COMP3010HK Security Operations and Incident Management 2025/2026

Coursework 1: Set Exercises - PCAP Analysis

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

First of all, 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. Below are the expressions used for analyzing the traffic in the pcap file .

```
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"
```

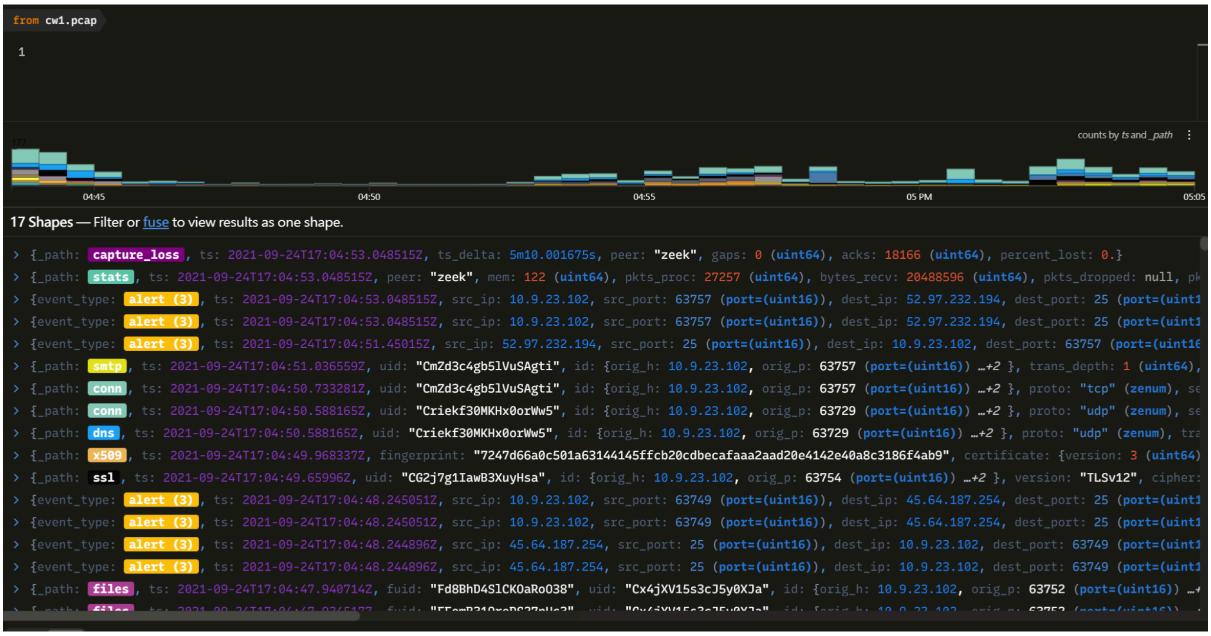
Expression 7. Filtering only the source IP from the user computer, the DNS protocol traffic, and containing “api”

```
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”

ZUI

Second, ZUI is a network forensic tool which provides a GUI interface to analyze and visualize large amounts of network traffic. It was utilized to analyze the CW1.pcap to investigate the network traffic that easily identifies the alert inside the PCAP file. It is similar to the SOC dashboard environment that allows us to filter out the event types of interest.



```
from cw1.pcap
1
```

17 Shapes — Filter or fuse to view results as one shape.

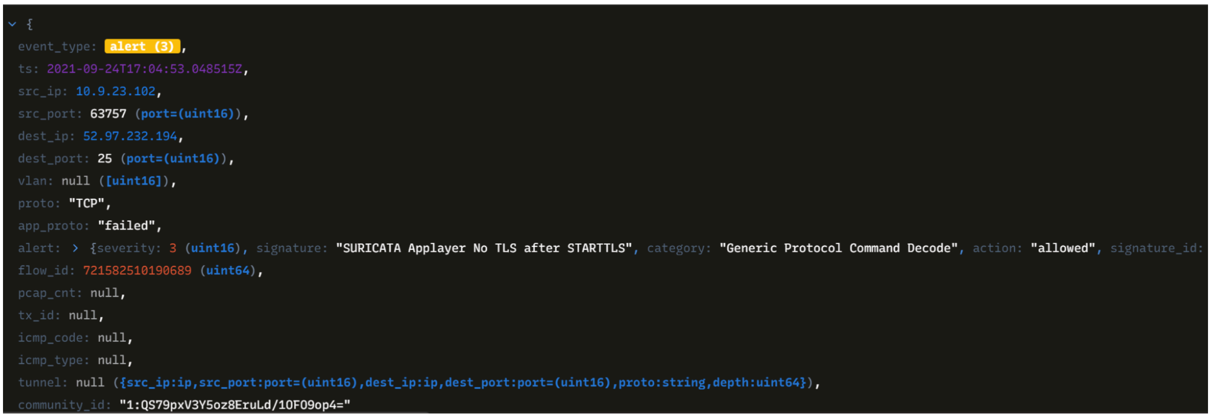
```
> {_path: capture_loss, ts: 2021-09-24T17:04:53.048515Z, ts_delta: 5m10.001675s, peer: "zeek", gaps: 0 (uint64), acks: 18166 (uint64), percent_lost: 0.}
> {_path: stats, ts: 2021-09-24T17:04:53.048515Z, peer: "zeek", mem: 122 (uint64), pkts_proc: 27257 (uint64), bytes_recv: 20488596 (uint64), pkts_dropped: null, pk
> {event_type: alert (3), ts: 2021-09-24T17:04:53.048515Z, src_ip: 10.9.23.102, src_port: 63757 (port=(uint16)), dest_ip: 52.97.232.194, dest_port: 25 (port=(uint1
> {event_type: alert (3), ts: 2021-09-24T17:04:53.048515Z, src_ip: 10.9.23.102, src_port: 63757 (port=(uint16)), dest_ip: 52.97.232.194, dest_port: 25 (port=(uint1
> {event_type: alert (3), ts: 2021-09-24T17:04:51.45015Z, src_ip: 52.97.232.194, src_port: 25 (port=(uint16)), dest_ip: 10.9.23.102, dest_port: 63757 (port=(uint16
> {_path: smtp, ts: 2021-09-24T17:04:51.036559Z, uid: "CmZd3c4gb5lVuSAgti", id: {orig_h: 10.9.23.102, orig_p: 63757 (port=(uint16)) …+2 }, trans_depth: 1 (uint64),
> {_path: conn, ts: 2021-09-24T17:04:50.733281Z, uid: "CmZd3c4gb5lVuSAgti", id: {orig_h: 10.9.23.102, orig_p: 63757 (port=(uint16)) …+2 }, proto: "tcp" (zenum), se
> {_path: conn, ts: 2021-09-24T17:04:50.588165Z, uid: "Criekf30MKHx0orWw5", id: {orig_h: 10.9.23.102, orig_p: 63729 (port=(uint16)) …+2 }, proto: "udp" (zenum), se
> {_path: dns, ts: 2021-09-24T17:04:50.588165Z, uid: "Criekf30MKHx0orWw5", id: {orig_h: 10.9.23.102, orig_p: 63729 (port=(uint16)) …+2 }, proto: "udp" (zenum), tra
> {_path: x509, ts: 2021-09-24T17:04:49.968337Z, fingerprint: "7247d66a0c501a63144145ffcb20cdbecafaaa2aad20e4142e40a8c3186f4ab9", certificate: {version: 3 (uint64)
> {_path: ssl, ts: 2021-09-24T17:04:49.65996Z, uid: "CG2j7g1IawB3XuyHsa", id: {orig_h: 10.9.23.102, orig_p: 63754 (port=(uint16)) …+2 }, version: "TLSv12", cipher:
> {event_type: alert (3), ts: 2021-09-24T17:04:48.245051Z, src_ip: 10.9.23.102, src_port: 63749 (port=(uint16)), dest_ip: 45.64.187.254, dest_port: 25 (port=(uint1
> {event_type: alert (3), ts: 2021-09-24T17:04:48.245051Z, src_ip: 10.9.23.102, src_port: 63749 (port=(uint16)), dest_ip: 45.64.187.254, dest_port: 25 (port=(uint1
> {event_type: alert (3), ts: 2021-09-24T17:04:48.244896Z, src_ip: 45.64.187.254, src_port: 25 (port=(uint16)), dest_ip: 10.9.23.102, dest_port: 63749 (port=(uint1
> {event_type: alert (3), ts: 2021-09-24T17:04:48.244896Z, src_ip: 45.64.187.254, src_port: 25 (port=(uint16)), dest_ip: 10.9.23.102, dest_port: 63749 (port=(uint1
> {_path: files, ts: 2021-09-24T17:04:47.940714Z, fuid: "Fd8BhD4SlCKOaRoO38", uid: "Cx4jXV15s3cJ5y0XJa", id: {orig_h: 10.9.23.102, orig_p: 63752 (port=(uint16)) …+
```

ZUI Screenshot 1. Activity overview

The preloaded query.json from brimcap in github was used in the analysis of pcap. We could try to analyze the alert event with the below query.

```
event_type=="alert"
```

Expression 9. Filter only alert events



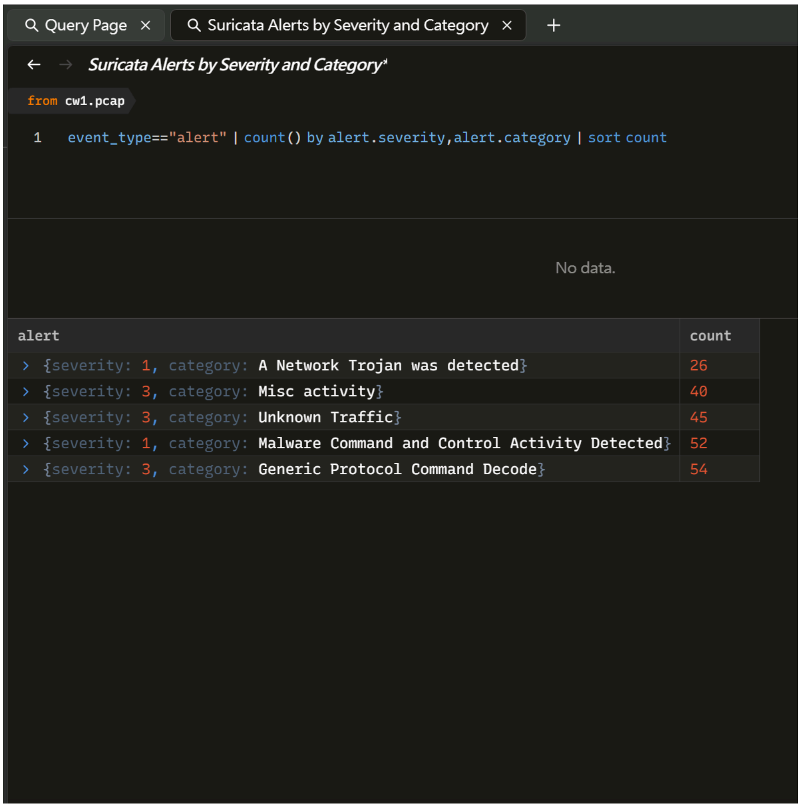
```
⌄ {
  event_type: alert (3),
  ts: 2021-09-24T17:04:53.048515Z,
  src_ip: 10.9.23.102,
  src_port: 63757 (port=(uint16)),
  dest_ip: 52.97.232.194,
  dest_port: 25 (port=(uint16)),
  vlan: null ([uint16]),
  proto: "TCP",
  app_proto: "failed",
  alert: › {severity: 3 (uint16), signature: "SURICATA Applayer No TLS after STARTTLS", category: "Generic Protocol Command Decode", action: "allowed", signature_id:
  flow_id: 721582510190689 (uint64),
  pcap_cnt: null,
  tx_id: null,
  icmp_code: null,
  icmp_type: null,
  tunnel: null ({src_ip:ip,src_port:port=(uint16),dest_ip:ip,dest_port:port=(uint16),proto:string,depth:uint64}),
  community_id: "1:QS79pxV3Y5oz8EruLd/1OFO9op4="
```

ZUI Screenshot 2. One of the details in alert events

For alert triage, the key attributes are the ones that uniquely identify the rule, describe the involved network session, and allow correlation to other logs. There are some key attributes that can analysis alert events, such as timestamp, src_ip, src_port, dest_ip, dest_port, proto, app_proto, alert.signature, alert.signature_id, alert.category and alert.severity.

Section 3 – Results

After the investigation, we found that the victim host was infected after downloading a ZIP file from a suspicious website. That ZIP contained a malicious Excel file. Shortly after, the host began beaconing to attacker-controlled infrastructure (C2) and later started sending large volumes of phishing/spam emails directly to many SMTP servers (port 25), including messages with a malicious ZIP attachment. From ZUI, we can identify the possible or potential attack that the victim is dealing with. In Zui Screenshot 3 showed the attack could be network trojan or malware activity.


Query Page
Suricata Alerts by Severity and Category
Suricata Alerts by Severity and Category*
No data.

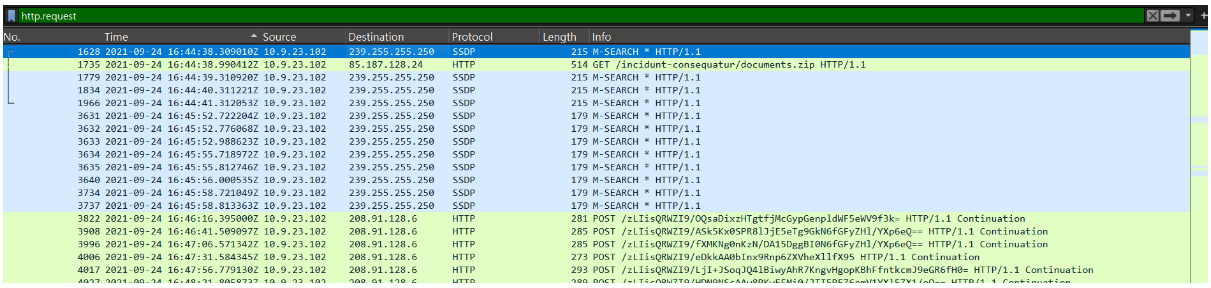
```
from cw1.pcap
event_type=="alert" | count() by alert.severity,alert.category | sort count
```

alert	count
{severity: 1, category: A Network Trojan was detected}	26
{severity: 3, category: Misc activity}	40
{severity: 3, category: Unknown Traffic}	45
{severity: 1, category: Malware Command and Control Activity Detected}	52
{severity: 3, category: Generic Protocol Command Decode}	54

ZUI Screenshot 3. Suricata Alerts by Severity and Category

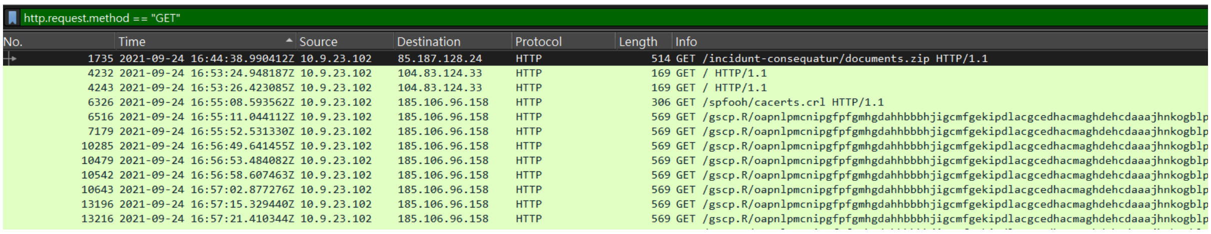
Infected system identification: The compromised host is the primary internal client observed initiating the earliest suspicious HTTP download and subsequent repeated C2 communications. Key identifiers captured include IP address, MAC address (from ARP/Ethernet headers), and hostname/user context from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



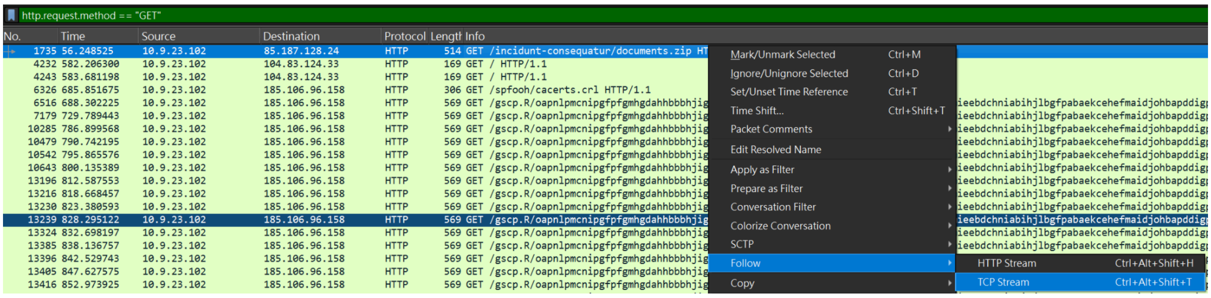
```
http.request
No.     Time                         Source       Destination      Protocol  Length Info
   1628 2021-09-24 16:44:38.309010Z 10.9.23.102  239.255.255.250  SSDP       215 M-SEARCH * HTTP/1.1
   1735 2021-09-24 16:44:38.990412Z 10.9.23.102  85.187.128.24    HTTP       514 GET /incidunt-consequatur/documents.zip 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
   4027 2021-09-24 16:48:21.805873Z 10.9.23.102  208.91.128.6     HTTP       289 POST
```

Figure 1. First HTTP request



```
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
```

Figure 2. HTTP GET request that discovers document.zip

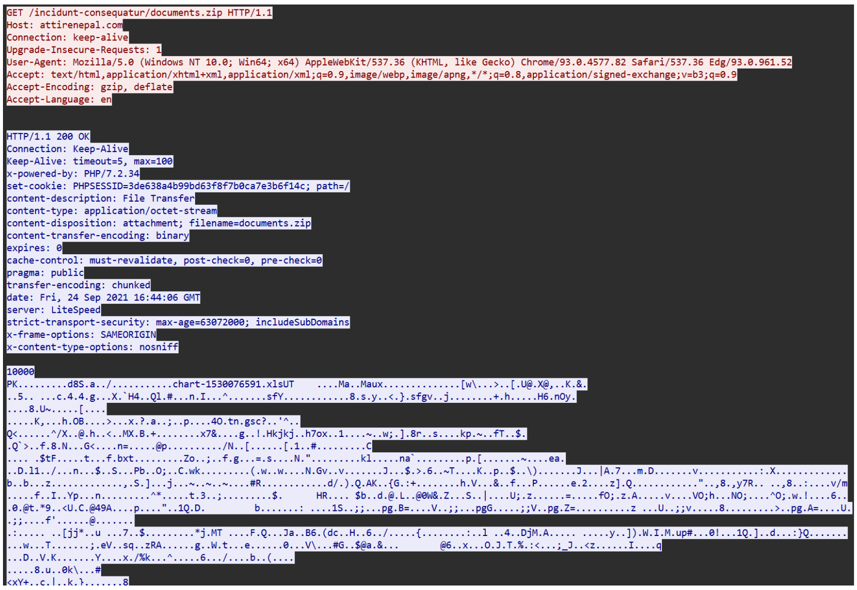


```
http.request.method == "GET"
No.    Time        Source       Destination     Protocol Length Info
  1735 56.248525   10.9.23.102  85.187.128.24   HTTP     514 GET /incidunt-consequatur/documents.zip HT
  4232 582.206300  10.9.23.102  104.83.124.33   HTTP     169 GET / HTTP/1.1
  4243 583.681198  10.9.23.102  104.83.124.33   HTTP     169 GET / HTTP/1.1
  6326 685.851675  10.9.23.102  185.106.96.158  HTTP     306 GET /spfooh/cacerts.crl HTTP/1.1
  6516 688.302225  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
  7179 729.789443  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 10285 786.899568  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 10479 790.742195  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 10542 795.865576  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 10643 800.135389  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13196 812.587553  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13216 818.668457  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13230 823.380593  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13239 828.295122  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13324 832.698197  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13385 838.136757  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig   ieebdchniabihjlbgfpabaekcehefmaidjohbapddig
 13396 842.529743  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig
 13405 847.627575  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig
 13416 852.973925  10.9.23.102  185.106.96.158  HTTP     569 GET /gscp.R/oapnlpmcnipgfpfgmhgdahhbbbhjig
```

Mark/Unmark Selected Ctrl+M
Ignore/Unignore Selected Ctrl+D
Set/Unset Time Reference Ctrl+T
Time Shift... Ctrl+Shift+T
Packet Comments
Edit Resolved Name
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize Conversation
SCTP
Follow
Copy
HTTP Stream Ctrl+Alt+Shift+H
TCP Stream Ctrl+Alt+Shift+T

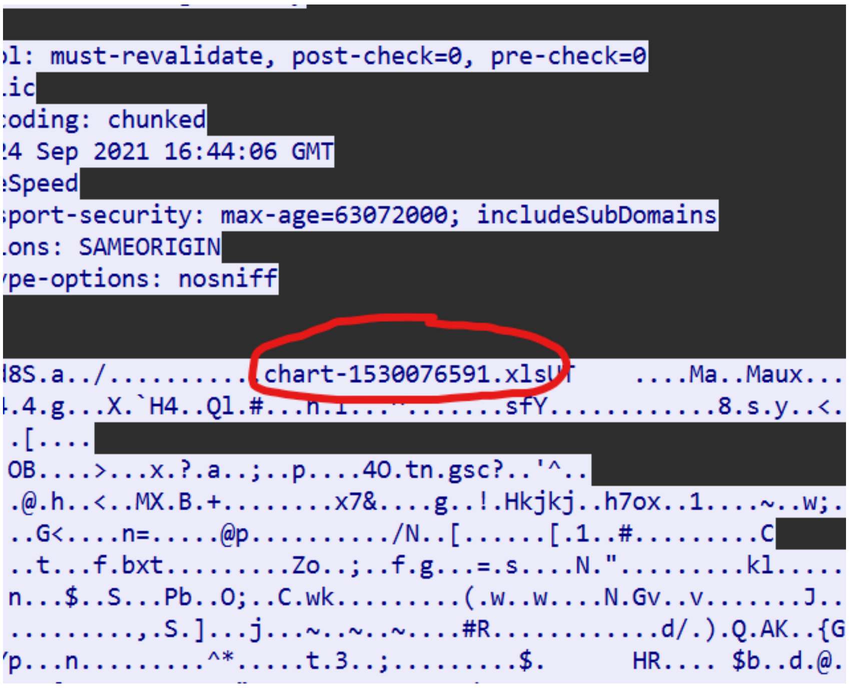
Figure 3. Select TCP Stream to view the dedicated traffic from GET /incidunt-consequatur/documents.zip HTTP/1.1

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.



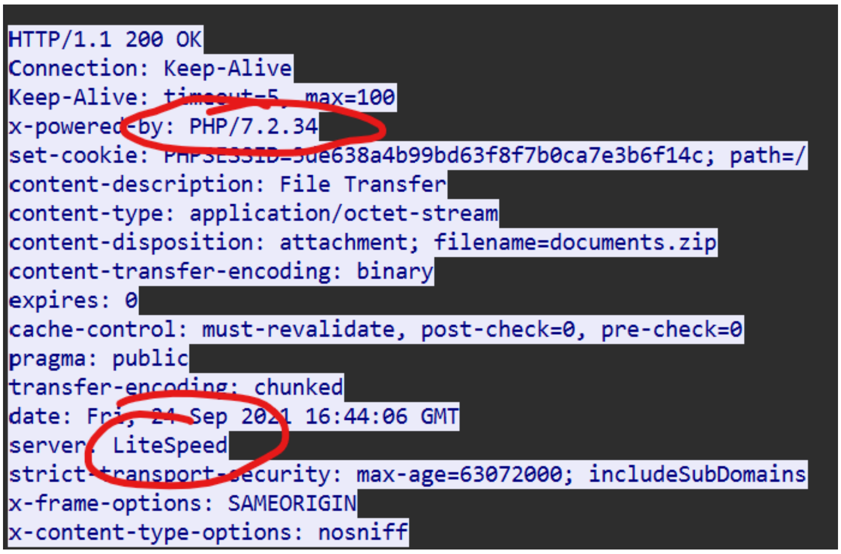
```
GET /incidunt-consequatur/documents.zip HTTP/1.1
Host: attirenepal.com
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safari/537.36 Edg/93.0.961.52
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,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=3de638a4b99bd63f8f7b0ca7e3b6f14c; 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.&.
..5.. ...c.4.4.g...X.`H4..Ql.#...n.I...^.......sfY...........8.s.y..<.}.sfgv..j........+.h.....H6.nOy.
....8.U~.....[....
.....K,...h.OB....>...x.?.a..;..p....4O.tn.gsc?..'^..
Q<......^/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.[.......~....ea.
..D.l1../...n...$..S...Pb..O;..C.wk.........(.w..w....N.Gv..v.......J...$.>.6..~T....K..p..$..\).......J...|A.7...m.D.......v...........:.X.............
b..b...z.............,.S.]...j...~..~..~....#R............d/.).Q.AK..{G.:+........h.V...&..f...P......e.2....z].Q..........."..,8.,y7R.. ..,8..:....v/m
.....f..I..Yp...n.........^*.....t.3..;.........$.      HR.... $b..d.@.L..@0W&.Z...S..|....U;.z......=.....fO;.z.A.....v....VO;h...NO;....^O;.w.!....6..
.0.@t.*9..<U.C.@49A....p...."..1Q.D.        b.......: ....1S..;;...pg.B=....V..;;...pgG.....;;V..pg.Z=..........z ...U..;;v.....8.........>..pg.A=....U.
.;;....f'......@.......
.:..... ..[jj*..u ...7..$.........*j.MT ....F.Q...Ja..B6.(dc..H..6../.....{........:..l ..4..DjM.A..... .....y..]).W.I.M.up#...0!...1Q.]..d...:}Q.......
...w...T.......;.eV..sq..zRA......g..W.t...e......0...V\...#G..$@a.&...       @6..x...O.J.T.%.:<...;_J..<z......I....q
...D..V.K.......Y....x./%k...^.....6.../....b..(....
.....8.u..0k\...#
<xY+..c.|..k.}.......8
```

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



```
l: must-revalidate, post-check=0, pre-check=0
ic
oding: chunked
4 Sep 2021 16:44:06 GMT
Speed
port-security: max-age=63072000; includeSubDomains
ons: SAMEORIGIN
pe-options: nosniff

8S.a../..........chart-1530076591.xlsUT    ....Ma..Maux...
.4.g...X.`H4..Ql.#...n.I...^.......sfY...........8.s.y..<.
.[....
OB....>...x.?.a..;..p....4O.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."........kl.....
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.@.
```

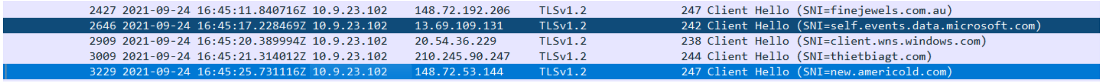
Figure 5. chart-1530076591.xls inside the stream



```
HTTP/1.1 200 OK
Connection: Keep-Alive
Keep-Alive: timeout=5, max=100
x-powered-by: PHP/7.2.34
set-cookie: PHPSESSID=3de638a4b99bd63f8f7b0ca7e3b6f14c; 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
```

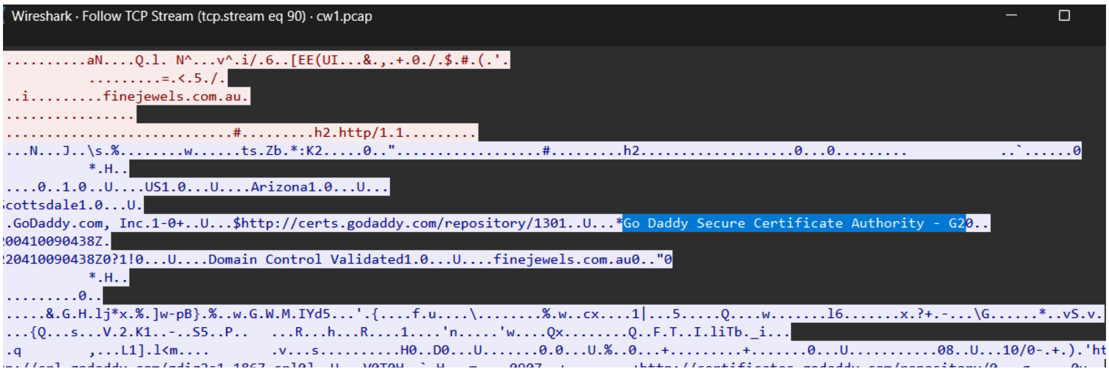
Figure 6. Web server and version

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.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)
```

Figure 7. DNS traffic



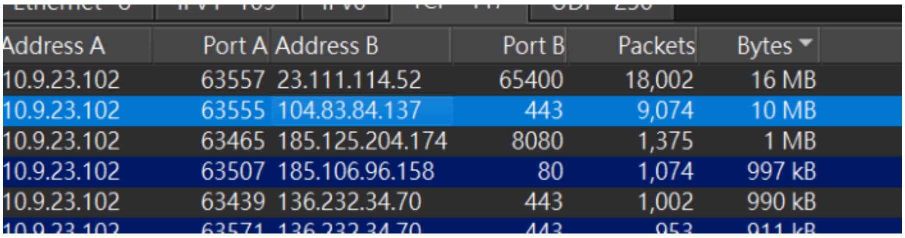
```
..........aN....Q.l. N^...v^.i/.6..[EE(UI...&.,.+.0./.$.#.(.'.
          .........=.<.5./.
..i.........finejewels.com.au.
................
...........................#.........h2.http/1.1.........
...N...J..\s.%........w......ts.Zb.*:K2.....0.."..................#.........h2..................0...0.........          ..`......0
          *.H..
....0..1.0..U....US1.0...U....Arizona1.0...U...
;cottsdale1.0...U.
.GoDaddy.com, Inc.1-0+..U...$http://certs.godaddy.com/repository/1301..U...*Go Daddy Secure Certificate Authority - G20..
:00410090438Z.
:20410090438Z0?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
```

Figure 8. CA issuer

Suspected C2 infrastructure consistent: 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).

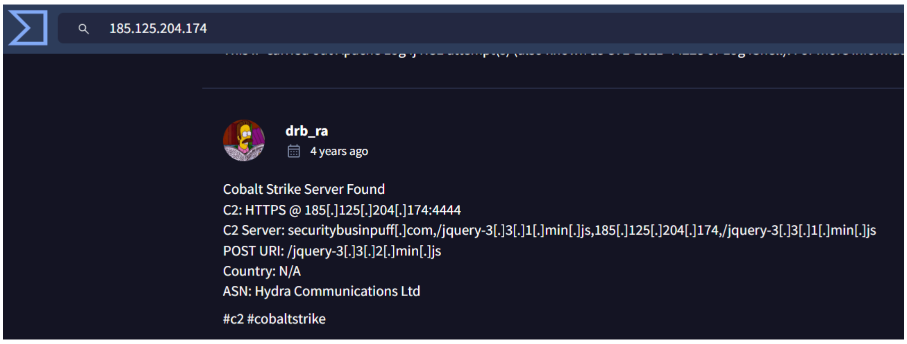
DNS analysis linked **185.106.96.158** (Port 80) to **survmeter.live** (Figure 12), and the Host/SNI value observed for this infrastructure was **ocsp.verisign.com** (Figure 13).

For **185.125.204.174**, HTTP POST traffic revealed an association with **securitybusinpuff.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



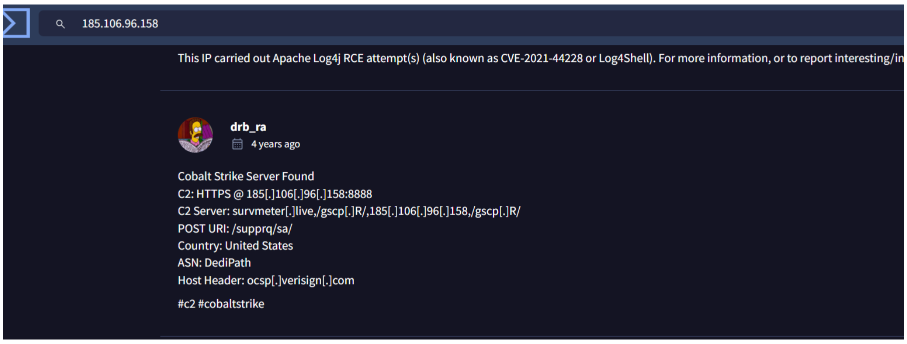
185.125.204.174

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

Figure 10. Virustotal review (1)



185.106.96.158

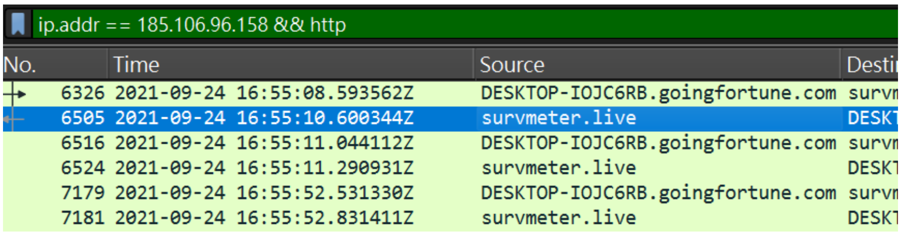
This IP carried out Apache Log4j RCE attempt(s) (also known as CVE-2021-44228 or Log4Shell). For more information, or to report interesting/in

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

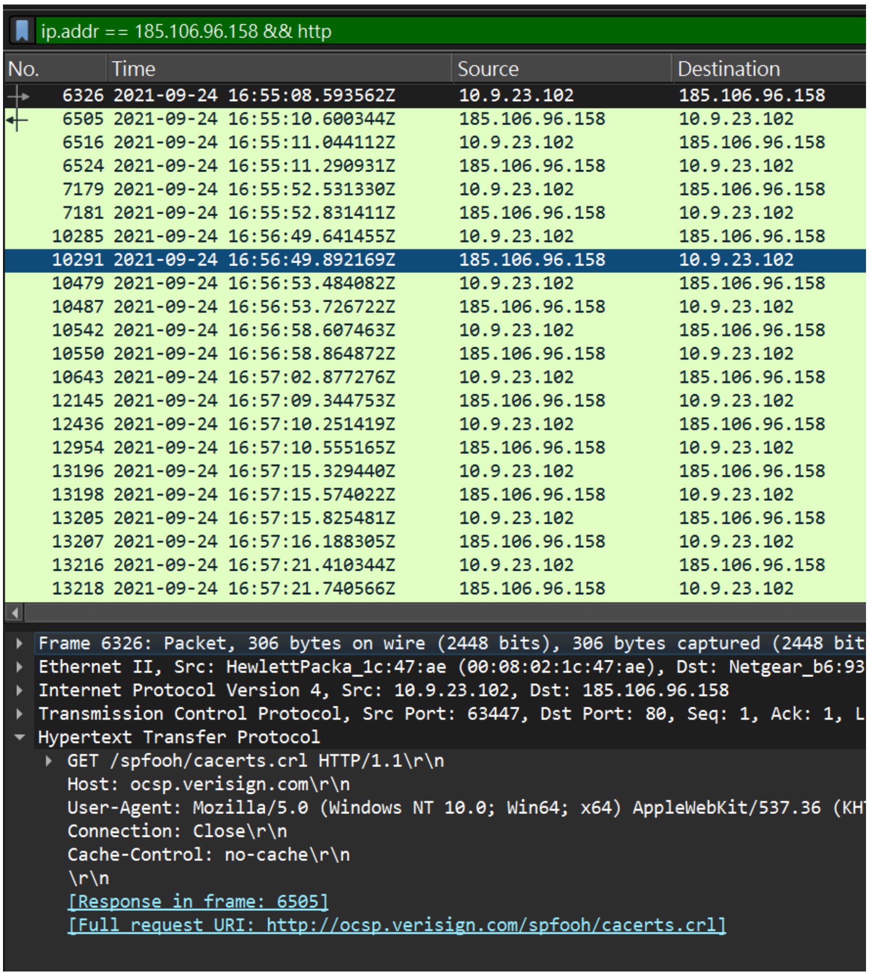
#c2 #cobaltstrike

Figure 11. Virustotal review (2)



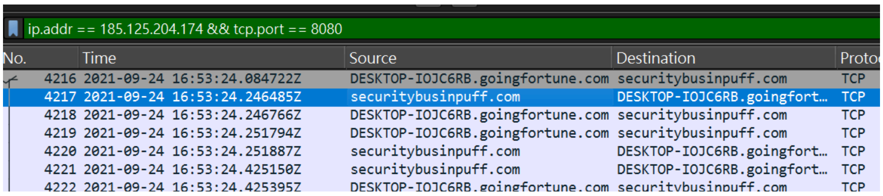
```
ip.addr == 185.106.96.158 && http
No.   Time                           Source                             Desti
6326 2021-09-24 16:55:08.593562Z    DESKTOP-IOJC6RB.goingfortune.com   survm
6505 2021-09-24 16:55:10.600344Z    survmeter.live                     DESKT
6516 2021-09-24 16:55:11.044112Z    DESKTOP-IOJC6RB.goingfortune.com   survm
6524 2021-09-24 16:55:11.290931Z    survmeter.live                     DESKT
7179 2021-09-24 16:55:52.531330Z    DESKTOP-IOJC6RB.goingfortune.com   survm
7181 2021-09-24 16:55:52.831411Z    survmeter.live                     DESKT
```

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: ocsp.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]
```

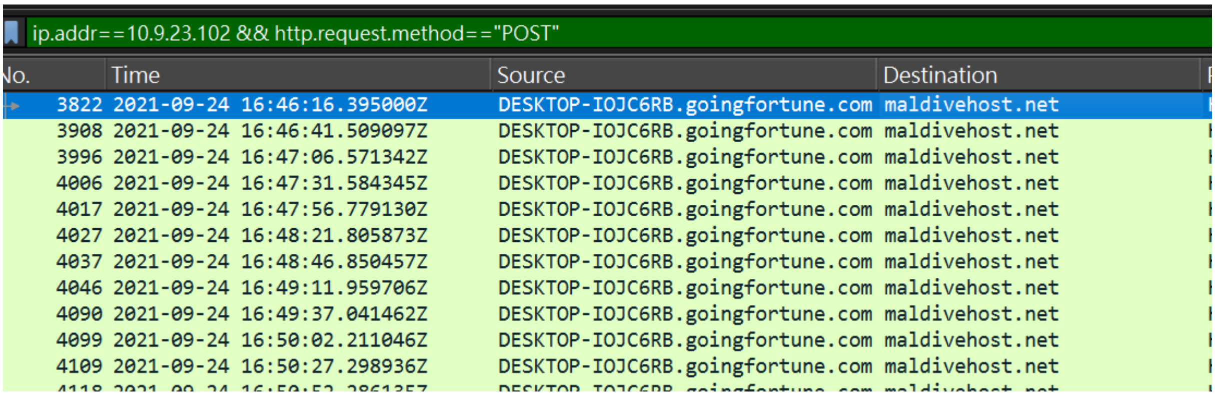
Figure 13. Request URL for 185.106.96.158



```
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   securitybusinpuff.com          TCP
4217 2021-09-24 16:53:24.246485Z    securitybusinpuff.com              DESKTOP-IOJC6RB.goingfort…     TCP
4218 2021-09-24 16:53:24.246766Z    DESKTOP-IOJC6RB.goingfortune.com   securitybusinpuff.com          TCP
4219 2021-09-24 16:53:24.251794Z    DESKTOP-IOJC6RB.goingfortune.com   securitybusinpuff.com          TCP
4220 2021-09-24 16:53:24.251887Z    securitybusinpuff.com              DESKTOP-IOJC6RB.goingfort…     TCP
4221 2021-09-24 16:53:24.425150Z    securitybusinpuff.com              DESKTOP-IOJC6RB.goingfort…     TCP
4222 2021-09-24 16:53:24.425395Z    DESKTOP-IOJC6RB.goingfortune.com   securitybusinpuff.com          TCP
```

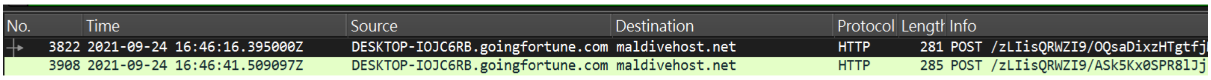
Figure 14. Domain linked to 185.125.204.174

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.



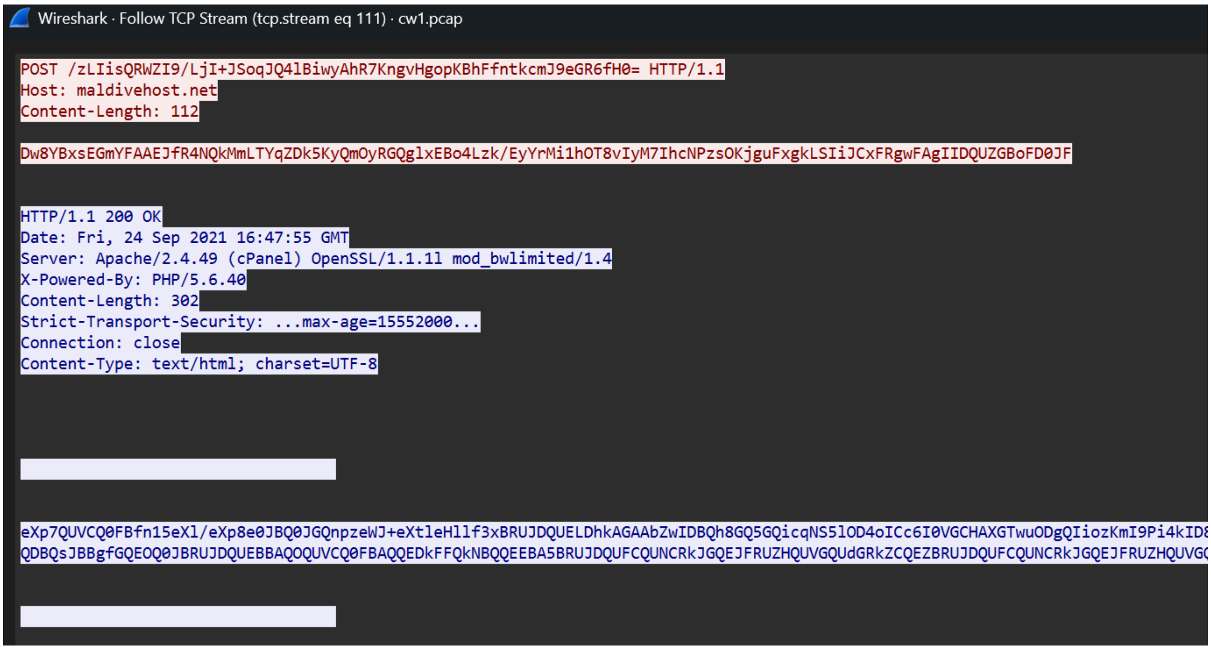
```
ip.addr==10.9.23.102 && http.request.method=="POST"

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 16:50:52.286135Z  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/ASk5Kx0SPR8lJj
```

Figure 16. Post-infection beaconing traffic

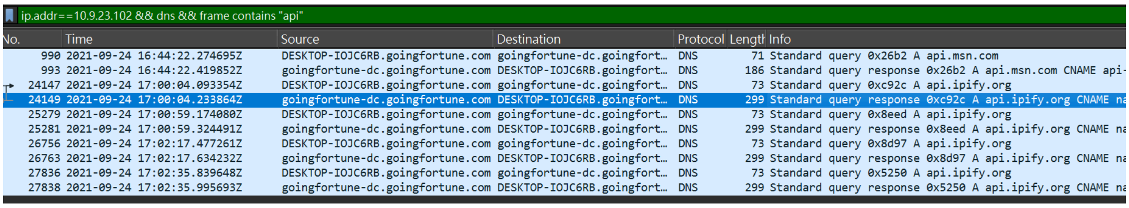


Wireshark · Follow TCP Stream (tcp.stream eq 111) · cw1.pcap

```
POST /zLIisQRWZI9/LjI+JSoqJQ4lBiwyAhR7KngvHgopKBhFfntkcmJ9eGR6fH0= HTTP/1.1
Host: maldivehost.net
Content-Length: 112

Dw8YBxsEGmYFAAEJfR4NQkMmLTYqZDk5KyQmOyRGQglxEBo4Lzk/EyYrMi1hOT8vIyM7IhcNPzsOKjguFxgkLSIiJCxFRgwFAgIIDQUZGBoFD0JF


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+eXtleHllf3xBRUJDQUELDhkAGAAbZwIDBQh8GQ5GQicqNS5lOD4oICc6I0VGCHAXGTwuODgQIiozKmI9Pi4kID8
QDBQsJBBgfGQEOQ0JBRUJDQUEBBAQOQUVCQ0FBAQQEDkFFQkNBQQEEBA5BRUJDQUFCQUNCRkJGQEJFRUZHQUVGQUdGRkZCQEZBRUJDQUFCQUNCRkJGQEJFRUZHQUVGQ
```

Figure 17. Server header

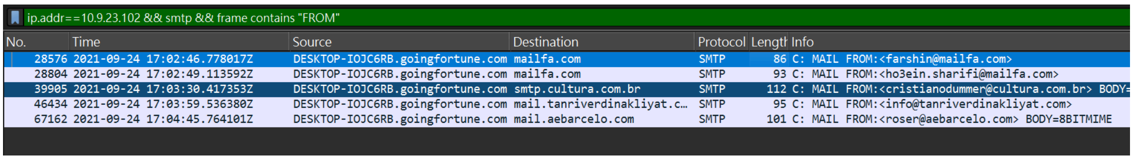
Final exfiltration/check-in: The malware performed an external IP check via DNS at **2021-09-24 17:00:04**, querying **api.ipify.org** (Figure 18). SMTP traffic showed the first MAIL FROM address as **farshin@mailfa.com** (Figure 19). Following the same TCP stream, the password was transmitted using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



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

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 17:00:04.233864Z	goingfortune-dc.goingfortune.com	DESKTOP-IOJC6RB.goingfort…	DNS	299	Standard query response 0xc92c A api.ipify.org CNAME na
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 na
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 na
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 na

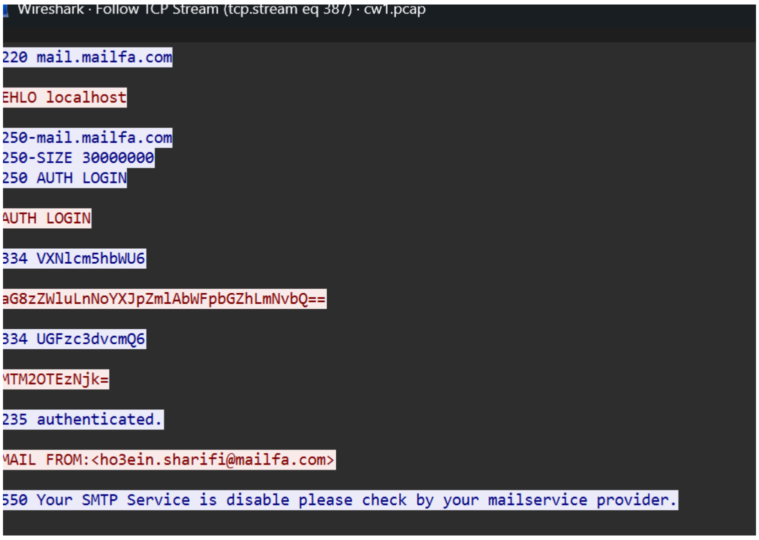
Figure 18. A DNS query occurred for the domain used by the malware



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

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>
39905	2021-09-24 17:03:30.417353Z	DESKTOP-IOJC6RB.goingfortune.com	smtp.cultura.com.br	SMTP	112	C: MAIL FROM:<cristianodummer@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@aebarcelo.com> BODY=8BITMIME

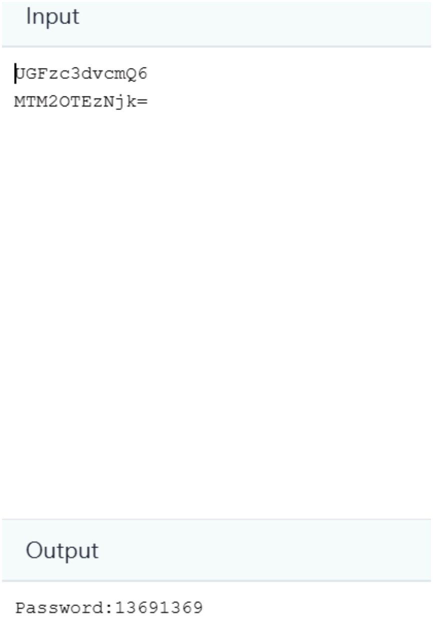
Figure 19. SMTP traffic



Wireshark · Follow TCP Stream (tcp.stream eq 387) · cw1.pcap

```
220 mail.mailfa.com

EHLO localhost

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

AUTH LOGIN

334 VXNlcm5hbWU6

aG8zZWluLnNoYXJpZmlAbWFpbGZhLmNvbQ==

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



```
UGFzc3dvcmQ6
MTM2OTEzNjk=
```

```
Password:13691369
```

Figure 21. BASE64 decryption

Section 4 – Conclusion and References

This investigation identified the compromised host (10.9.23.102) and reconstructed the infection lifecycle observed in the PCAP. The incident began with the download of a malicious compressed archive containing an Excel file, which likely acted as the initial execution vector. The host subsequently established persistent command-and-control communication through HTTP POST beaconing and encrypted TLS connections, performed external IP discovery, and later initiated outbound SMTP authentication attempts, indicating that the system was repurposed for malspam or phishing activity.

To mitigate similar incidents, organisations should enforce web and email filtering to block malicious domains and compressed attachments, disable macro execution by default, and apply egress filtering to detect abnormal outbound connections. DNS monitoring and restricting outbound SMTP traffic to authorised mail servers can further reduce the impact of compromised hosts. However, encrypted C2 traffic and the abuse of legitimate services remain key challenges, highlighting the need for layered security controls and continuous network monitoring.

Attack Stage	Evidence Observed	Targeted Prevention
Initial Access	HTTP download of ZIP	Web proxy + file-type blocking + Phishing protection + Firewall/Anti-virus
Execution	XLS macro payload	Disable Office macros by default
C2	Obfuscated POST beacons	Egress filtering + TLS inspection
Recon	api.ipify.org lookup	DNS anomaly detection
Impact	SMTP spam	Outbound SMTP restrictions

Table 1. Mapping of observed attack stages to preventative controls

References

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/

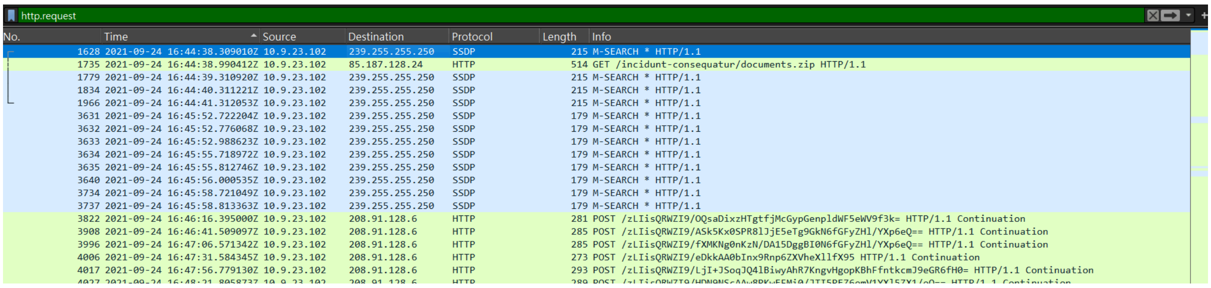
3. Brim Data. (2026). ZUI GitHub. https://github.com/brimdata/zui

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
```

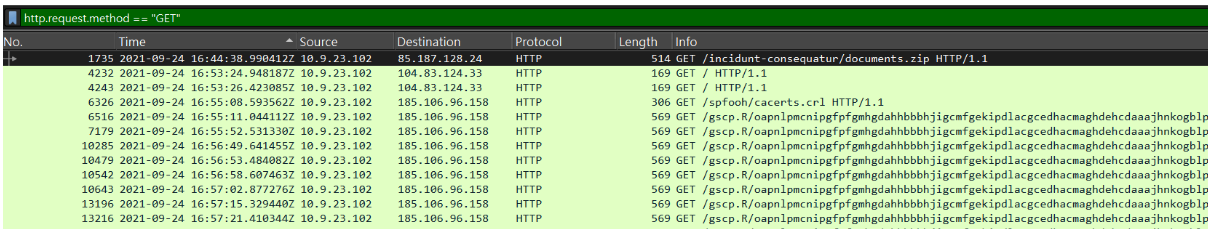
1735 2021-09-24 16:44:38.990412Z 10.9.23.102 85.187.128.24 HTTP 514 GET /incidunt-consequatur/documents.zip HTTP/1.1

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

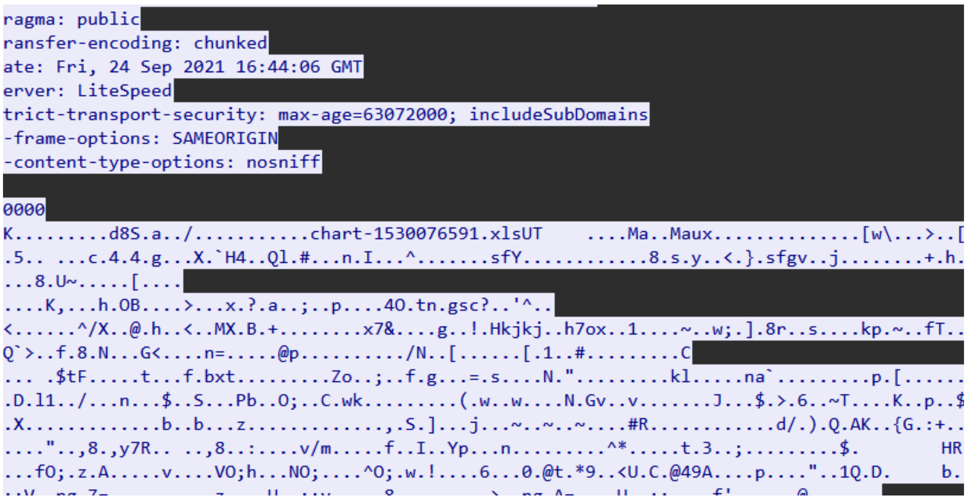
3. Which domain hosted the malicious compressed file?

Ans:

attirenepal.com

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

Ans:

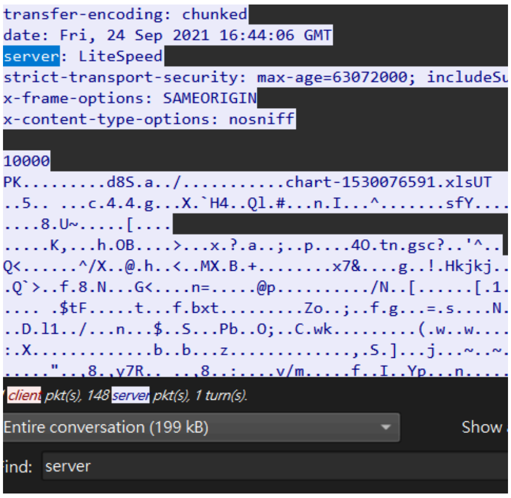


```
ragma: public
ransfer-encoding: chunked
ate: Fri, 24 Sep 2021 16:44:06 GMT
erver: LiteSpeed
trict-transport-security: max-age=63072000; includeSubDomains
-frame-options: SAMEORIGIN
-content-type-options: nosniff

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).
Entire conversation (199 kB)
Show
ind: server

LiteSpeed

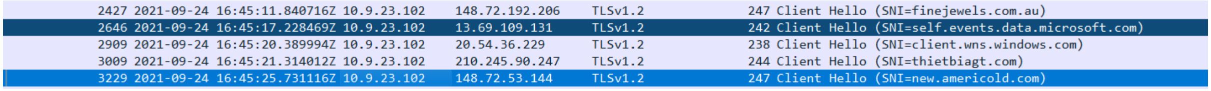
6. What is the version number of the web server identified in the previous question?

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.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

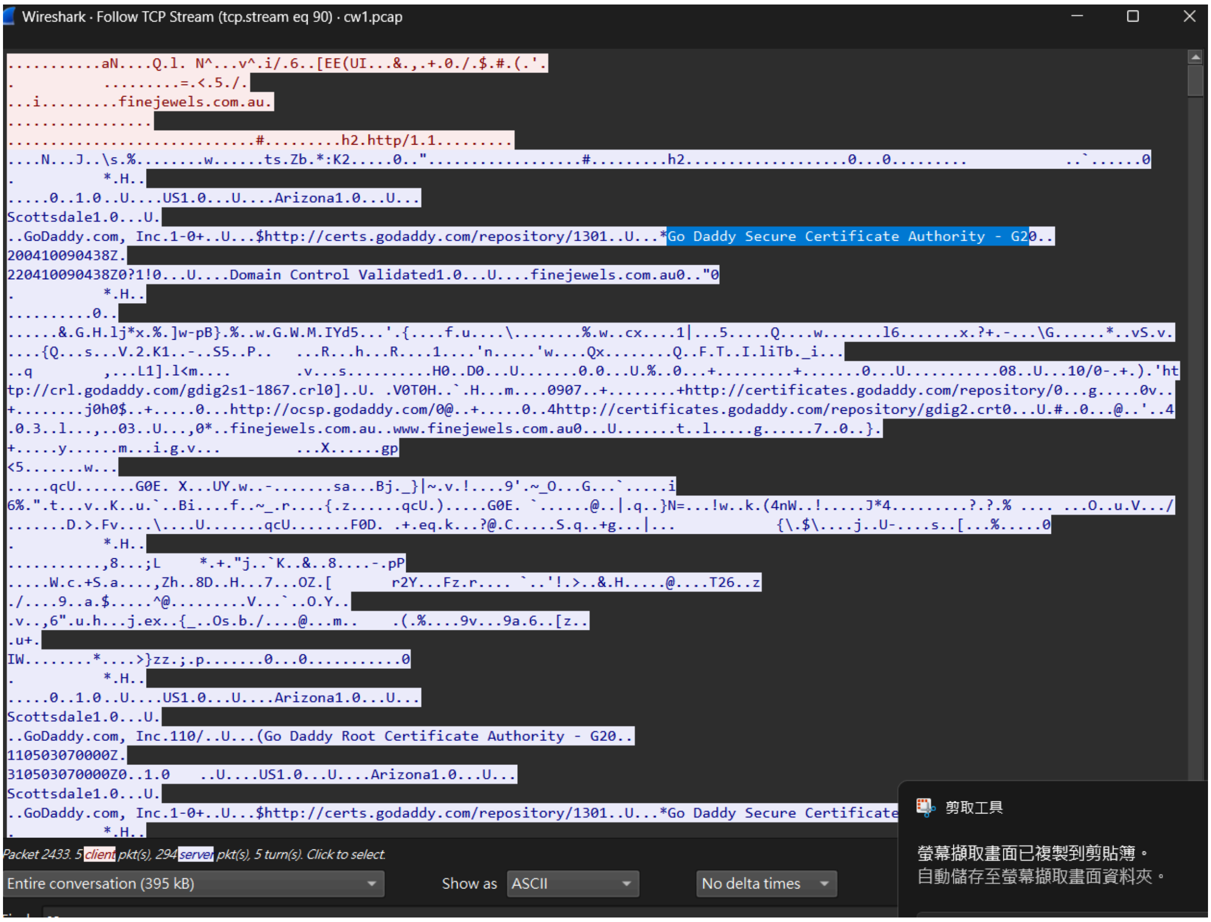
thietbiagt.com

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.lj*x.%.]w-pB}.%..w.G.W.M.IYd5...'.{....f.u....\........%.w..cx....1|...5.....Q....w.......l6.......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

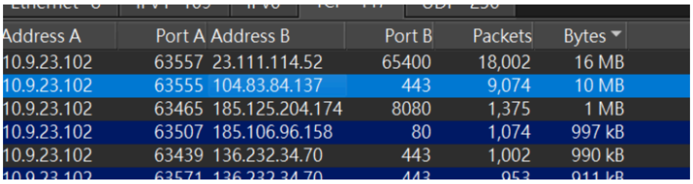
螢幕擷取畫面已複製到剪貼簿。
自動儲存至螢幕擷取畫面資料夾。

GoDaddy

9. What are the two IP addresses of the Cobalt Strike servers? (Provide them in sequential order).

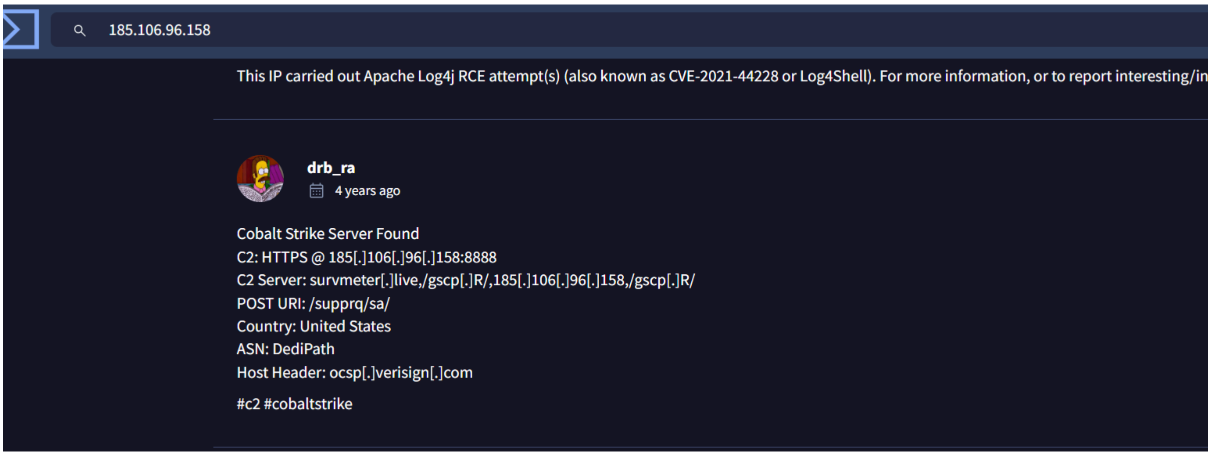
Hint: Inspect the Conversations menu option

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



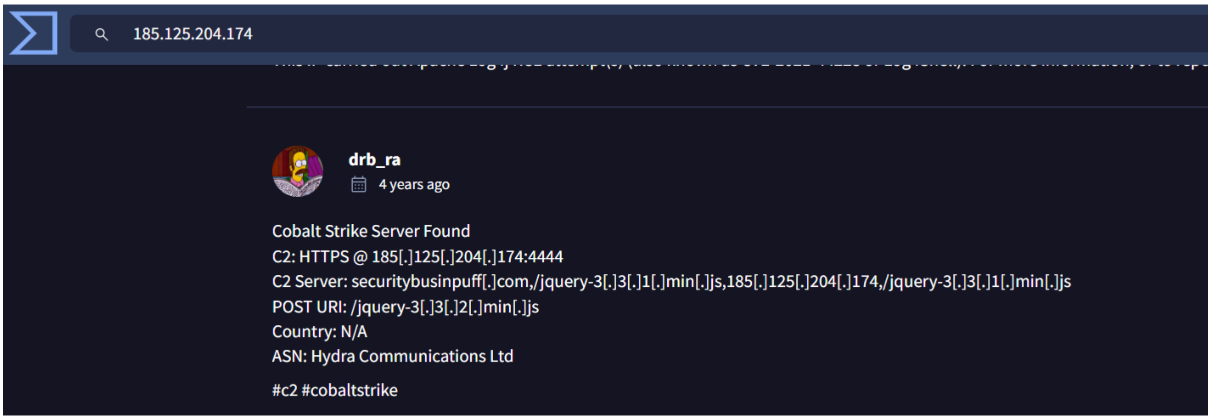
185.106.96.158

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**

Run below query will get the clear detail of alert event:

```
event_type==”alert” | cut
ts,src_ip,dest_ip,dest_port,flow_id,alert.signature,alert.severity
,alert.category | sort -r ts
```

The result can be found on github repository (https://github.com/aka331/COMP3010HK/blob/main/CW1/event_alert.csv)

Timeline (key events with exact times)

All times are from the PCAP timestamps.

1. **Initial download (infection vector)**

- **16:44:38.990** — Victim downloads a ZIP over HTTP:
  GET /incidunt-consequatur/documents.zip from **attirenepal.com** (IP: **85.187.128.24**)

Extracted that file from the PCAP and it contains:

- chart-1530076591.xls (inside documents.zip)

This is a classic pattern: **ZIP → Excel lure → macro/dropper execution**.

2. **First C2 / malware check-in**

- **16:46:16.395** — Victim starts POST beacons to **maldivehost.net** (IP: **208.91.128.6**) with highly obfuscated URI paths like:
  POST /zLIisQRWZI9/<base64-ish blob>

This looks like **malware C2 polling / tasking**.

3. **Second C2 channel over TLS**

- **16:53:28.188** — Victim initiates TLS sessions to **185.125.204.174:8080** with SNI:
  securitybusinpuff.com
  Certificate chain shows **Let’s Encrypt (R3)**, which is common for attacker infrastructure too.

4. **External IP discovery**

- **17:00:04.093** — DNS query for **api.ipify.org**
  This is often used by malware to learn the victim's **public IP**.

5. **Botnet spamming / phishing begins**

- **17:02:43.150** — Clear SMTP commands observed from victim to external mail servers (port **25**), e.g. EHLO localhost
- The victim then performs many SMTP deliveries to different domains/servers (direct-to-MX behavior).

The victim host (10.9.23.102) became infected and began communicating with a known malware loader infrastructure. ZUI/Suricata generated repeated "ET MALWARE SQUIRRELWAFFLE Loader Activity (POST)" alerts for HTTP POST beacons to 208.91.128.6 starting at 16:46Z, followed by "SQUIRRELWAFFLE Server Response" alerts indicating successful C2 responses. Shortly after, the host initiated multiple TLS sessions that matched an "ET JA3 Hash – Possible Dridex" fingerprint (including traffic to 185.125.204.174:8080 and 136.232.34.70:443), suggesting a second-stage bot/trojan component. The host then performed external IP discovery via api.ipify.org. Finally, SMTP anomalies and email-delivery behavior indicate the compromised machine was used to send malspam/phishing emails (often via direct SMTP to external servers), consistent with botnet/spambot activity.

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.

Solo Work	**S1 - Generative AI tools have not been used for this assessment.**	□
Assisted Work	**A1 – Idea Generation and Problem Exploration** 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.	□
	A2 - Planning & Structuring Projects AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student's own work.	□
	A3 – Code Architecture 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.	□
	A4 – Research Assistance 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.	
	A5 - Language Refinement 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.	☐
	A6 – Code Review 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.	☐
	A7 - Code Generation for Learning Purposes 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.	☐
	A8 - Technical Guidance & Debugging Support 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.	☐
	A9 - Testing and Validation Support 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.	
	A10 - Data Analysis and Visualization Guidance 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.	☐
	A11 - Other uses not listed above Please specify:	☐
Partnered Work	**P1 - Generative AI tool usage has been used integrally for this assessment** Students can adopt approaches that are compliant with instructions in the assessment brief. Please Specify: - The analysis of the pcap file to verify the answer of founding - README.md - report drafting and improvement - generate suggested expression in Wireshark	☒

Please provide details of AI usage and which elements of the coursework this relates to:

improve the report, pcap analysis

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	☒
I confirm that all details provide above are an accurate description of how AI was used for this assessment.	☒