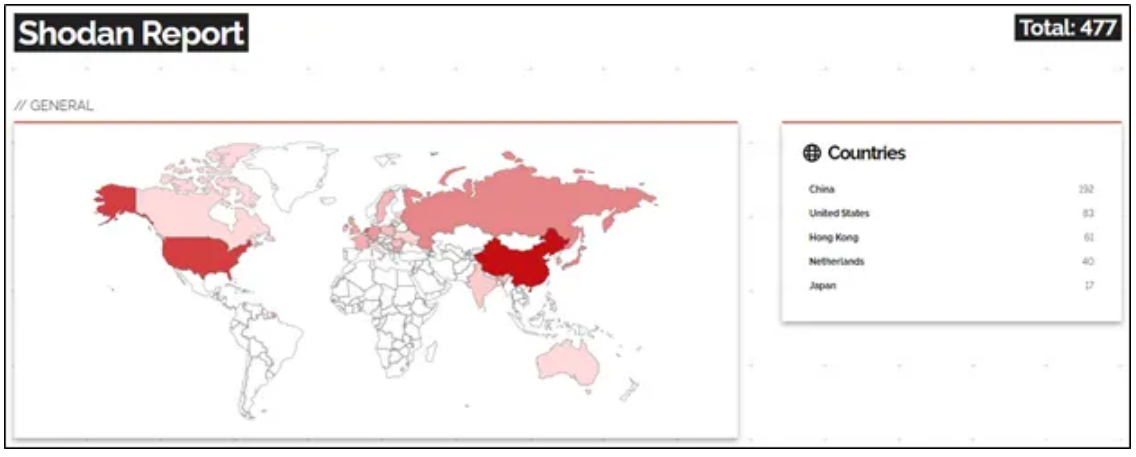
This script allows organizations to scale their Cobalt Strike detection across thousands of IP addresses. While scanning the entire internet for Cobalt Strike C2 servers would be excessive for most organizations, focusing on a well-defined threat surface is far more manageable.

Get Sergiu Sechel, PhD's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

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.



Conclusions

The network-based detection techniques discussed here provide a cost-effective method for defending networks against threat actors leveraging Cobalt Strike, particularly in big-game ransomware campaigns. While no single detection method is foolproof, combining JARM fingerprinting, certificate serial number analysis, and payload

retrieval significantly enhances detection accuracy. As threat actors continue to modify their use of Cobalt Strike, defenders must also evolve their detection and mitigation strategies to stay ahead of these evolving threats.

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
101.132.149.198,/match
101.132.251.212,/en_US/all.js101.28.128.125,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=b
103.234.54.146,/ptj
103.234.54.146,/push
103.234.72.248,/pixel
103.234.72.248,/ptj
103.234.72.64,/updates
103.242.133.19,/dpixel
103.73.97.119,/updates
103.79.79.16,/jquery-3.3.1.min.js
104.243.46.74,/__utm.gif
104.243.46.74,/ca
104.243.46.74,/push
104.248.148.74,/cx
104.248.148.74,/en_US/all.js
104.36.231.42,/cx
104.36.231.42,/j.ad
106.15.197.67,/jquery-3.3.1.min.js
106.52.152.85,/IE9CompatViewList.xml
106.52.152.85,/push
106.52.181.247,/match
106.55.153.204,/en_US/all.js
108.166.207.133,/cm
108.166.207.133,/pixel
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
117.78.1.204,/jquery-3.3.1.min.js
119.29.189.237,/cx
119.29.189.237,/load
119.3.141.162,/jquery-3.3.1.min.js
120.48.22.178,/j.ad
120.79.29.153,/cm
120.92.139.155,/en_US/all.js
120.92.139.155,/j.ad
120.92.139.155,/match
120.92.139.155,/ptj
121.196.153.136,/ca
121.196.63.110,/cx
121.5.103.116,/visit.js
121.5.162.169,/ga.js
123.57.73.247,/updates
124.156.148.167,/pixel.gif
13.51.149.17,/cm
13.51.149.17,/cx
13.51.149.17,/match
134.122.134.87,/activity
134.209.5.246,/j.ad
134.209.5.246,/visit.js134.209.92.85,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books139
139.155.27.71,/dpixel
139.155.27.71,/en_US/all.js
139.155.42.254,/ga.js
139.155.42.254,/ptj139.162.221.161,/jquery-3.3.1.min.js,192.46.221.58,/jquery-3.3.1.min.js139.196.15
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
149.248.1.200,/updates.rss
149.28.20.245,/search/
149.28.233.123,/__utm.gif
149.28.233.123,/ca
149.28.233.123,/visit.js
151.236.14.53,/en_US/all.js
151.236.14.53,/load
154.220.3.226,/preload
154.91.164.69,/cm
154.91.164.69,/dpixel
155.138.215.103,/ca
156.236.114.72,/dpixel
156.236.114.72,/ptj
156.255.2.36,/pixel.gif
156.255.3.224,/visit.js
159.75.136.108,/g.pixel
160.124.103.152,/updates.rss
163.172.39.102,/index.jsp
164.138.25.191,/resolve/alter/,46.19.37.133,/resolve/alter/
167.179.79.212,/jquery-3.3.1.min.js
172.241.27.70,/bg.css
172.67.129.206,/bfs/static/jinkela/long/sentry/sentry-5.7.1.vue.min.js
172.81.205.217,/IE9CompatViewList.xml
172.82.148.202,/us/ky/louisville/312-s-fourth-st.html172.98.192.91,/s/ref=nb_sb_noss_1/167-3294888-0
172.98.192.94,/g.pixel
173.82.197.229,/fwlink
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
185.158.249.38,/dpixel
185.158.249.38,/ga.js
185.158.249.38,/pixel
```

```
185.158.249.38,/pixel.gif
185.162.235.35,/fwlink
185.162.235.35,/pixel.gif
185.162.235.35,/push185.20.186.108,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books185.2
185.232.52.137,/dpixel
185.232.52.137,/IE9CompatViewList.xml
185.232.52.137,/load
185.25.51.172,/mobile-android
185.25.51.55,/copyright.js
185.82.202.123,/j.ad
188.119.113.24,/__utm.gif
192.168.100.103,/fam_newspaper.html
193.112.10.125,/en_US/all.js
193.29.13.201,/__utm.gif
193.29.13.201,/g.pixel
193.29.13.201,/j.ad
193.29.13.209,/pixel
193.29.13.209,/updates.rss
194.15.216.20,/dot.gif
194.165.16.60,/cx
194.165.16.60,/fwlink
194.165.16.60,/push
195.123.217.45,/jquery-3.3.1.min.js
195.123.222.12,/jquery-3.3.1.min.js
195.123.222.5,/jquery-3.3.1.min.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
213.217.0.217,/pixel.gif
213.217.0.218,/ca
213.217.0.218,/IE9CompatViewList.xml
213.252.244.213,/fam_cart
213.252.245.19,/ab
217.12.201.100,/jquery-3.3.1.min.js
```

```
217.12.218.46,/jquery-3.3.1.min.js
218.253.251.115,/ga.js
218.253.251.115,/IE9CompatViewList.xml
23.106.223.79,/activity23.163.0.12,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books3.137
31.44.184.232,/__utm.gif
31.44.184.232,/pixel
31.44.184.73,/dot.gif
31.44.184.73,/en_US/all.js
31.44.184.73,/IE9CompatViewList.xml
31.44.184.73,/updates.rss
31.44.3.198,/ptj
34.92.237.17,/dot.gif
34.96.156.66,/pixel.gif
35.200.6.25,/ur.js
35.221.239.215,/jquery-3.3.1.min.js
35.224.197.52,/__utm.gif
35.224.197.52,/ga.js
35.224.197.52,/pixel.gif
35.236.132.18,/load
35.236.132.18,/updates.rss
37.252.120.101,/resolve/alter/
37.61.205.212,/updates
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,/ca45.32.136.204,/jquery-3.3.1.min.js,axiommortgagebankers.com,/jquery-3.3.1.min.js45
45.32.92.183,/j.ad
45.33.27.73,/cx
45.33.27.73,/dpixel
45.33.27.73,/en_US/all.js
45.33.27.73,/push
45.76.202.78,/IE9CompatViewList.xml
45.76.202.78,/j.ad
45.77.249.181,/updates.rss
45.92.156.97,/__utm.gif
45.92.156.97,/updates.rss
45.93.201.114,/en_US/all.js
```

```
45.93.201.114,/pixel.gif
46.101.98.38,/sxn/start
47.103.102.194,/pixel
47.103.158.65,/cm
47.104.143.234,/__utm.gif
47.104.156.242,/v1/act
47.104.253.89,/cx
47.104.253.89,/push
47.108.16.11,/2016-08-15/proxy/Test/main/index
47.108.246.116,/pixel
47.110.147.243,/ca47.111.163.10,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books47.114.3
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,/dpixel49.235.217.243,/pixel,https://m1xg.tk,/pixel,https://m1xg.cf,/activity49.235.92
49.235.92.191,/cm
5.181.156.46,/j.ad
5.189.184.60,/RELEASE.html
5.2.70.173,/__utm.gif
5.2.70.173,/fwlink
5.2.70.173,/visit.js
5.252.179.195,/match
5.34.178.43,/posting.js
5.34.182.210,/updates.rss5.39.221.60,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books51.
51.83.79.151,/load52.211.36.208,/s/ref=nb_sb_noss_1/089-89185991-7448134/field-keywords=eye52.229.22
61.168.100.179,/api/getit
62.171.142.145,/api/getit
66.42.56.42,/jquery-3.3.1.min.js
69.49.229.88,/ca
69.49.229.88,/dot.gif
69.49.229.88,/dpixel
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
95.179.239.225,/dot.gif
95.179.239.225,/IE9CompatViewList.xml
98.142.143.100,/access/
a.officecalendar.biz,/owa/
accounts.bankpaygateway.com,/jquery-1.12.1.min.js
aphina-sec.com,/j.ad
aphina-sec.com,/push
api.onedriev.tk,/jquery-3.3.1.min.jsasismdnu.asisdns.space,/s/ref=nb_sb_noss_1/167-3294888-0262949/f
avetool.com,/us/ky/louisville/312-s-fourth-st.html
azama12.com,/jquery-3.3.1.min.jsbanweb.cityu.dev,/core/wp-includes/pol.php,cc12234.cityu.dev,/center
banweb.cityu.dev,/include/template/ClassSvc.php,cc12234.cityu.dev,/include/template/ClassSvc.php,lb2
best73.com,/SocContent/webfont.css,www.shopex.cn,/SocContent/webfont.cssbigbrotheriswatchingyou.hero
bigbrotheriswatchingyou.herokuapp.com,/pixel
bookcasegreeting632.roman-indigo.com,/viewerng/meta
braunballon.com,/jquery-3.3.1.min.js
buy9182.com,/RELEASES.jscdn.lbwd.net,/s/ref=nb_sb_noss_1/596-20814129-5816322/field-keywords=timecdn
cdn.sogou-update.com,/template.css
cdn.usbankcreditcards.com,/oscp/
charityhouseofbrooklin.com,/mobile-androidchmowd.xyz,/MicrosoftUpdate/ShellEx/KB242742/default.aspx,
cloudflare.com,/r_config
clubuz.com,/us/ky/louisville/312-s-fourth-st.html
control.commanderinthe.cloud,/search/
cuphq.com,/pixel.gif,104.243.41.123,/cm
cuphq.com,/visit.js,104.243.41.123,/fwlink
cymkpuadkduz.xyz,/latest/pip-check
d3kgm44zuz83i3.cloudfront.net,/access/
DailyHealthGuide.org,/jquery-3.3.1.min.js
dain22.net,/userid=
dataoss.microsoft.com.w.kunluncan.com,/jquery-3.3.1.min.js
dataprotocol.site,/config
dataprotocol.site,/login
docrule.com,/en.css,prepcar.com,/sq.css
docrule.com,/link.css,prepcar.com,/sq.css
domways.com,/us/ky/louisville/312-s-fourth-st.html
drellio.com,/userid=ec2-54-82-176-65.compute-1.amazonaws.com,/s/ref=nb_sb_noss_1/167-3294888-0262949
exrap.com,/us/ky/louisville/312-s-fourth-st.html
fastpic-domain.com,/logo.js,185.25.51.67,/na.js
fastpic-domain.com,/na.js,185.25.51.67,/logo.js
```

```
fastpighostmerch.com,/html
fedex-global.com,/MicrosoftUpdate/ShellEx/KB242742/default.aspx
feusa.net,/userid=findcola.com,/us/ky/louisville/312-s-fourth-st.html,64.187.239.74,/us/ky/louisvill
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.t
idxup.com,/us/ky/louisville/312-s-fourth-st.html,dbhigh.com,/us/ky/louisville/312-s-fourth-st.htmlim
isaacrevia.com,/bg
jquery.thinkphp.me,/jquery-3.3.1.min.js
js.news1010.net,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books
kasaa.net,/userid=
keit1on.net,/userid=
lagrom.com,/send.html
lhweb.xyz,/Sample/DownloadFile
liojikd.com,/posting.js
liojikd.com,/RELEASE.js
luoli233.top,/dot.gif
luoli233.top,/IE9CompatViewList.xml
luoli233.top,/ptj
maren2.com,/userid=
massflip.com,/us/ky/louisville/312-s-fourth-st.html,mixalt.com,/us/ky/louisville/312-s-fourth-st.htm
mgfee.com,/fo.html
microsoftchina.org,/dot.gif
mingrand.com,/jquery-3.3.1.min.js
oaelf.com,/us/ky/louisville/312-s-fourth-st.html,sslfeed.com,/us/ky/louisville/312-s-fourth-st.htmlp
pnwcontent-delivery.com,/updates.rss
presidentofschool14.com,/ab
private.medicaloptionsfinance.com,/real-world-investing/qw.hashsystem.xyz,/RELEASE,as.hashsystem.xyz
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.
safeconnections.xyz,/__utm.gif
safeconnections.xyz,/__utm.gif,176.123.8.228,/__utm.gif
sbgprodib.oberto.za.net,/__utm.gif
scalewa.com,/sm.html
service.office247.tech,/match
service-0dibtqsv-1255352921.cd.apigw.tencentcs.com,/api/getit
service-4f1dmvy9-1252742900.sh.apigw.tencentcs.com,/api/getit
service-6eqxujkd-1255352921.cd.apigw.tencentcs.com,/api/getit
service-dr6r4kg0-1304343953.gz.apigw.tencentcs.com,/api/getid
```

```
service-j024ikqq-1259268926.gz.apigw.tencentcs.com,/api/getit
service-muqfpxbh-1304245224.cd.apigw.tencentcs.com,/api/getit
service-p44yb571-1300400844.cd.apigw.tencentcs.com,/script/VUE/src/main.js
service-pfzr9eww-1304703456.hk.apigw.tencentcs.com,/api/getit
services.rogerscorp.cloud,/jquery-3.3.1.min.js
shimatos.com,/jquery-3.3.1.min.jsshop.redlist.cyou,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-key
sitehealthcheck.org,/oscp/
ssl363648.cloudflaressl.com,/cmstatic.azureimgages.com,/s/ref=nb_sb_noss_1/167-3294888-0262949/field
syscx.com,/dpixel
tailgatethenation.com,/find.htmltelemetry.wessonlabpartners.com,/jquery-3.3.1.min.js,admitting.healt
test.axibala.club,/cm
test.axibala.club,/g.pixel
test.axibala.club,/ga.js
test2.floridasattorneys.com,/blog
tmestoragetest.azureedge.net,/obj_
touchroof.com,/modcp,focuslex.com,/modcp
ts.wii.qq.com,/ping
tulls.net,/userid=
udpdeliveryddp.com,/fam_cart
update.software-update.tk,/upload/google-3
us.netsuite-labs.com,/ocsp/a/us-systemtest.com,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keyword
vianodata.com,/match
vianodata.com,/push
w.668526.com,/default
wellser.org,/userid=
wenku.qq.com.0a492012.c.cdnhwc1.com,/Activate/v1.87/3O3SB5SNQ5
workfromhomeblueprints.azureedge.net,/update/
www.bankrate.com,/index.html,cnn.com,/index.html
www.bloomberg.com,/table/
www.csmu.website,/cx
www.csmu.website,/ga.js
www.cumberlandplasticsurgery.com,/user/profile
www.google-dev.tk,/jquery-3.3.1.min.js
www.hellomrsone.com,/jquery-3.3.1.min.js
www.nfsq.ml,/__utm.gif
www.qiniu.com,/pixel
www.qiniu.com,/s
www.qs-hosting.com,/ocsp/a/www.unwomen.org,/jquery-3.3.1.min.js,www.prodibi.com,/jquery-3.3.1.min.js
x-w-x.herokuapp.com,/jquery-3.3.1.min.js
zipflag.com,/us/ky/louisville/312-s-fourth-st.html
```

Source: https://sergiusechel.medium.com/improving-the-network-based-detection-of-cobalt-strike-c2-servers-in-the-wild-while-reducing-the-6964205f6468