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

Sergiu Sechel · Follow

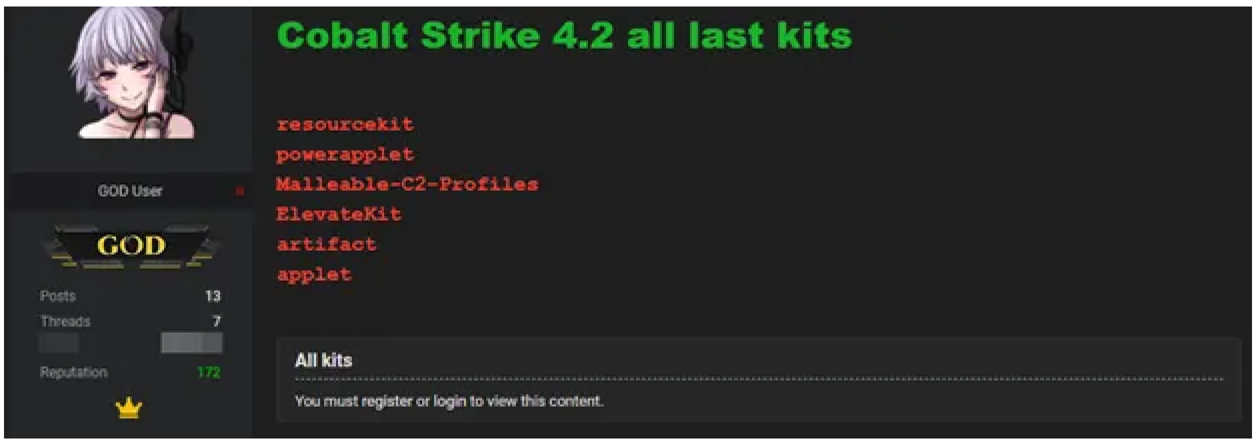
9 min read · May 3, 2021

40

months, as well as in one APT campaign. This echoes findings from other re

> *"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.



Cobalt Strike 4.2 all last kits

```
resourcekit
powerapplet
Malleable-C2-Profiles
ElevateKit
artifact
applet
```

All kits

You must register or login to view this content.

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?

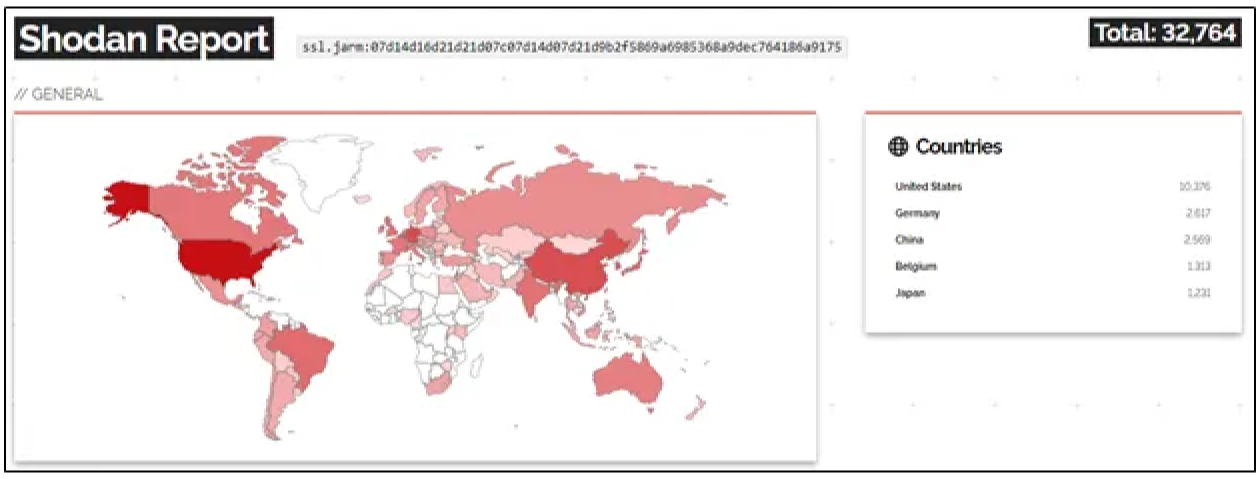
Cobalt Strike's appeal lies in its balance between advanced functionality and ease of use, making it attractive to both seasoned professionals and novice attackers. Its official video course is even available for free, further broadening its reach.

JARM fingerprints, developed by Salesforce Engineering, are an effective wa e fr g 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.



Shodan Report

ssl.jarm:07d14d16d21d21d07c07d14d07d21d9b2f5869a6985368a9dec764186a9175

Total: 32,764

// GENERAL

Countries

United States	10,376
Germany	2,617
China	2,569
Belgium	1,313
Japan	1,231

07d14d16d21d21d07c07d14d07d21d9b2f5869a6985368a9dec764186a9175 (32,764 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)
```

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:

```
| Proxy AccessType: 2 (Use IE settings)
| Port: 80
| Polling: 60000
| Jitter: 0
| C2 Server: 193.29.13.201,/j.ad
| HTTP Method Path 2: /submit.php
| Method1: GET
| Method2: POST
| Spawnto_x86: %windir%\syswow64\rundll32.exe
| Spawnto_x64: %windir%\sysnative\rundll32.exe
| 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
| Method1: GET
| Method2: POST
| Spawnto_x86: %windir%\syswow64\rundll32.exe
| Spawnto_x64: %windir%\sysnative\rundll32.exe
| Proxy_AccessType: 2 (Use IE settings)
| x64 URI Response:
| BeaconType: 8 (HTTPS)
```

On May 3, 2021, by scanning the servers identified using JARM fingerprints an

se

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
```

```
104.248.148.74,/en_US/all.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.js
```

```
151.236.14.53,/en_US/all.js
```

```
154.91.164.65,/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.html

172.98.192.91,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-
keywords=books

172.98.192.94,/__utm.gif
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
```

```
209.141.37.21,/dot.gif
```

```
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,/activity
23.163.0.12,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books
3.137.217.140,/dot.gif
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
```

```
47.104.156.242,/v1/act
```

```
47.108.240.110,/pixel
47.110.147.243,/ca

47.111.163.10,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-
keywords=books

47.114.36.45,/dot.gif

47.115.54.254,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-
keywords=books

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

49.235.92.191,/__utm.gif
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.rss

5.39.221.60,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-
keywords=books

51.83.79.151,/cm
51.83.79.151,/load

52.211.36.208,/s/ref=nb_sb_noss_1/089-89185991-7448134/field-
```

```
95.179.239.225,/IE9CompatViewList.xml
```

```
aphina-sec.com,/j.ad
aphina-sec.com,/push
api.onedriev.tk,/jquery-3.3.1.min.js

asismdnu.asisdns.space,/s/ref=nb_sb_noss_1/167-3294888-
0262949/field-keywords=books

assets.outlook.com,/find.html
avetool.com,/us/ky/louisville/312-s-fourth-st.html
azama12.com,/jquery-3.3.1.min.js

banweb.cityu.dev,/core/wp-
includes/pol.php,cc12234.cityu.dev,/center/gateway/common.php,lb23
311.cityu.dev,/center/gateway/common.php

banweb.cityu.dev,/core/wp-
includes/pol.php,cc12234.cityu.dev,/core/wp-
includes/pol.php,lb23311.cityu.dev,/core/wp-includes/pol.php
banweb.cityu.dev,/include/template/ClassSvc.php,cc12234.cityu.dev,
/include/template/ClassSvc.php,lb23311.cityu.dev,/core/wp-
includes/pol.php

bbs.robomaster.com,/viewerng/meta,tianqi.com,/viewerng/meta,juejin
.cn,/viewerng/meta,btcfans.com,/viewerng/meta,xue338.com,/viewerng
/meta,python2.net,/viewerng/meta,w2bc.com,/viewerng/meta,jiangzi.c
om,/viewerng/meta,mytokencap.com,/viewerng/meta
best73.com,/SocContent/webfont.css,www.shopex.cn,/SocContent/webfo
nt.css

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

client.elisea-mutuelle.fr,/jquery-3.3.1.min.js
```

```
fish.hellomrsone.com,/jquery-3.3.1.min.js
```

```
fubakipr.xyz,/js
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

img.alicdn.com,/contentsvc/microsofticon,at.alicdn.com,/contentsvc
/microsofticon,ald.taobao.com,/contentsvc/microsofticon,www.aliyun
baike.com,/contentsvc/microsofticon

iorgcloud.cf,/visit.js
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.html
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.html

pebrord.com,/homes/for_sale/atlanta/,www.pebrord.com,/homes/for_sa
le/atlanta/

pepesec.azureedge.net,/s/ref=nb_sb_noss_1/647-50007454-
8514032/field-keywords=person
```

```
service-p44yb571-
```

```
shimatos.com,/jquery-3.3.1.min.js

shop.redlist.cyou,/s/ref=nb_sb_noss_1/167-3294888-0262949/field-
keywords=books

shopdsld-invoce.com,/ky.js
sitehealthcheck.org,/oscp/
ssl363648.cloudflaressl.com,/cm

static.azureimgages.com,/s/ref=nb_sb_noss_1/167-3294888-
0262949/field-keywords=books

stereeofficeknot.net,/safebrowsing/rd/nX4Yecwd6qp3a3T7BhgTvJbjFwAw
gUZj0-N3zAu1AP4BE

support.cloudways.com,/ocsp/a/

synergiedental.com,/safebrowsing/rd/CltOb12nLW1IbHehcmUtd2hUdmFzEB
AY7-0KIOkUDC7h2

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
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-
keywords=books,207.148.29.168,/s/ref=nb_sb_noss_1/167-3294888-
0262949/field-keywords=books

vanguard.medicaloptionsfinance.com,/real-world-investing/
vianodata.com,/match
```

Written by Sergiu Sechel

Follow

76 Followers

PhD, CISA, CISM, CRISC, CFE, CEH, CBP, CSSLP, CDPSE, GICSP, GPEN, GWAPT, GCFA, GNFA, GASF, GCTI, GREM, PMP

More from Sergiu Sechel

Sergiu Sechel

Insecure permissions in Glen Dimplex Deutschland GmbH...

About Carel pCOWeb

Mar 1, 2019 5

Sergiu Sechel in The Dark Water Journal

Latin Phisher

Exploring a phishing campaign designed impersonate Banco Santander Brazil's...

Dec 16, 2019

Recommended from Medium

Satyam Pathania in InfoSec Write-ups

Why I Don’t Recommend People To Get into Cybersecurity?

Cybersecurity isn’t always what it seems — it’s tough, demanding, and stressful.

Oct 24 388 6

Jonathan Mondaut

How ChatGPT Turned Me into a Hacker

Discover how ChatGPT helped me become a hacker, from gathering resources to tackling...

Jun 18 1.6K 53

Lists

Tech & Tools
21 stories · 332 saves

Medium's Huge List of Publications Accepting...
378 stories · 3812 saves

Staff Picks
755 stories · 1415 saves

Natural Language Processing
1788 stories · 1391 saves

RED TEAM

Malware Development Part 8 : Reverse Shell Via Dll Hijacking

“From DLL to Shell: A Step-by-Step Guide to Reverse Shell via DLL Hijacking”

✦ Jun 22 147

Dean

Setting Up Velociraptor for Forensic Analysis in a Home Lab |...

Before I start, Update you will not find article related to setting up Velociraptor in home la...

Oct 6

See more recommendations

Help Status About Careers Press Blog Privacy Terms Text to speech Teams