

Github repo: <https://github.com/aka331/COMP3010HK/tree/main/CW1>

## Section 1 – Introduction

This report presents a network traffic investigation based on the provided PCAP file and associated quiz questions. The objective is to identify the infected system, understand how the infection occurred, and determine the nature of the malware or attack involved.

The structure of this report is as follows:

Section 2 describes the tools and methodology used to analyse the PCAP and extract key indicators of compromise (IOCs).

Section 3 presents the main findings, drawing on the quiz answers and supporting evidence from the traffic analysis.

Section 4 concludes with prevention techniques, open challenges, and relevant references.

## Section 2 – Methodology

Wireshark was used to investigate the PCAP. I filtered HTTP GET traffic to find the first malicious download and extracted the timestamp, domain, file name, and server headers. I exported the downloaded archive via Export Objects to confirm the embedded file. I then used DNS/TLS evidence and Conversations statistics to identify C2 IPs and map them to domains/Host headers. Lastly, I followed the SMTP TCP stream and decoded Base64 authentication data to obtain the required email and password details.

```
http.request
```

Expression 1. Filtering only HTTP request traffic

```
http.request.method == "GET"
```

Expression 2. Filtering only HTTP GET requests

```
ip.src==10.9.23.102 && dns
```

Expression 3. Filtering only the source IP from 10.9.23.102 and the DNS protocol traffic

```
ip.addr == 185.106.96.158 && http
```

Expression 4. Filtering only the source IP from 185.106.96.158 and the HTTP traffic

```
ip.addr == 185.125.204.174 && tcp.port == 8080
```

Expression 5. Filtering only the source IP from 185.125.204.174 and the port 8080 protocol traffic

```
ip.addr==10.9.23.102 && http.request.method=="POST"
```

Expression 6. Filtering only the source IP from the user computer and the HTTP POST traffic

```
ip.addr==10.9.23.102 && dns && frame contains "api"
```

Expression 7. Filtering only the source IP from the user computer, the DNS protocol traffic, and containing “api”

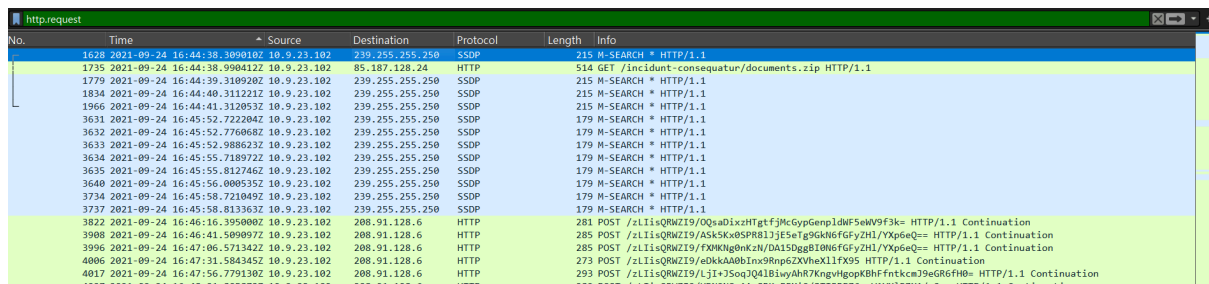
```
ip.addr==10.9.23.102 && smtp && frame contains "FROM"
```

Expression 8. Filtering only the source IP from the user computer, the SMTP protocol traffic, and containing “FROM”

## Section 3 – Results

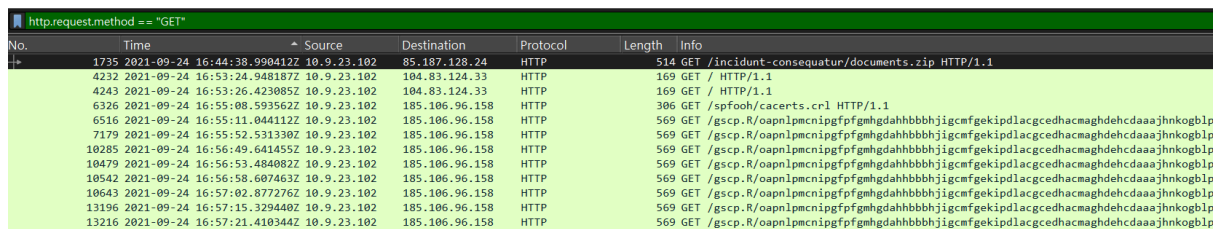
**Infected system identification:** The compromised host is the primary internal client observed initiating the earliest suspicious HTTP download and subsequent repeated C2 communications. Key identifiers captured include IP address [victim IP], MAC address [victim MAC] (from ARP/Ethernet headers), and (if present) hostname/user context from relevant traffic.

**Initial infection & file transfer:** At **2021-09-24 16:44:38** (Figure 1), the victim made an HTTP GET request to **attirenepal.com**, retrieving **documents.zip** (Figure 2&3).



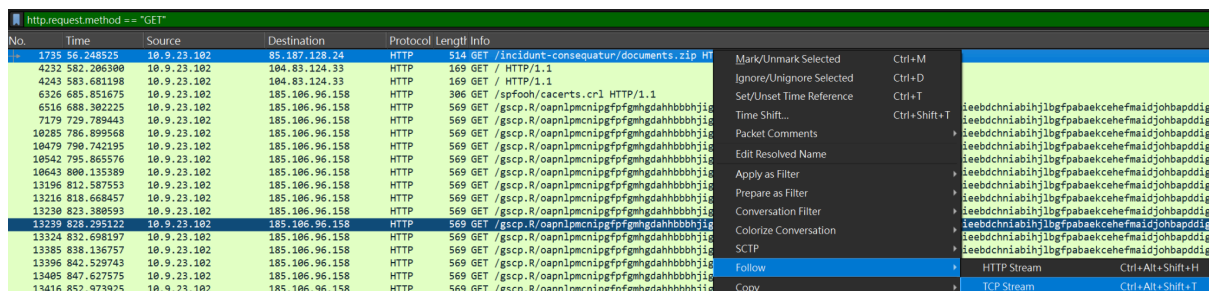
No.	Time	Source	Destination	Protocol	Length	Info
1628	2021-09-24 16:44:38.3090182	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1735	2021-09-24 16:44:38.9904122	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1
1779	2021-09-24 16:44:39.3109202	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1834	2021-09-24 16:44:40.3112212	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1966	2021-09-24 16:44:41.3120532	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3631	2021-09-24 16:45:52.7222042	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3632	2021-09-24 16:45:52.7760682	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3633	2021-09-24 16:45:52.9886232	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3634	2021-09-24 16:45:55.7189722	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3635	2021-09-24 16:45:55.8127462	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3640	2021-09-24 16:45:56.0005352	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3734	2021-09-24 16:45:58.7210492	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3737	2021-09-24 16:45:58.8133632	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3822	2021-09-24 16:46:16.3950002	10.9.23.102	208.91.128.6	HTTP	281	POST /zLIisQRWZ19/OQwaD1xzHTgtf3KcGypGepnldwF5wW9f3k= HTTP/1.1 Continuation
3908	2021-09-24 16:46:41.3090972	10.9.23.102	208.91.128.6	HTTP	285	POST /zLIisQRWZ19/ASkSkxSPR81jE5etgGAM6fGyZHI/YXp6eQ= HTTP/1.1 Continuation
3996	2021-09-24 16:47:06.5713422	10.9.23.102	208.91.128.6	HTTP	285	POST /zLIisQRWZ19/FXWKLg0nkzN/DAl50gg810M6fGyZHI/YXp6eQ= HTTP/1.1 Continuation
4006	2021-09-24 16:47:31.5843452	10.9.23.102	208.91.128.6	HTTP	273	POST /zLIisQRWZ19/e0kkA0bInx9Rnp6ZXheX11fX95 HTTP/1.1 Continuation
4017	2021-09-24 16:47:56.7791302	10.9.23.102	208.91.128.6	HTTP	293	POST /zLIisQRWZ19/LjI+3Soq3Q41BiuyAhr7KngvHgopKBHfntkc39eGR6FH0= HTTP/1.1 Continuation

Figure 1. First HTTP request



No.	Time	Source	Destination	Protocol	Length	Info
1735	2021-09-24 16:44:38.9904122	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1
4232	2021-09-24 16:53:24.9481872	10.9.23.102	104.83.124.33	HTTP	169	GET / HTTP/1.1
4243	2021-09-24 16:53:26.4230852	10.9.23.102	104.83.124.33	HTTP	169	GET / HTTP/1.1
6326	2021-09-24 16:55:08.5935622	10.9.23.102	185.106.96.158	HTTP	306	GET /spfooh/cacerts.cr1 HTTP/1.1
6516	2021-09-24 16:55:11.0441122	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
7179	2021-09-24 16:55:52.5313302	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10285	2021-09-24 16:56:49.6414552	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10479	2021-09-24 16:56:53.4840822	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10542	2021-09-24 16:56:58.6074632	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10643	2021-09-24 16:57:02.8772762	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13196	2021-09-24 16:57:15.3294402	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13216	2021-09-24 16:57:21.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp

Figure 2. HTTP GET request that discovers document.zip



No.	Time	Source	Destination	Protocol	Length	Info
1735	2021-09-24 16:44:38.9904122	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1
4232	2021-09-24 16:53:24.9481872	10.9.23.102	104.83.124.33	HTTP	169	GET / HTTP/1.1
4243	2021-09-24 16:53:26.4230852	10.9.23.102	104.83.124.33	HTTP	169	GET / HTTP/1.1
6326	2021-09-24 16:55:08.5935622	10.9.23.102	185.106.96.158	HTTP	306	GET /spfooh/cacerts.cr1 HTTP/1.1
6516	2021-09-24 16:55:11.0441122	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
7179	2021-09-24 16:55:52.5313302	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10285	2021-09-24 16:56:49.6414552	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10479	2021-09-24 16:56:53.4840822	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10542	2021-09-24 16:56:58.6074632	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
10643	2021-09-24 16:57:02.8772762	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13196	2021-09-24 16:57:15.3294402	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13216	2021-09-24 16:57:21.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13230	2021-09-24 16:57:23.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13239	2021-09-24 16:57:25.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13324	2021-09-24 16:57:27.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13385	2021-09-24 16:57:29.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13396	2021-09-24 16:57:31.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13405	2021-09-24 16:57:33.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp
13416	2021-09-24 16:57:35.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oaaplpmcniipgfpfgmghdahbbbhjgicmfgekipdlacgedhacmaghdchdaaaahjnkogblp

Figure 3. Select TCP Stream to view the dedicated traffic from GET /incident-consequatur/documents.zip HTTP/1.1

Exporting HTTP objects confirmed the archive contained **chart-1530076591.xls** (Figures 4 & 5). The malicious web server responded with Server: **LiteSpeed** with **PHP/7.2.34** (Figure 6), indicating the attacker-controlled infrastructure delivering the initial payload.

```
GET /incident-consequatur/documents.zip HTTP/1.1
Host: attirenepal.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36 Edg/93.0.961.52
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
x-powered-by: PHP/7.2.34
Set-Cookie: PHPSESSID=638a4b99bd3f8f7b0ca7e3b6f14c; path=/
Content-Description: File Transfer
Content-Type: application/octet-stream
Content-Disposition: attachment; filename=documents.zip
Content-Transfer-Encoding: binary
Expires: 0
Cache-Control: must-revalidate, post-check=0, pre-check=0
Pragma: public
Transfer-Encoding: chunked
Date: Fri, 24 Sep 2021 16:44:06 GMT
Server: LiteSpeed
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff

10000
PK.....d8S.a./.....chart-1530076591.xlsUT.....Ma..Maux.....[w....[.U@X@...K&
...S...c.4.4.g...X.`H4..Q1.#...n.I.....sfY.....8.s.y.<.
...B.U.....[.....
...K...h.OB....>...x.?..a.;..p....40.tn.gsc?..'^(
...Q.....^/X..@.h.<..MX.B.+.....x7&....g..!.Hkjkj..h7ox..1....~..w;..
..Q>..f.8.N...G<....n=.....@p...../N..[.....[.1..#.....C
...$F.....t...f.bxt.....Zo.;..f.g...=s....N..".....k1....
..D.II./...n..$..S...Pb..O;.C.wk.....(w.w...N.Gv..v.....J..
b..b...S.]...j...~..~..~..#R.....d/.)..Q.AK..{G
...f.I..Yp...n.....t.3.;.....$.....HR...$b..d.@
..@.t..9..u.C.@49A...p...^.....t.Q.D. b.....15...pg.Bm...V...pgG...pg.Ze...U...V...8...pg.Am...U.
...j...F...B
...[j]..U...7..S.....*J.MT...F.Q...3a..B6.(dc.H..6./.....{.....1..4..DjM.A.....y...}..W.I.M.up#...01...1Q;..d...Q
...w..w.T.....sq.zRA...g..W.t...e...V...MG...$@a.8... @6.X...O.3.T.%:;...3..42.....I...@
...D..V.K.....X/Nk...^...6...b...b...
...8..u...@k...Y...X/Nk...^...6...b...b...
xXVe..c..l..k).......8
```

Figure 4. TCP Stream for /incident-consequatur/documents.zip

```
Cache-Control: must-revalidate, post-check=0, pre-check=0
Content-Encoding: chunked
Date: Fri, 24 Sep 2021 16:44:06 GMT
Server: LiteSpeed
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff

18S.a./.....chart-1530076591.xlsUT.....Ma..Maux...
..4.g...X.`H4..Q1.#...n.I.....sfY.....8.s.y.<.
..[.....
OB....>...x.?..a.;..p....40.tn.gsc?..'^(
..@.h.<..MX.B.+.....x7&....g..!.Hkjkj..h7ox..1....~..w;..
..G<....n=.....@p...../N..[.....[.1..#.....C
...t...f.bxt.....Zo.;..f.g...=s....N..".....k1....
n...$..S...Pb..O;.C.wk.....(w.w...N.Gv..v.....J..
.....,S.]...j...~..~..~..#R.....d/.)..Q.AK..{G
p...n.....^*.....t.3.;.....$.....HR...$b..d.@
```

Figure 5. chart-1530076591.xls inside the stream

```

HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
x-powered-by: PHP/7.2.34
set-cookie: PHPSESSID=5de638a4b99bd63f8f7b0ca7e3b6f14c; path=/
content-description: File Transfer
content-type: application/octet-stream
content-disposition: attachment; filename=documents.zip
content-transfer-encoding: binary
expires: 0
cache-control: must-revalidate, post-check=0, pre-check=0
pragma: public
transfer-encoding: chunked
date: Fri, 24 Sep 2021 16:44:06 GMT
server: LiteSpeed
strict-transport-security: max-age=63072000; includeSubDomains
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff

```

Figure 6. Web server and version

Additional download infrastructure: Within 16:45:11–16:45:30 UTC, additional domains contacted by the victim were **finejewels.com.au**, **thietbiagt.com**, and **new.americold.com**, as shown via DNS/TLS evidence (Figure 7). For the first domain, the TLS certificate issuer (CA) was **GoDaddy** (Figure 8).

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.wms.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)

Figure 7. DNS traffic

```

Wireshark - Follow TCP Stream (tcp.stream eq 90) - cw1.pcap
.....aN....Q.1. N^...v^./6..[EE(UI...&.,+.0./.$#.(.'
.....=<.5./
..i.....finejewels.com.au.
.....#.....h2.http/1.1.....
..N...J...s.%.....w.....ts.Zb.*:K2.....0.....#.....h2.....0...0.....
*.H..
....0..1.0..U...US1.0..U...Arizona1.0..U...
icottsdale1.0..U.
.GoDaddy.com, Inc.1-0+...U...$http://certs.godaddy.com/repository/1301.U...*Go Daddy Secure Certificate Authority - G2D..
00410090438Z.
!20410090438Z0?1!0...U...Domain Control Validated1.0..U...finejewels.com.au0..0
*.H..
.....0..
....&.G.H.lj*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..U...%..0...+.....0...U.....08..U...10/0-+.).'ht

```

Figure 8. CA issuer

C2 activity (Cobalt Strike): Using Statistics → Conversations, two C2 candidate servers were identified: **185.125.204.174** (Port 8080) and **185.106.96.158** (Port 80) (Figures 9 & 10 & 11).

DNS analysis linked **185.106.96.158** (Port 80) to **survmeter.live** (Figure 12), and the Host/SNI value observed for this infrastructure was **ocsp.verisign.com** (Figure 13).

For **185.125.204.174**, HTTP POST traffic revealed an association with **securitybusinpuuff.com** (Figure 14).

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

Figure 9. TCP stream statistics in order of packets

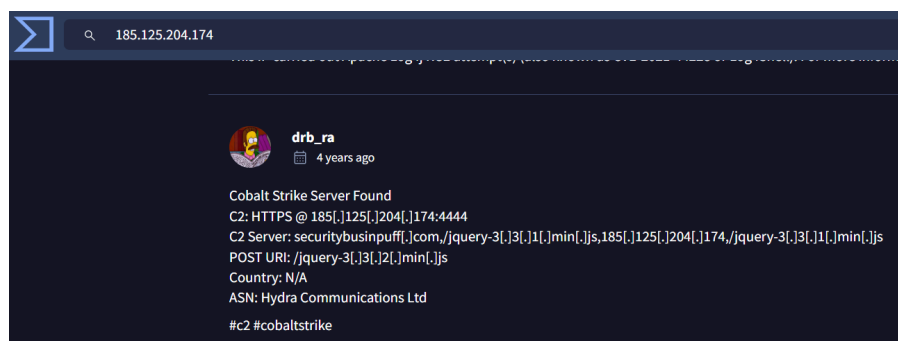


Figure 10. Virustotal review (1)

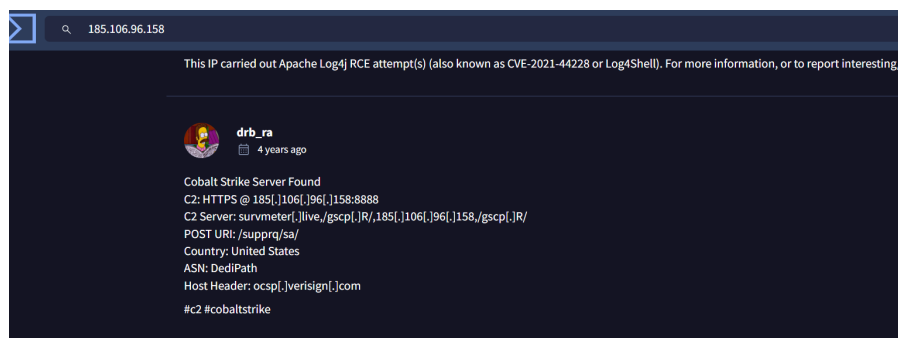


Figure 11. Virustotal review (2)

No.	Time	Source	Desti
6326	2021-09-24 16:55:08.593562Z	DESKTOP-IOJC6RB.goingfortune.com	surv
6505	2021-09-24 16:55:10.600344Z	survmeter.live	DESK
6516	2021-09-24 16:55:11.044112Z	DESKTOP-IOJC6RB.goingfortune.com	surv
6524	2021-09-24 16:55:11.290931Z	survmeter.live	DESK
7179	2021-09-24 16:55:52.531330Z	DESKTOP-IOJC6RB.goingfortune.com	surv
7181	2021-09-24 16:55:52.831411Z	survmeter.live	DESK

Figure 12. Domain linked to 185.106.96.158

ip.addr == 185.106.96.158 && http				
No.	Time	Source	Destination	
6326	2021-09-24 16:55:08.593562Z	10.9.23.102	185.106.96.158	
6505	2021-09-24 16:55:10.600344Z	185.106.96.158	10.9.23.102	
6516	2021-09-24 16:55:11.044112Z	10.9.23.102	185.106.96.158	
6524	2021-09-24 16:55:11.290931Z	185.106.96.158	10.9.23.102	
7179	2021-09-24 16:55:52.531330Z	10.9.23.102	185.106.96.158	
7181	2021-09-24 16:55:52.831411Z	185.106.96.158	10.9.23.102	
10285	2021-09-24 16:56:49.641455Z	10.9.23.102	185.106.96.158	
10291	2021-09-24 16:56:49.892169Z	185.106.96.158	10.9.23.102	
10479	2021-09-24 16:56:53.484082Z	10.9.23.102	185.106.96.158	
10487	2021-09-24 16:56:53.726722Z	185.106.96.158	10.9.23.102	
10542	2021-09-24 16:56:58.607463Z	10.9.23.102	185.106.96.158	
10550	2021-09-24 16:56:58.864872Z	185.106.96.158	10.9.23.102	
10643	2021-09-24 16:57:02.877276Z	10.9.23.102	185.106.96.158	
12145	2021-09-24 16:57:09.344753Z	185.106.96.158	10.9.23.102	
12436	2021-09-24 16:57:10.251419Z	10.9.23.102	185.106.96.158	
12954	2021-09-24 16:57:10.555165Z	185.106.96.158	10.9.23.102	
13196	2021-09-24 16:57:15.329440Z	10.9.23.102	185.106.96.158	
13198	2021-09-24 16:57:15.574022Z	185.106.96.158	10.9.23.102	
13205	2021-09-24 16:57:15.825481Z	10.9.23.102	185.106.96.158	
13207	2021-09-24 16:57:16.188305Z	185.106.96.158	10.9.23.102	
13216	2021-09-24 16:57:21.410344Z	10.9.23.102	185.106.96.158	
13218	2021-09-24 16:57:21.740566Z	185.106.96.158	10.9.23.102	
Frame 6326: Packet, 306 bytes on wire (2448 bits), 306 bytes captured (2448 bit) Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear_b6:93: Internet Protocol Version 4, Src: 10.9.23.102, Dst: 185.106.96.158 Transmission Control Protocol, Src Port: 63447, Dst Port: 80, Seq: 1, Ack: 1, L Hypertext Transfer Protocol GET /spfooh/cacerts.crl HTTP/1.1\r\n Host: ocp.verisign.com\r\n User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH Connection: Close\r\n Cache-Control: no-cache\r\n \r\n [Response in frame: 6505] [Full request URI: http://ocsp.verisign.com/spfooh/cacerts.crl]				

Figure 13. Request URL for 185.106.96.158

ip.addr == 185.125.204.174 && tcp.port == 8080				
No.	Time	Source	Destination	Proto
4216	2021-09-24 16:53:24.084722Z	DESKTOP-IOJC6RB.goingfortune.com	securitybusinpu...com	TCP
4217	2021-09-24 16:53:24.246485Z	securitybusinpu...com	DESKTOP-IOJC6RB.goingfort...	TCP
4218	2021-09-24 16:53:24.246766Z	DESKTOP-IOJC6RB.goingfortune.com	securitybusinpu...com	TCP
4219	2021-09-24 16:53:24.251794Z	DESKTOP-IOJC6RB.goingfortune.com	securitybusinpu...com	TCP
4220	2021-09-24 16:53:24.251887Z	securitybusinpu...com	DESKTOP-IOJC6RB.goingfort...	TCP
4221	2021-09-24 16:53:24.425150Z	securitybusinpu...com	DESKTOP-IOJC6RB.goingfort...	TCP
4222	2021-09-24 16:53:24.425395Z	DESKTOP-IOJC6RB.goingfortune.com	securitybusinpu...com	TCP

Figure 14. Domain linked to 185.125.204.174



Post-infection beaconing traffic was primarily directed to **maldivehost.net** (Figure 15), with the victim sending data beginning with **zLIisQRWZI9** (Figure 16). The first packet from the victim to the C2 server had a frame length of **281** bytes (Figure 16). Server-side response headers from **maldivehost.net** indicated Server: **Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod\_bwlimited/1.4** (Figure 17), which further supports that this domain was attacker-controlled and actively responding to client beacons.

ip.addr==10.9.23.102 && http.request.method=="POST"

No.	Time	Source	Destination
3822	2021-09-24 16:46:16.395000Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
3908	2021-09-24 16:46:41.509097Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
3996	2021-09-24 16:47:06.571342Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4006	2021-09-24 16:47:31.584345Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4017	2021-09-24 16:47:56.779130Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4027	2021-09-24 16:48:21.805873Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4037	2021-09-24 16:48:46.850457Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4046	2021-09-24 16:49:11.959706Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4090	2021-09-24 16:49:37.041462Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4099	2021-09-24 16:50:02.211046Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4109	2021-09-24 16:50:27.298936Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net
4118	2021-09-24 16:50:52.306135Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net

Figure 15. Post-infection beaconing traffic

No.	Time	Source	Destination	Protocol	Length	Info
3822	2021-09-24 16:46:16.395000Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net	HTTP	281	POST /zLIisQRWZI9/OQsaDixzHTgtfj
3908	2021-09-24 16:46:41.509097Z	DESKTOP-IOJC6RB.goingfortune.com	maldivehost.net	HTTP	285	POST /zLIisQRWZI9/Ask5Kx0SPR81Jj

Figure 16. Post-infection beaconing traffic

Wireshark · Follow TCP Stream (tcp.stream eq 111) · cw1.pcap

POST /zLIisQRWZI9/LjI+JSQJQ4lBiwyAhR7KngvHgopKBhFfntkcmJ9eGR6fH0= HTTP/1.1
Host: maldivehost.net
Content-Length: 112
Dw8YBxsEGmYFAAEJfR4NQkMmLTyqZDk5KyQmOyRGQglxEBo4Lzk/EyYrMi1hOT8vIyM7IhcNPzsOKjguFvgkLSIiJCxFRgwFAgIIDQUZGB0FD0JF
HTTP/1.1 200 OK
Date: Fri, 24 Sep 2021 16:47:55 GMT
Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4
X-Powered-By: PHP/5.6.40
Content-Length: 302
Strict-Transport-Security: ...max-age=15552000...
Connection: close
Content-Type: text/html; charset=UTF-8
eXp7QUVCQ0FBfn15eXl/eXp8e0JBQ0JGQnpzeWJ+eXtleH1f3xBRUJDQUELDhkAGAAbZwIDBQh8GQ5GQicqNS5lOD4oICc6I0VGCHAXGTWuODgQIiozKmI9Pi4kIDeQDBQsJBBgfgQE0Q0JBRUJDQUEBBAQ0Q0VVCQ0FBAQ0EDkFFQkNBQ0EEBA5BRUJDQUFCQUNCRkJGQ0JFRUZHQUVGQudGRkZCQ0EZBRUJDQUFCQUNCRkJGQ0JFRUZHQUVGQ

Figure 17. Server header



Final exfiltration/check-in: The malware performed an external IP check via DNS at **2021-09-24 17:00:04**, querying **api.ipify.org** (Figure 18). SMTP traffic showed the first MAIL FROM address as **farshin@mailfa.com** (Figure 19). Following the same TCP stream, the password was transmitted using AUTH LOGIN (Base64), and the password associated with ho3ein.sharifi's password is **13691369** (Figures 20 & 21).

No.	Time	Source	Destination	Protocol	Length	Info
990	2021-09-24 16:44:22.274695Z	DESKTOP-IOJC6RB.goingfortune.com	goingfortune-dc.goingfort...	DNS	71	Standard query 0x26b2 A api.msn.com
993	2021-09-24 16:44:22.419852Z	goingfortune-dc.goingfortune.com	DESKTOP-IOJC6RB.goingfort...	DNS	186	Standard query response 0x26b2 A api.msn.com CNAME api...
24147	2021-09-24 17:00:04.093354Z	DESKTOP-IOJC6RB.goingfortune.com	goingfortune-dc.goingfort...	DNS	73	Standard query 0xc92c A api.ipify.org
24149	2021-09-24 17:00:04.233364Z	goingfortune-dc.goingfortune.com	DESKTOP-IOJC6RB.goingfort...	DNS	299	Standard query response 0xc92c A api.ipify.org CNAME n...
25279	2021-09-24 17:00:59.174080Z	DESKTOP-IOJC6RB.goingfortune.com	goingfortune-dc.goingfort...	DNS	73	Standard query 0x8eed A api.ipify.org
25281	2021-09-24 17:00:59.324491Z	goingfortune-dc.goingfortune.com	DESKTOP-IOJC6RB.goingfort...	DNS	299	Standard query response 0x8eed A api.ipify.org CNAME n...
26756	2021-09-24 17:02:17.477261Z	DESKTOP-IOJC6RB.goingfortune.com	goingfortune-dc.goingfort...	DNS	73	Standard query 0x8d97 A api.ipify.org
26763	2021-09-24 17:02:17.634232Z	goingfortune-dc.goingfortune.com	DESKTOP-IOJC6RB.goingfort...	DNS	299	Standard query response 0x8d97 A api.ipify.org CNAME n...
27836	2021-09-24 17:02:35.839648Z	DESKTOP-IOJC6RB.goingfortune.com	goingfortune-dc.goingfort...	DNS	73	Standard query 0x5250 A api.ipify.org
27838	2021-09-24 17:02:35.995693Z	goingfortune-dc.goingfortune.com	DESKTOP-IOJC6RB.goingfort...	DNS	299	Standard query response 0x5250 A api.ipify.org CNAME n...

Figure 18. A DNS query occurred for the domain used by the malware

No.	Time	Source	Destination	Protocol	Length	Info
28576	2021-09-24 17:02:46.778017Z	DESKTOP-IOJC6RB.goingfortune.com	mailfa.com	SMTP	86	C: MAIL FROM:<farshin@mailfa.com>
28804	2021-09-24 17:02:49.113592Z	DESKTOP-IOJC6RB.goingfortune.com	mailfa.com	SMTP	93	C: MAIL FROM:<ho3ein.sharifi@mailfa.com>
38985	2021-09-24 17:03:30.417353Z	DESKTOP-IOJC6RB.goingfortune.com	smtp.cultura.com.br	SMTP	112	C: MAIL FROM:<cristianoedummar@cultura.com.br> BODY=
46434	2021-09-24 17:03:59.536380Z	DESKTOP-IOJC6RB.goingfortune.com	mail.tanriverdinakliyat.c...	SMTP	95	C: MAIL FROM:<info@tanriverdinakliyat.com>
67162	2021-09-24 17:04:45.764101Z	DESKTOP-IOJC6RB.goingfortune.com	mail.aebarcelo.com	SMTP	101	C: MAIL FROM:<roser@ebarcelo.com> BODY=8BITMIME

Figure 19. SMTP traffic

```

Wireshark - Follow TCP Stream (tcp.stream eq 387) - cwi.pcap
220 mail.mailfa.com
EHLO localhost
250-mail.mailfa.com
250-SIZE 30000000
250 AUTH LOGIN
AUTH LOGIN
334 VXNlcm5hbWU6
aG8zZWludnNoYXJpZm1AbWpibGZlLnVibQ==
334 UGFzc3dvcmQ6
MTM2OTEzNjk=
235 authenticated.
MAIL FROM:<ho3ein.sharifi@mailfa.com>
550 Your SMTP Service is disable please check by your mailservice provider.

```

Figure 20. Packet content

Input

```

UGFzc3dvcmQ6
MTM2OTEzNjk=

```

Output

```

Password:13691369

```

Figure 21. BASE64 decryption

## **Section 4 – Conclusion and References**

The investigation successfully identified the infected system, reconstructed the initial infection vector, and characterised the C2 infrastructure and final exfiltration behaviour observed in the PCAP. The combination of protocol filtering, conversation analysis, and correlation with the quiz questions enabled a coherent incident narrative from initial compromise to attacker objectives.

To prevent similar incidents in the future, organisations should enforce secure web gateways, robust endpoint protection, and strict email filtering, as well as monitor network traffic for abnormal HTTP/HTTPS patterns and known malicious domains. Implementation of network intrusion detection systems (NIDS), regular patching, least-privilege access, and multi-factor authentication can further reduce the risk of successful compromise and lateral movement.

Open challenges remain around detecting encrypted C2 traffic, identifying zero-day malware, and distinguishing benign from malicious use of legitimate cloud and web services. Continued improvement of threat intelligence integration, behavioural analytics, and incident response processes is essential for enhancing situational awareness and resilience.

## Reference

1. Palo Alto Networks Unit 42:  
Unit 42. (n.d.). Using Wireshark display filter expressions. Palo Alto Networks.  
<https://unit42.paloaltonetworks.com/using-wireshark-display-filter-expressions/>
2. Wireshark User's Guide :  
Wireshark Foundation. (2019). Wireshark user's guide (Version 4.7.0).  
[https://www.wireshark.org/docs/wsug\\_html\\_chunked/](https://www.wireshark.org/docs/wsug_html_chunked/)

# 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:

No.	Time	Source	Destination	Protocol	Length	Info
1628	2021-09-24 16:44:38.3090102	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1735	2021-09-24 16:44:38.9904122	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1
1779	2021-09-24 16:44:39.3109207	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1834	2021-09-24 16:44:40.3112212	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
1966	2021-09-24 16:44:41.3120532	10.9.23.102	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3631	2021-09-24 16:45:52.7222042	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3632	2021-09-24 16:45:52.7768082	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3633	2021-09-24 16:45:52.9886232	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3634	2021-09-24 16:45:55.7189722	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3635	2021-09-24 16:45:55.8127462	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3640	2021-09-24 16:45:56.0005352	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3734	2021-09-24 16:45:58.7218492	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3717	2021-09-24 16:45:58.8133632	10.9.23.102	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
3822	2021-09-24 16:46:16.3950002	10.9.23.102	208.91.128.6	HTTP	281	POST /zLIisQRWZ19/OQsaDixzHTgtfJMcGypGenpldwf5ekW9f3k= HTTP/1.1 Continuation
3908	2021-09-24 16:46:41.5090972	10.9.23.102	208.91.128.6	HTTP	285	POST /zLIisQRWZ19/ASK5Kx0SPR81jE5eTg9Gkh6FGyZHL/Yxp6eQ== HTTP/1.1 Continuation
3996	2021-09-24 16:47:06.5713422	10.9.23.102	208.91.128.6	HTTP	285	POST /zLIisQRWZ19/FXWKhGbnkzN/DA150gg8I0M6FGyZHL/Yxp6eQ== HTTP/1.1 Continuation
4006	2021-09-24 16:47:31.5843452	10.9.23.102	208.91.128.6	HTTP	273	POST /zLIisQRWZ19/e0KkAA0bInx9Rnp6ZXheXlF905 HTTP/1.1 Continuation
4017	2021-09-24 16:47:56.7791302	10.9.23.102	208.91.128.6	HTTP	293	POST /zLIisQRWZ19/Lj1+35oqQ4l8I8eyMR7KngvlgopKBHffntkcm3e0R6FH0= HTTP/1.1 Continuation
4027	2021-09-24 16:48:31.0862732	10.9.23.102	208.91.128.6	HTTP	180	POST /zLIisQRWZ19/ANM0MC-AA80VJECMIG/1TTCDE7C=WHVVL62V4/0= HTTP/1.1 Continuation

1735 2021-09-24 16:44:38.990412Z 10.9.23.102 85.187.128.24 HTTP 514  
GET /incident-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:

No.	Time	Source	Destination	Protocol	Length	Info
1735	2021-09-24 16:44:38.9904122	10.9.23.102	85.187.128.24	HTTP	514	GET /incident-consequatur/documents.zip HTTP/1.1
4232	2021-09-24 16:53:24.9481872	10.9.23.102	104.83.124.33	HTTP	169	GET / HTTP/1.1
4243	2021-09-24 16:53:26.4230852	10.9.23.102	104.83.124.33	HTTP	169	GET / HTTP/1.1
6326	2021-09-24 16:55:08.5935622	10.9.23.102	185.106.96.158	HTTP	306	GET /spfooh/cacerts.crl HTTP/1.1
6516	2021-09-24 16:55:11.0441122	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
7179	2021-09-24 16:55:52.5313302	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
10285	2021-09-24 16:56:49.6414552	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
10479	2021-09-24 16:56:53.4840822	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
10542	2021-09-24 16:56:58.6074632	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
10643	2021-09-24 16:57:02.8772762	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
13196	2021-09-24 16:57:15.3294402	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp
13216	2021-09-24 16:57:21.4103442	10.9.23.102	185.106.96.158	HTTP	569	GET /gscp.R/oapnlpmcnpgfpfgmghdahhbbbjigcmfgekipdlacgedhacmaghdehdaaaajhknogblp

[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:

```
pragma: public
transfer-encoding: chunked
date: Fri, 24 Sep 2021 16:44:06 GMT
server: LiteSpeed
strict-transport-security: max-age=63072000; includeSubDomains
x-frame-options: SAMEORIGIN
x-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....40.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..0;..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
...f0;z.A....v....VO;h...NO;....^0;w..!....6....0.@t.*9..<U.C.@49A....p....."1Q.D. b.
...V...7-...H...9...>...A...H...f'...@...
```

**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; includeSubDomains
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....40.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..0;..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).
Entire conversation (199 kB) Show
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.wms.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](#)**

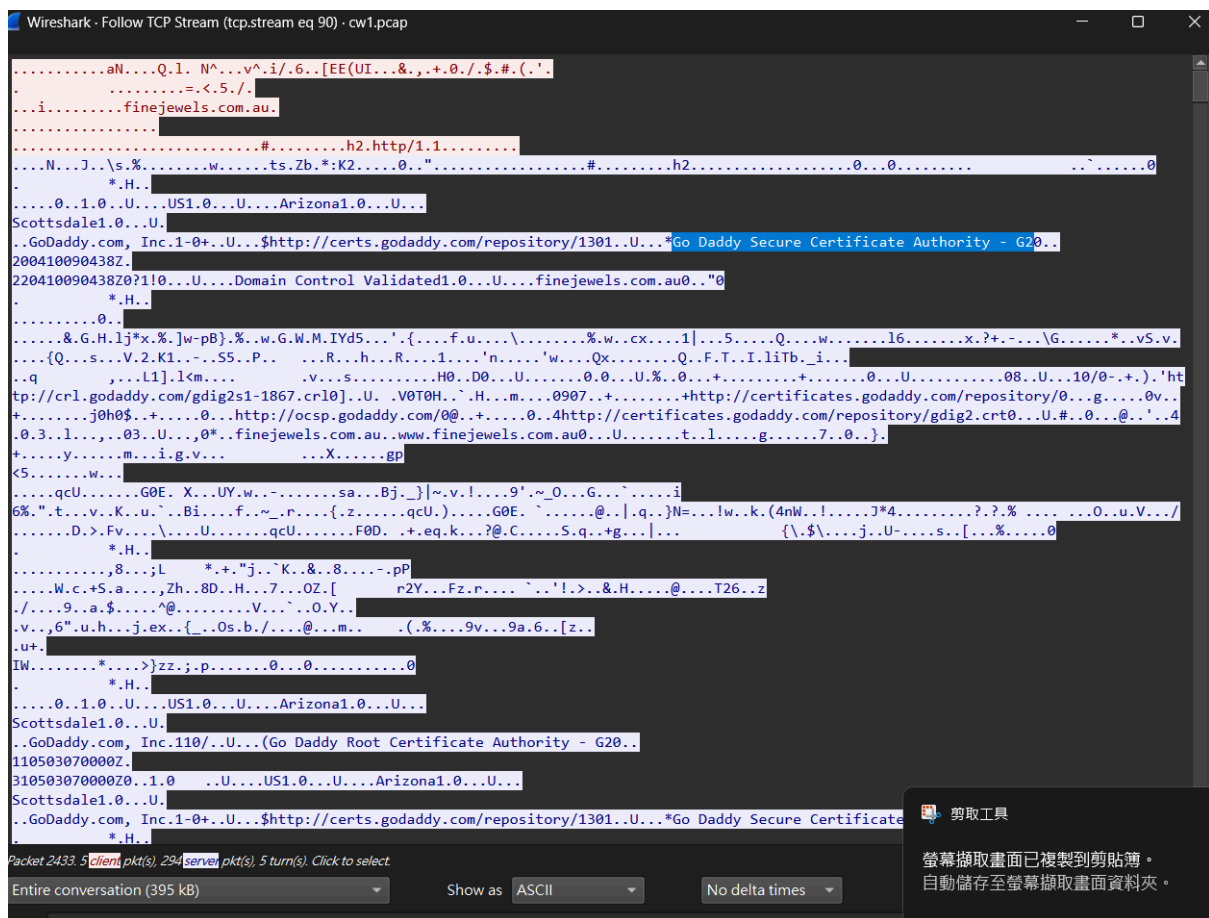
**[thietbiagt.com](#)**

**[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:



**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

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[.]125[.]204[.]174:4444  
C2 Server: securitybusinuff[.]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 disabled 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**

## Student Declaration of AI Tool use in this Assessment

Please indicate your level of usage of generative AI for this assessment - please tick the appropriate category(s).

If the “Assisted Work” or “Partnered Work” category is selected, please expand on the usage and in which elements of the assignment the usage refers to.

<b>Solo Work</b>	<b>S1 - Generative AI tools have not been used for this assessment.</b>	<input type="checkbox"/>
<b>Assisted Work</b>	<b>A1 – Idea Generation and Problem Exploration</b>  Used to generate project ideas, explore different approaches to solving a problem, or suggest features for software or systems. Students must critically assess AI-generated suggestions and ensure their own intellectual contributions are central.	<input type="checkbox"/>
	<b>A2 - Planning &amp; Structuring Projects</b> AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student’s own work.	<input type="checkbox"/>
	<b>A3 – Code Architecture</b>  AI tools maybe used to help outline code architecture (e.g. suggesting class hierarchies or module breakdowns). The final code structure must be the student’s own work.	<input type="checkbox"/>
	<b>A4 – Research Assistance</b>  Used to locate and summarise relevant articles, academic papers, technical documentation, or online resources (e.g. Stack Overflow, GitHub discussions). The interpretation and integration of research into the assignment remain the student’s responsibility.	<input type="checkbox"/>
	<b>A5 - Language Refinement</b> Used to check grammar, refine language, improve sentence structure in documentation not code. AI should be used only to provide suggestions for improvement. Students must ensure that the documentation accurately reflects the code and is technically correct.	<input type="checkbox"/>

	<b>A6 – Code Review</b>  AI tools can be used to check comments within the code and to suggest improvements to code readability, structure or syntax. AI should be used only to provide suggestions for improvement. Students must ensure that the code accurately reflects their knowledge and is technically correct.	<input type="checkbox"/>
	<b>A7 - Code Generation for Learning Purposes</b> Used to generate example code snippets to understand syntax, explore alternative implementations, or learn new programming paradigms. Students must not submit AI-generated code as their own and must be able to explain how it works.	<input type="checkbox"/>
	<b>A8 - Technical Guidance &amp; Debugging Support</b> AI tools can be used to explain algorithms, programming concepts, or debugging strategies. Students may also help interpret error messages or suggest possible fixes. However, students must write, test, and debug their own code independently and understand all solutions submitted.	<input type="checkbox"/>
	<b>A9 - Testing and Validation Support</b> AI may assist in generating test cases, validating outputs, or suggesting edge cases for software testing. Students are responsible for designing comprehensive test plans and interpreting test results.	<input type="checkbox"/>
	<b>A10 - Data Analysis and Visualization Guidance</b> AI tools can help suggest ways to analyse datasets or visualize results (e.g. recommending chart types or statistical methods). Students must perform the analysis themselves and understand the implications of the results.	<input type="checkbox"/>
	<b>A11 - Other uses not listed above</b>  Please specify:	<input type="checkbox"/>

Partnered Work	<p><b>P1 - Generative AI tool usage has been used integrally for this assessment</b></p> <p>Students can adopt approaches that are compliant with instructions in the assessment brief.</p> <p>Please Specify:</p> <ul style="list-style-type: none"> <li>- The analysis of the pcap file to verify the answer of founding</li> <li>- README.md</li> <li>- report drafting and improvement</li> <li>- generate suggested expression in Wireshark</li> </ul>	<input checked="" type="checkbox"/>
----------------	---	-------------------------------------

<p><b>Please provide details of AI usage and which elements of the coursework this relates to:</b></p> <p>improve the report, pcap analysis</p>
---

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	<input checked="" type="checkbox"/>
I confirm that all details provide above are an accurate description of how AI was used for this assessment.	<input checked="" type="checkbox"/>