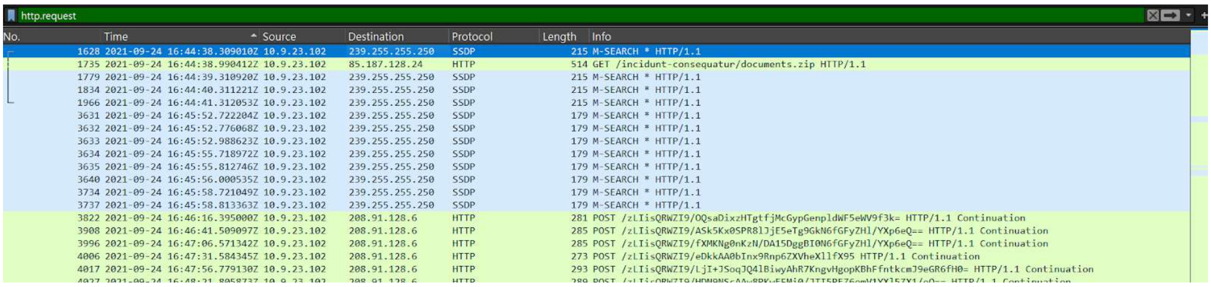
Appendix

Part 1: Initial Infection & File Transfer

1. When did the initial malicious HTTP connection occur? (Provide the date and time in yyyy-mm-dd hh:mm:ss format).

Ans:



```
http.request
No.     Time                         Source       Destination      Protocol  Length Info
   1628 2021-09-24 16:44:38.309010Z 10.9.23.102  239.255.255.250  SSDP         215 M-SEARCH * HTTP/1.1
   1735 2021-09-24 16:44:38.990412Z 10.9.23.102  85.187.128.24    HTTP         514 GET /incidunt-consequatur/documents.zip HTTP/1.1
   1779 2021-09-24 16:44:39.310920Z 10.9.23.102  239.255.255.250  SSDP         215 M-SEARCH * HTTP/1.1
   1834 2021-09-24 16:44:40.311221Z 10.9.23.102  239.255.255.250  SSDP         215 M-SEARCH * HTTP/1.1
   1966 2021-09-24 16:44:41.312053Z 10.9.23.102  239.255.255.250  SSDP         215 M-SEARCH * HTTP/1.1
   3631 2021-09-24 16:45:52.722204Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3632 2021-09-24 16:45:52.776068Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3633 2021-09-24 16:45:52.988623Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3634 2021-09-24 16:45:55.718972Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3635 2021-09-24 16:45:55.812746Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3640 2021-09-24 16:45:56.000535Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3734 2021-09-24 16:45:58.721049Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3737 2021-09-24 16:45:58.813363Z 10.9.23.102  239.255.255.250  SSDP         179 M-SEARCH * HTTP/1.1
   3822 2021-09-24 16:46:16.395000Z 10.9.23.102  208.91.128.6     HTTP         281 POST /zLIisQRWZI9/OQsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1 Continuation
   3908 2021-09-24 16:46:41.509097Z 10.9.23.102  208.91.128.6     HTTP         285 POST /zLIisQRWZI9/ASk5Kx0SPR8lJjE5eTg9GkN6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
   3996 2021-09-24 16:47:06.571342Z 10.9.23.102  208.91.128.6     HTTP         285 POST /zLIisQRWZI9/fXMKNg0nKzN/DA15DggBI0N6fGFyZHl/YXp6eQ== HTTP/1.1 Continuation
   4006 2021-09-24 16:47:31.584345Z 10.9.23.102  208.91.128.6     HTTP         273 POST /zLIisQRWZI9/eDkkAA0bInx9Rnp6ZXVheXllfX95 HTTP/1.1 Continuation
   4017 2021-09-24 16:47:56.779130Z 10.9.23.102  208.91.128.6     HTTP         293 POST /zLIisQRWZI9/LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFfntkcmJ9eGR6fH0= HTTP/1.1 Continuation
```

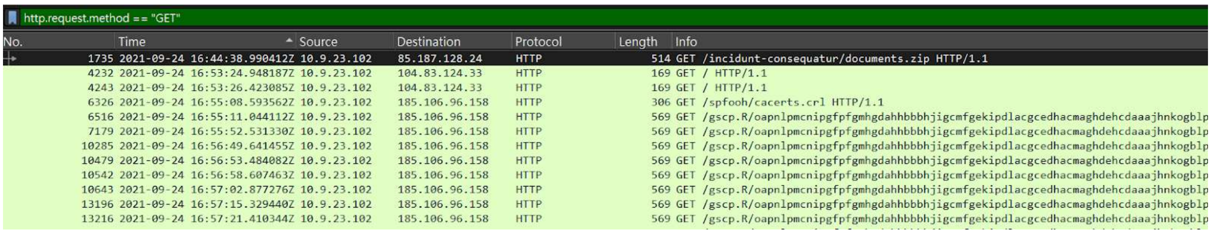
1735 2021-09-24 16:44:38.990412Z 10.9.23.102 85.187.128.24 HTTP 514 GET /incidunt-consequatur/documents.zip HTTP/1.1

UTC Arrival Time: Sep 24, 2021 16:44:38.309010000 UTC

2021-09-24 16:44:38

2. What is the name of the compressed file that the victim downloaded?

Ans:



```
http.request.method == "GET"
No.     Time                         Source       Destination      Protocol  Length Info
   1735 2021-09-24 16:44:38.990412Z 10.9.23.102  85.187.128.24    HTTP         514 GET /incidunt-consequatur/documents.zip HTTP/1.1
   4232 2021-09-24 16:53:24.948187Z 10.9.23.102  104.83.124.33    HTTP         169 GET / HTTP/1.1
   4243 2021-09-24 16:53:26.423085Z 10.9.23.102  104.83.124.33    HTTP         169 GET / HTTP/1.1
   6326 2021-09-24 16:55:08.593562Z 10.9.23.102  185.106.96.158   HTTP         306 GET /spfooh/cacerts.crl HTTP/1.1
   6516 2021-09-24 16:55:11.044112Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
   7179 2021-09-24 16:55:52.531330Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
  10285 2021-09-24 16:56:49.641455Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
  10479 2021-09-24 16:56:53.484082Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
  10542 2021-09-24 16:56:58.607463Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
  10643 2021-09-24 16:57:02.877276Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
  13196 2021-09-24 16:57:15.329440Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
  13216 2021-09-24 16:57:21.410344Z 10.9.23.102  185.106.96.158   HTTP         569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjigcmfgekipdlacgcedhacmaghdehcdaaajhnkogblp
```

[Full request URI: http://attirenepal.com/incidunt-consequatur/documents.zip]

documents.zip

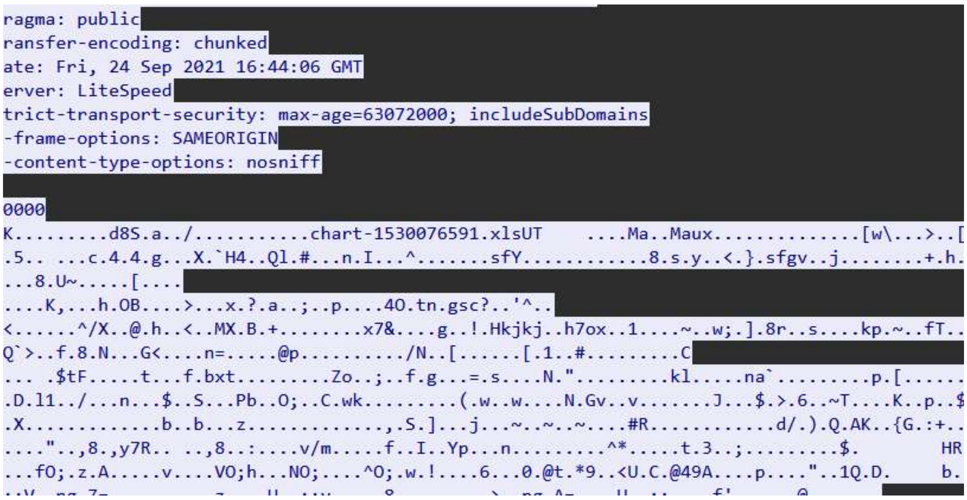
3. Which domain hosted the malicious compressed file?

Ans:

attirenepal.com

4. What is the name of the file located inside the compressed archive?

Ans:



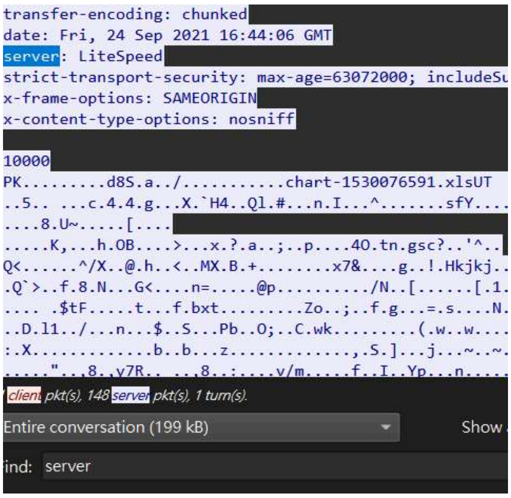
```
ragma: public
ransfer-encoding: chunked
ate: Fri, 24 Sep 2021 16:44:06 GMT
erver: LiteSpeed
trict-transport-security: max-age=63072000; includeSubDomains
-frame-options: SAMEORIGIN
-content-type-options: nosniff

0000
K.........d8S.a../...........chart-1530076591.xlsUT    ....Ma..Maux..............[w\...>..[
.5.. ...c.4.4.g...X.`H4..Ql.#...n.I...^.......sfY............8.s.y..<.}.sfgv..j........+.h.
...8.U~.....[....
....K,...h.OB....>...x.?.a..;..p....4O.tn.gsc?..'^..
<......^/X..@.h..<..MX.B.+........x7&....g..!.Hkjkj..h7ox..1....~..w;.].8r..s....kp.~..fT..
Q`>..f.8.N...G<....n=.....@p........../N..[......[.1..#.........C
... .$tF.....t...f.bxt.........Zo..;..f.g...=.s....N."..........kl.....na`.........p.[......
.D.l1../...n...$..S...Pb..O;..C.wk.........(.w..w....N.Gv..v.......J...$.>.6..~T....K..p..$
.X.............b..b...z.............,.S.]...j...~..~..~....#R............d/.).Q.AK..{G.:+..
...."..,8.,y7R.. ..,8..:....v/m.....f..I..Yp...n.........^*.....t.3..;.........$.      HR
...fO;.z.A.....v....VO;h...NO;....^O;.w.!....6...0.@t.*9..<U.C.@49A....p...."..1Q.D.     b.
```

chart-1530076591.xls

5. Identify the specific web server software (Server header) running on the malicious IP address that served the compressed file.

Ans:



```
transfer-encoding: chunked
date: Fri, 24 Sep 2021 16:44:06 GMT
server: LiteSpeed
strict-transport-security: max-age=63072000; includeSu
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff

10000
PK.........d8S.a../...........chart-1530076591.xlsUT
..5.. ...c.4.4.g...X.`H4..Ql.#...n.I...^.......sfY....
....8.U~.....[....
.....K,...h.OB....>...x.?.a..;..p....4O.tn.gsc?..'^..
Q<......^/X..@.h..<..MX.B.+........x7&....g..!.Hkjkj..
.Q`>..f.8.N...G<....n=.....@p........../N..[......[.1.
.... .$tF.....t...f.bxt.........Zo..;..f.g...=.s....N.
..D.l1../...n...$..S...Pb..O;..C.wk.........(.w..w....
:.X.............b..b...z.............,.S.]...j...~..~.
....."...8.,y7R.. ...8..:....v/m.....f..I..Yp...n.....
```

client pkt(s), 148 server pkt(s), 1 turn(s).

ind: server

LiteSpeed

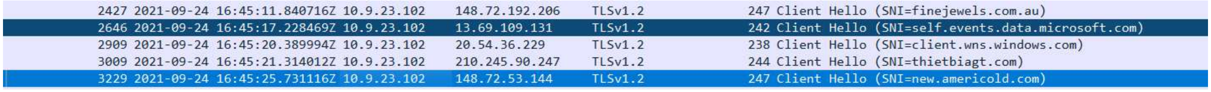
6. What is the version number of the web server identified in the previous question?

Ans:

PHP/7.2.34

7. Identify the three additional domains that were involved in downloading malicious files to the victim host.
Hint: Inspect HTTPS traffic and focus on the time window between 16:45:11 and 16:45:30. Note this range is in UTC, not BST.

Ans:

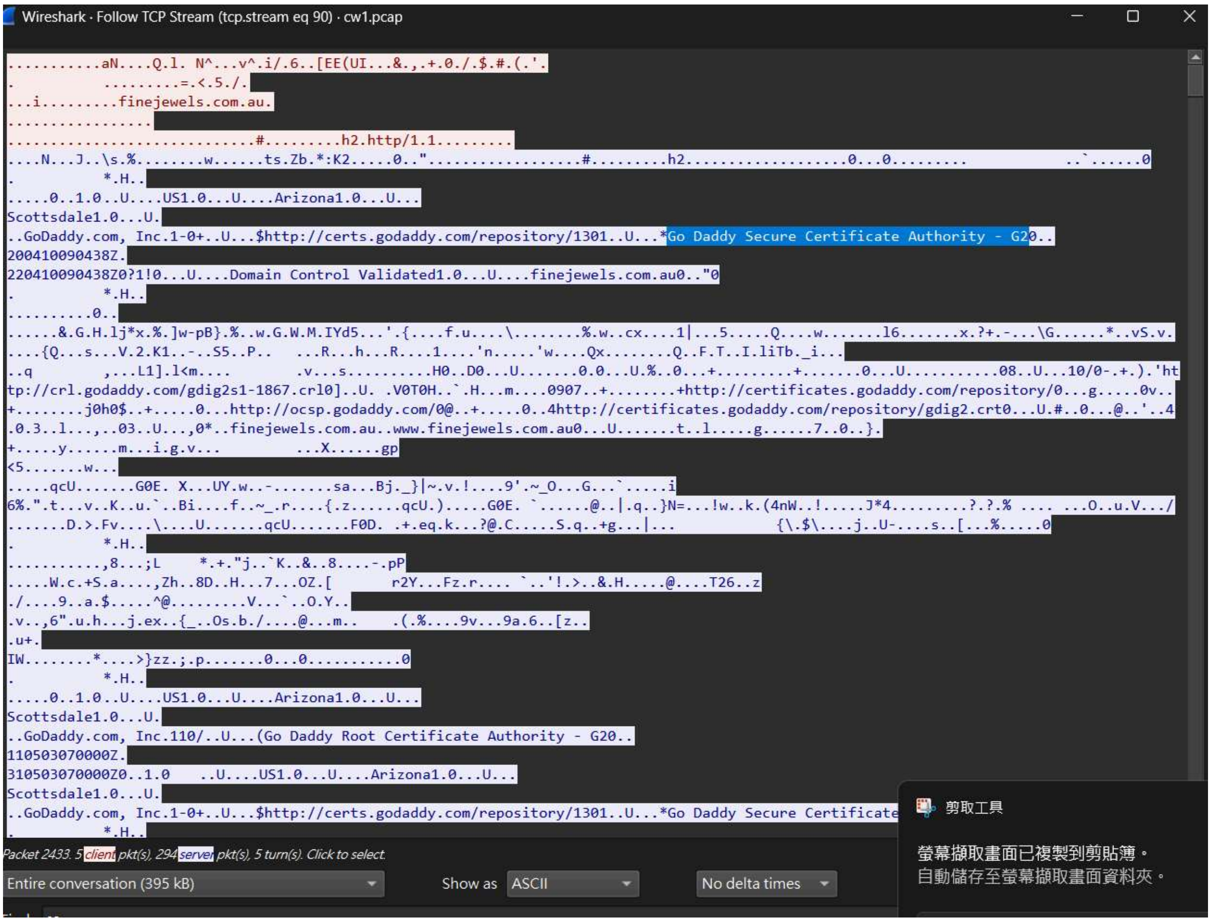


```
2427 2021-09-24 16:45:11.840716Z 10.9.23.102    148.72.192.206    TLSv1.2    247 Client Hello (SNI=finejewels.com.au)
2646 2021-09-24 16:45:17.228469Z 10.9.23.102    13.69.109.131     TLSv1.2    242 Client Hello (SNI=self.events.data.microsoft.com)
2909 2021-09-24 16:45:20.389994Z 10.9.23.102    20.54.36.229      TLSv1.2    238 Client Hello (SNI=client.wns.windows.com)
3009 2021-09-24 16:45:21.314012Z 10.9.23.102    210.245.90.247    TLSv1.2    244 Client Hello (SNI=thietbiagt.com)
3229 2021-09-24 16:45:25.731116Z 10.9.23.102    148.72.53.144     TLSv1.2    247 Client Hello (SNI=new.americold.com)
```

finejewels.com.au
thietbiagt.com
new.americold.com

Part 2: Command and Control (C2) Activity
8. Which Certificate Authority (CA) issued the SSL certificate for the first domain identified in question 7?

Ans:



Wireshark · Follow TCP Stream (tcp.stream eq 90) · cw1.pcap

```
..........aN....Q.l. N^...v^.i/.6..[EE(UI...&.,.+.0./.$.#.(.'.
.         .........=.<.5./.
...i.........finejewels.com.au.
................
...........................#.........h2.http/1.1........
....N...J..\s.%........w......ts.Zb.*:K2.....0.."..................#.........h2..................0...0........          ..`......0
.         *.H..
.....0..1.0..U....US1.0...U....Arizona1.0...U...
Scottsdale1.0...U.
..GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate Authority - G20..
200410090438Z.
220410090438Z0?1!0...U....Domain Control Validated1.0...U....finejewels.com.au0.."0
.         *.H..
.........0..
......&.G.H.1j*x.%.]w-pB}.%..w.G.W.M.IYd5...'.{....f.u....\........%.w..cx....1|...5.....Q....w.......16.......x.?+.-...\G......*..vS.v.
....{Q...s...V.2.K1..-..S5..P..   ...R...h...R....1....'n.....'w....Qx........Q..F.T..I.liTb._i...
..q         ,...L1].l<m....        .v...s..........H0..D0...U.......0.0...U.%..0...+.........+.......0...U...........08..U...10/0-.+.).'ht
tp://crl.godaddy.com/gdig2s1-1867.crl0]..U. .V0T0H..`.H...m....0907..+........+http://certificates.godaddy.com/repository/0...g.....0v..
+........j0h0$..+.....0...http://ocsp.godaddy.com/0@..+.....0..4http://certificates.godaddy.com/repository/gdig2.crt0...U.#..0...@..'..4
.0.3..l...,..03..U...,0*..finejewels.com.au..www.finejewels.com.au0...U.......t..l.....g......7..0..}.
+.....y......m...i.g.v...         ...X......gp
<5.......w...
.....qcU.......G0E. X...UY.w..-.......sa...Bj._}|~.v.!....9'.~_O...G...`.....i
6%.".t...v..K..u.`..Bi....f..~_.r....{.z......qcU.).....G0E. `......@..|.q..}N=...!w..k.(4nW..!.....J*4.........?.?.% ....  ...O..u.V.../
.......D.>.Fv....\....U.......qcU.......F0D. .+.eq.k...?@.C.....S.q..+g...|...            {\.$\....j..U-....s..[...%.....0
.         *.H..
..........,8...;L     *.+."j..`K..&..8....-.pP
.....W.c.+S.a....,Zh..8D..H...7...OZ.[       r2Y...Fz.r....  `..'!.>..&.H.....@....T26..z
./....9..a.$.....^@.........V...`..O.Y..
.v..,6".u.h...j.ex..{_..Os.b./....@...m..    .(.%....9v...9a.6..[z..
.u+.
IW........*....>}zz.;.p.......0...0...........0
.         *.H..
.....0..1.0..U....US1.0...U....Arizona1.0...U...
Scottsdale1.0...U.
..GoDaddy.com, Inc.110/..U...(Go Daddy Root Certificate Authority - G20..
110503070000Z.
310503070000Z0..1.0    ..U....US1.0...U....Arizona1.0...U...
Scottsdale1.0...U.
..GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate
.         *.H..
```

Packet 2433. 5 client pkt(s), 294 server pkt(s), 5 turn(s). Click to select.

Entire conversation (395 kB) Show as ASCII No delta times

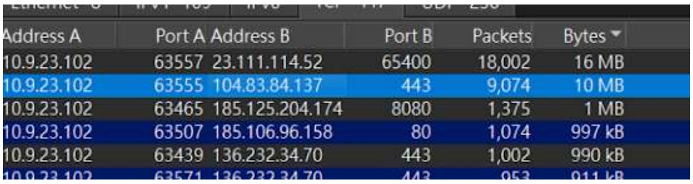
剪取工具

螢幕擷取畫面已複製到剪貼簿。
自動儲存至螢幕擷取畫面資料夾。

GoDaddy

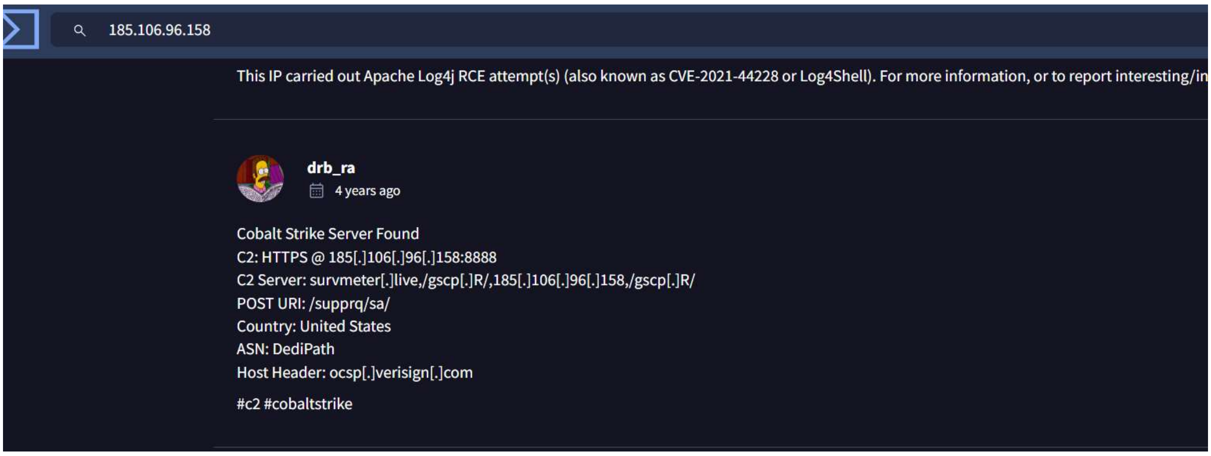
9. What are the two IP addresses of the Cobalt Strike servers? (Provide them in sequential order).
Hint: Inspect the Conversations menu option

Ans:



Address A	Port A	Address B	Port B	Packets	Bytes
10.9.23.102	63557	23.111.114.52	65400	18,002	16 MB
10.9.23.102	63555	104.83.84.137	443	9,074	10 MB
10.9.23.102	63465	185.125.204.174	8080	1,375	1 MB
10.9.23.102	63507	185.106.96.158	80	1,074	997 kB
10.9.23.102	63439	136.232.34.70	443	1,002	990 kB
10.9.23.102	63571	136.232.34.70	443	953	911 kB

Virustotal



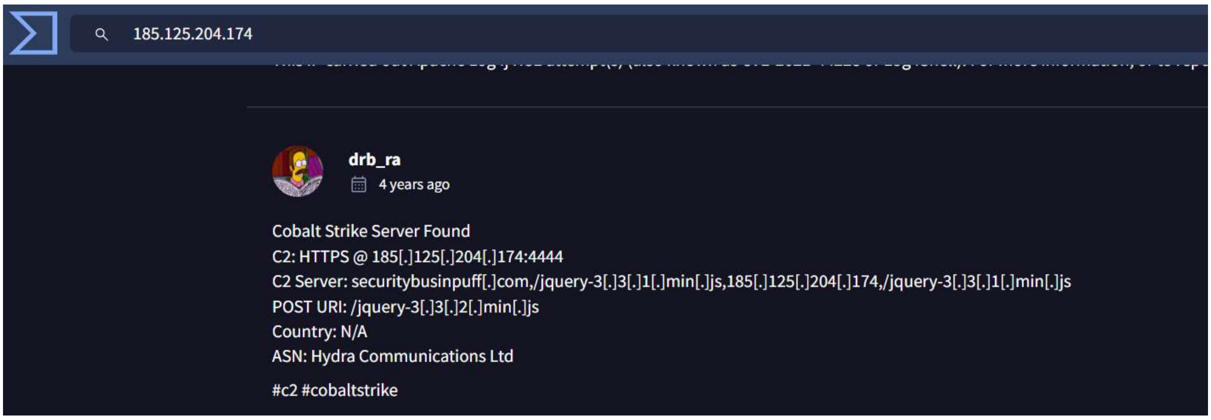
185.106.96.158

This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/in

drb_ra
4 years ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]106[.]96[.]158:8888
C2 Server: survmeter[.]live,/gscp[.]R/,185[.]106[.]96[.]158,/gscp[.]R/
POST URI: /supprq/sa/
Country: United States
ASN: DediPath
Host Header: ocsp[.]verisign[.]com

#c2 #cobaltstrike



185.125.204.174

drb_ra
4 years ago

Cobalt Strike Server Found
C2: HTTPS @ 185[.]125[.]204[.]174:4444
C2 Server: securitybusinpuff[.]com,/jquery-3[.]3[.]1[.]min[.]js,185[.]125[.]204[.]174,/jquery-3[.]3[.]1[.]min[.]js
POST URI: /jquery-3[.]3[.]2[.]min[.]js
Country: N/A
ASN: Hydra Communications Ltd

#c2 #cobaltstrike

185.106.96.158
185.125.204.174

10.What is the value of the Host header for the first Cobalt Strike IP address?
Hint: Apply a filter to isolate DNS queries.

Ans:
ocsp.verisign.com

11.What is the domain name associated with the first Cobalt Strike IP address?
Hint: Take a closer look at HTTPS (443)

Ans:
survmeter.live

12.What is the domain name associated with the second Cobalt Strike IP address?
Hint: Apply a filter to capture HTTP POST requests.

Ans:
securitybusinpuff.com

13.What is the domain name used for the post-infection traffic?

Ans:
maldivehost.net

14.What are the first eleven characters of the data the victim host sends to the malicious domain identified in the previous question?

Ans:
zLIisQRWZI9

15.What was the length of the first packet the victim sent to the C2 server?

Ans:
281

16.What was the Server header value for the malicious domain from question 13?

Ans:

Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4

Part 3: Final Exfiltration/Check-in

17.What was the date and time (in yyyy-mm-dd hh:mm:ss UTC format) when the DNS query occurred for the domain used by the malware to check the victim's external IP address?

Ans:

2021-09-24 17:00:04

18.What was the domain name in the DNS query from the previous question?

Ans:

api.ipify.org

19.What was the first email address observed in the SMTP traffic in the pcap file (the MAIL FROM address)?

Ans:

```
28576  2021-09-24 17:02:46.778017Z        10.9.23.102     185.4.29.135   SMTP  86        C:
MAIL FROM:<farshin@mailfa.com>
```

farshin@mailfa.com

20.Follow the stream from Q19. What is ho3ein.sharifi’s password?

Ans:

```
220 mail.mailfa.com

EHLO localhost

250-mail.mailfa.com
250-SIZE 30000000
250 AUTH LOGIN

AUTH LOGIN

334 VXNlcm5hbWU6

ZmFyc2hpbkBtYWlsZmEuY29t

334 UGFzc3dvcmQ6

ZGluYW1pdA==

235 authenticated.

MAIL FROM:<farshin@mailfa.com>

550 Your SMTP Service is disable please check by your mailservice provider.
```

Due to the communication using BASE64, which is decryptable, the password was found in the decrypt output.

Password:**13691369**