

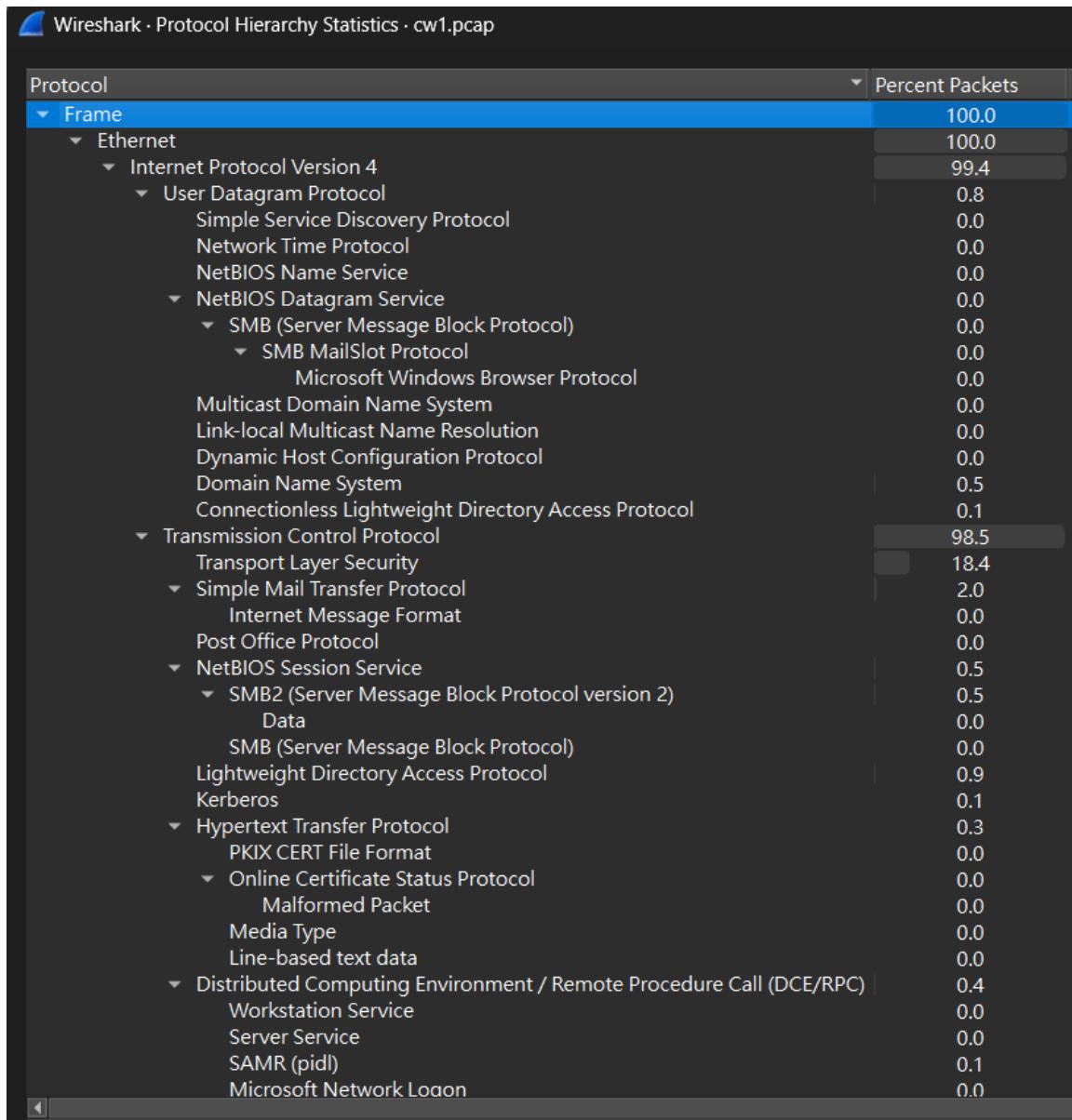
## Incident Report: Malicious Network Traffic Analysis

**Section 1 – Introduction** This incident report documents a comprehensive forensic investigation into suspicious network activity captured in the file cw1.pcap. The analysis was initiated following an endpoint security alert indicating unusual outbound connections from an internal Windows workstation shortly after a user opened an attachment. As a security analyst, the primary objectives were to identify the compromised system, trace the infection vector, classify the malware family, reconstruct the attack chain, and provide actionable recommendations to prevent recurrence.

The investigation leveraged 20 targeted quiz questions that systematically guided the discovery of key indicators of compromise (IOCs), including malicious domains, IP addresses, payloads, command-and-control (C2) infrastructure, and exfiltration attempts. Wireshark served as the core analysis platform, supplemented by manual packet dissection, protocol decoding, and external IOC validation via VirusTotal. The report is structured as follows: methodology (tools, techniques, and step-by-step process), results (detailed findings with evidence), and conclusion (lessons learned and prevention strategies). All timestamps are in UTC unless otherwise stated.

**Section 2 – Methodology** The analysis was performed using **Wireshark** (stable release) as the primary tool due to its powerful filtering engine, protocol dissectors, stream reconstruction, Conversations statistics, and HTTP object export capabilities. No additional commercial tools were required, ensuring reproducibility in resource-constrained environments. The investigative process followed a structured, repeatable approach aligned with NIST SP 800-86 (Guide to Integrating Forensic Techniques into Incident Response):

1. **Initial Triage and Scope Definition** Opened cw1.pcap and reviewed Statistics > Protocol Hierarchy to identify dominant protocols: TCP (majority), HTTP, TLS/HTTPS, DNS, and SMTP. Filtered on the suspected victim IP ip.src == 10.9.23.102 (private 10.0.0.0/8 range) and confirmed the endpoint MAC address 00:08:02:1c:47:ae (Hewlett Packard) as the consistent source of malicious traffic.



### Protocol Hierarchy

```

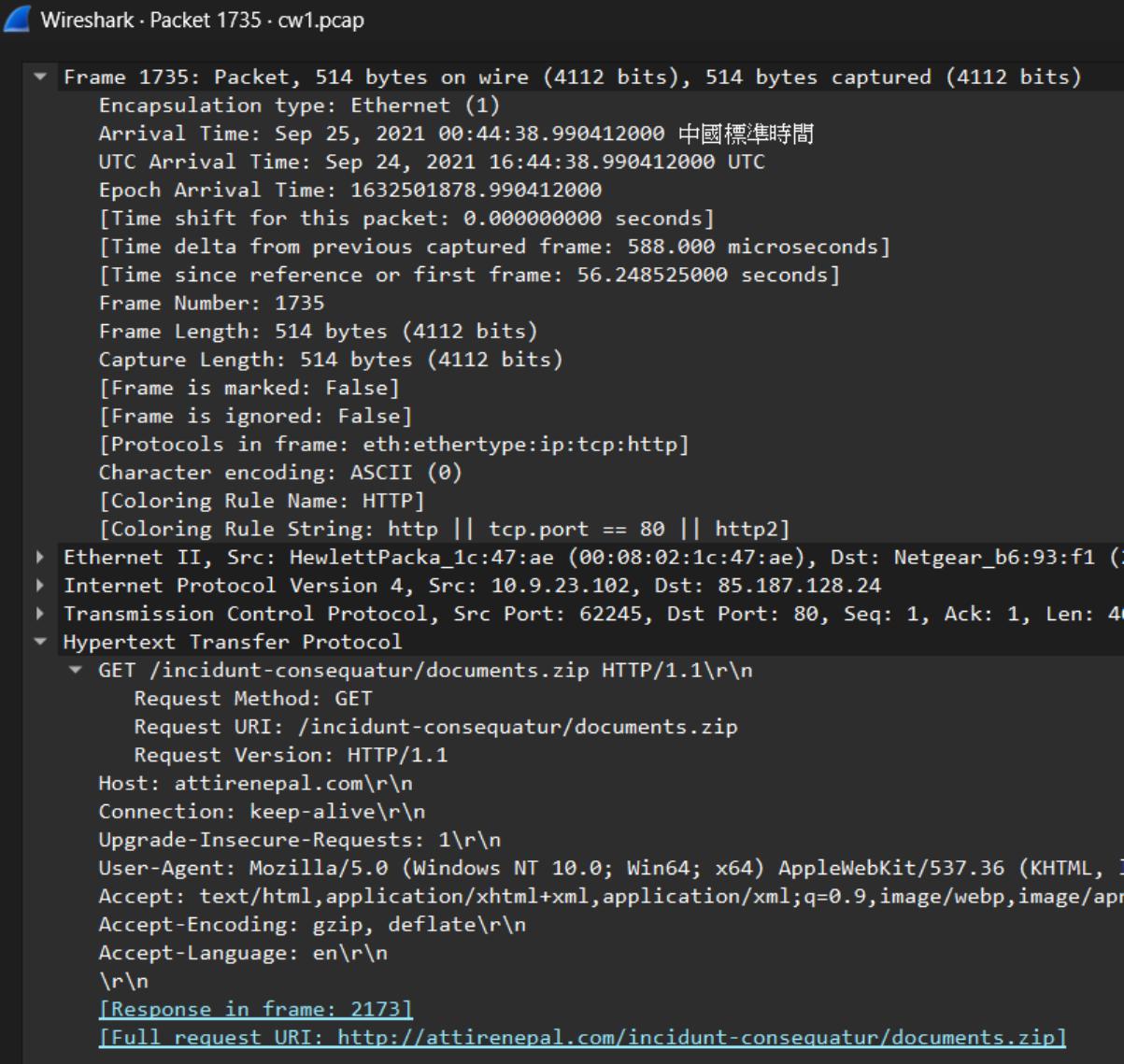
▼ Ethernet II, Src: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
  ▼ Destination: IPv4mcast_16 (01:00:5e:00:00:16)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..1. .... .... .... = IG bit: Group address (multicast/broadcast)
  ▼ Source: HewlettPacka_1c:47:ae (00:08:02:1c:47:ae)
    .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
    .... ..0. .... .... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 2]

```

MAC address of infected machine

2. **Reconstruction of Initial Infection Vector** Applied filter http to isolate clear-text web traffic. Identified the first malicious HTTP transaction at 2021-09-24 16:44:38 UTC:

Frame 1735 (GET /incidunt-consequatur/documents.zip HTTP/1.1) to domain [attirenepal.com](http://attirenepal.com). The server response in Frame 2173 returned **documents.zip** (198125 bytes) with headers: Server: **LiteSpeed** (no version disclosed), X-Powered-By: PHP/7.2.34, Content-Disposition: attachment; filename=documents.zip. Exported the file via File > Export Objects > HTTP, decompressed it locally, and discovered the internal file **chart-1530076591.xls** (likely containing malicious VBA macros).



Wireshark - Packet 1735 · cw1.pcap

Frame 1735: Packet, 514 bytes on wire (4112 bits), 514 bytes captured (4112 bits)  
Encapsulation type: Ethernet (1)  
Arrival Time: Sep 25, 2021 00:44:38.990412000 中國標準時間  
UTC Arrival Time: Sep 24, 2021 16:44:38.990412000 UTC  
Epoch Arrival Time: 1632501878.990412000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 588.000 microseconds]  
[Time since reference or first frame: 56.248525000 seconds]  
Frame Number: 1735  
Frame Length: 514 bytes (4112 bits)  
Capture Length: 514 bytes (4112 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http]  
Character encoding: ASCII (0)  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
Ethernet II, Src: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear\_b6:93:f1 (00:0c:29:b6:93:f1)  
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 85.187.128.24  
Transmission Control Protocol, Src Port: 62245, Dst Port: 80, Seq: 1, Ack: 1, Len: 404  
Hypertext Transfer Protocol  
GET /incident-consequatur/documents.zip HTTP/1.1\r\nRequest Method: GET  
Request URI: /incident-consequatur/documents.zip  
Request Version: HTTP/1.1  
Host: attirenepal.com\r\nConnection: keep-alive\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/94.0.4606.61 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,\*/\*;q=0.8  
Accept-Encoding: gzip, deflate\r\nAccept-Language: en\r\n\r\n[Response in frame: 2173]  
[Full request URI: http://attirenepal.com/incidunt-consequatur/documents.zip]

Frame 1735

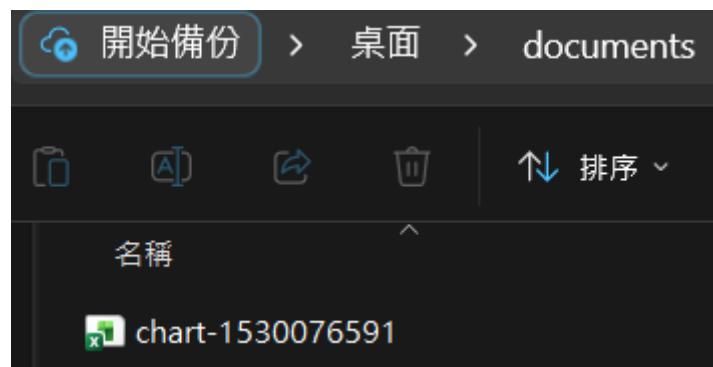
```

Wireshark - Packet 2173 · cw1.pcap

▼ Frame 2173: Packet, 580 bytes on wire (4640 bits), 580 bytes captured (4640 bits)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 25, 2021 00:44:41.976037000 中國標準時間
  UTC Arrival Time: Sep 24, 2021 16:44:41.976037000 UTC
  Epoch Arrival Time: 1632501881.976037000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 7.000 microseconds]
  [Time delta from previous displayed frame: 2.985625000 seconds]
  [Time since reference or first frame: 59.234150000 seconds]
  Frame Number: 2173
  Frame Length: 580 bytes (4640 bits)
  Capture Length: 580 bytes (4640 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http:data]
  Character encoding: ASCII (0)
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
▶ Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1c:47
▶ Internet Protocol Version 4, Src: 85.187.128.24, Dst: 10.9.23.102
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 62245, Seq: 198269, Ack: 198270
▶ [148 Reassembled TCP Segments (198794 bytes): #1841(1460), #1842(1236), #1844(134)]
▼ Hypertext Transfer Protocol, has 5 chunks (including last chunk)
  ▼ HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Connection: Keep-Alive\r\n
    Keep-Alive: timeout=5, max=100\r\n
    x-powered-by: PHP/7.2.34\r\n
    set-cookie: PHPSESSID=3de638a4b99bd63f8f7b0ca7e3b6f14c; path=/\r\n
    content-description: File Transfer\r\n
    content-type: application/octet-stream\r\n
    content-disposition: attachment; filename=documents.zip\r\n
    content-transfer-encoding: binary\r\n
    expires: 0\r\n
    cache-control: must-revalidate, post-check=0, pre-check=0\r\n
    pragma: public\r\n
    transfer-encoding: chunked\r\n
    date: Fri, 24 Sep 2021 16:44:06 GMT\r\n
    server: LiteSpeed\r\n
    strict-transport-security: max-age=63072000; includeSubDomains\r\n
    x-frame-options: SAMEORIGIN\r\n
    x-content-type-options: nosniff\r\n
  \r\n
  [Request in frame: 1735]

```

Frame 2173



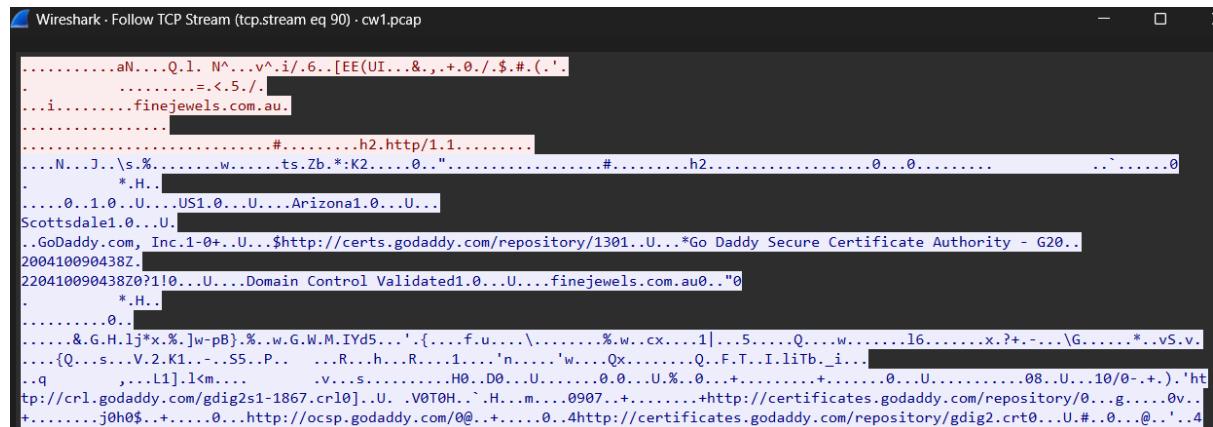
Decompressed documents.zip internal file chart-1530076591.xls

3. Secondary Payload Staging and Lateral Delivery Narrowed analysis to the critical time window 16:45:11 – 16:45:30 UTC (quiz hint) using filter tls. Examined Client Hello packets for Server Name Indication (SNI) extension, revealing three additional malicious domains involved in payload delivery:

- a. **finejewels.com.au** (Frame 2427; certificate chain issued by GoDaddy)
- b. **Thietbiagt.com** (Frame 3009)
- c. **new.americold.com** (Frame 3229)

These domains hosted secondary payloads or loaders that facilitated the next stage of compromise.

| 2427 89.098829 10.9.23.102 148.72.192.206 63368 443 247 Client Hello (SNI=finejewels.com.au)



```
Wireshark - Follow TCP Stream (tcp.stream eq 90) · cw1.pcap
.....aN....Q.l. N^...v^.i/.6..[EE(UI...8.,.+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.
220410090438Z?1!0..U....Domain Control Validated1.0...U....finejewels.com.au0.."0
*.H..
....0...
....&G.H.\j*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.....0..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 ..VOTH..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
```

Frame 2427

| 3009 98.572125 10.9.23.102 210.245.90.247 63375 443 244 Client Hello (SNI=thietbiagt.com)

Frame 3009

| 3229 102.989229 10.9.23.102 148.72.53.144 63376 443 247 Client Hello (SNI=new.americold.com)

Frame 3229

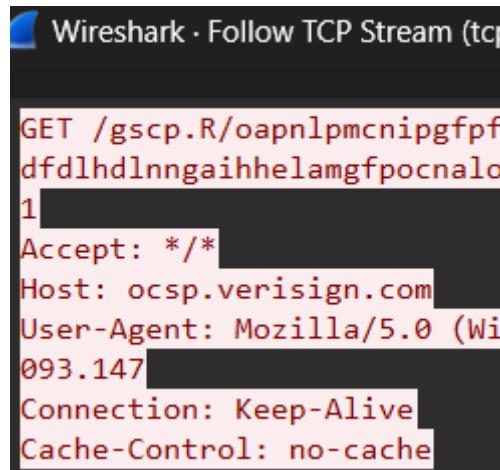
4. Command-and-Control (C2) Infrastructure Identification Used Statistics > Conversations > TCP (sorted by packet count and duration) to detect persistent, periodic outbound connections indicative of beaconing. Identified two Cobalt Strike Team Servers:

- a. **185.106.96.158** (port 80/HTTP): Host header **ocsp.verisign.com** (domain fronting technique), associated domain **survmeter.live**

b. 185.125.204.174 (port 443/HTTPS): SNI securitybusinpuff.com (Frame 7112  
 Client Hello)

| No.   | Time       | ip.src      | ip.dst         | src port | dst port | Length | info   |
|-------|------------|-------------|----------------|----------|----------|--------|--|
| 24088 | 964.936527 | 10.9.23.102 | 185.106.96.158 | 63579    | 80       | 54     | 63579 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                               |
| 24089 | 964.936713 | 10.9.23.102 | 185.106.96.158 | 63579    | 80       | 569    | GET /gscp.R/oapnlpmcnipgfpfghdahhbhbjigcmfgekipdla...cedhacmaghdehcdaajhnk |
| 24092 | 965.182666 | 10.9.23.102 | 185.106.96.158 | 63579    | 80       | 54     | 63579 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24093 | 965.182797 | 10.9.23.102 | 185.106.96.158 | 63579    | 80       | 54     | 63579 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0                      |
| 24100 | 969.883283 | 10.9.23.102 | 185.106.96.158 | 63580    | 80       | 66     | 63580 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM           |
| 24102 | 970.226286 | 10.9.23.102 | 185.106.96.158 | 63580    | 80       | 54     | 63580 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                               |
| 24103 | 970.226632 | 10.9.23.102 | 185.106.96.158 | 63580    | 80       | 569    | GET /gscp.R/oapnlpmcnipgfpfghdahhbhbjigcmfgekipdla...cedhacmaghdehcdaajhnk |
| 24106 | 970.532855 | 10.9.23.102 | 185.106.96.158 | 63580    | 80       | 54     | 63580 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24107 | 970.533127 | 10.9.23.102 | 185.106.96.158 | 63580    | 80       | 54     | 63580 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0                      |
| 24112 | 973.758681 | 10.9.23.102 | 185.106.96.158 | 63581    | 80       | 66     | 63581 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM           |
| 24115 | 974.011344 | 10.9.23.102 | 185.106.96.158 | 63581    | 80       | 54     | 63581 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24116 | 974.011721 | 10.9.23.102 | 185.106.96.158 | 63581    | 80       | 569    | GET /gscp.R/oapnlpmcnipgfpfghdahhbhbjigcmfgekipdla...cedhacmaghdehcdaajhnk |
| 24119 | 974.323239 | 10.9.23.102 | 185.106.96.158 | 63581    | 80       | 54     | 63581 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24120 | 974.323567 | 10.9.23.102 | 185.106.96.158 | 63581    | 80       | 54     | 63581 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0                      |
| 24126 | 978.479001 | 10.9.23.102 | 185.106.96.158 | 63582    | 80       | 66     | 63582 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM           |
| 24128 | 978.826983 | 10.9.23.102 | 185.106.96.158 | 63582    | 80       | 54     | 63582 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                               |
| 24129 | 978.827163 | 10.9.23.102 | 185.106.96.158 | 63582    | 80       | 569    | GET /gscp.R/oapnlpmcnipgfpfghdahhbhbjigcmfgekipdla...cedhacmaghdehcdaajhnk |
| 24133 | 979.076217 | 10.9.23.102 | 185.106.96.158 | 63582    | 80       | 54     | 63582 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24134 | 979.076416 | 10.9.23.102 | 185.106.96.158 | 63582    | 80       | 54     | 63582 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0                      |
| 24165 | 982.148637 | 10.9.23.102 | 185.106.96.158 | 63585    | 80       | 66     | 63585 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM           |
| 24181 | 982.383628 | 10.9.23.102 | 185.106.96.158 | 63585    | 80       | 54     | 63585 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                               |
| 24184 | 982.383854 | 10.9.23.102 | 185.106.96.158 | 63585    | 80       | 569    | GET /gscp.R/oapnlpmcnipgfpfghdahhbhbjigcmfgekipdla...cedhacmaghdehcdaajhnk |
| 24196 | 982.628255 | 10.9.23.102 | 185.106.96.158 | 63585    | 80       | 54     | 63585 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24197 | 982.628494 | 10.9.23.102 | 185.106.96.158 | 63585    | 80       | 54     | 63585 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0                      |
| 24275 | 986.947777 | 10.9.23.102 | 185.106.96.158 | 63586    | 80       | 66     | 63586 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM           |
| 24277 | 987.199376 | 10.9.23.102 | 185.106.96.158 | 63586    | 80       | 54     | 63586 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                               |
| 24278 | 987.199620 | 10.9.23.102 | 185.106.96.158 | 63586    | 80       | 569    | GET /gscp.R/oapnlpmcnipgfpfghdahhbhbjigcmfgekipdla...cedhacmaghdehcdaajhnk |
| 24281 | 987.532099 | 10.9.23.102 | 185.106.96.158 | 63586    | 80       | 54     | 63586 → 80 [ACK] Seq=516 Ack=310 Win=65535 Len=0                           |
| 24282 | 987.532375 | 10.9.23.102 | 185.106.96.158 | 63586    | 80       | 54     | 63586 → 80 [FIN, ACK] Seq=516 Ack=310 Win=65535 Len=0                      |
| 24292 | 991.227850 | 10.9.23.102 | 185.106.96.158 | 63587    | 80       | 66     | 63587 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM           |
| 24294 | 991.532478 | 10.9.23.102 | 185.106.96.158 | 63587    | 80       | 54     | 63587 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0                               |

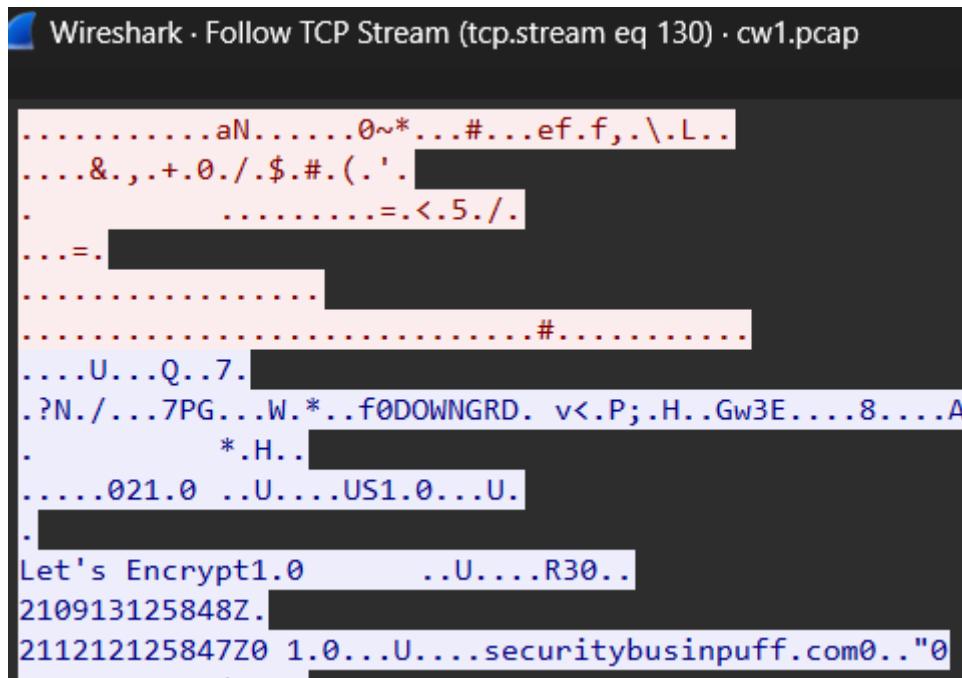
Traffic of 185.106.96.158



Host header ocsp.verisign.com

| No.  | Time       | ip.src           | ip.dst          | src port | dst port | Length | info  |
|------|------------|------------------|-----------------|----------|----------|--------|---|
| 4216 | 581.342835 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 66     | 63410 → 8080 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK |
| 4217 | 581.504598 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 58     | 8080 → 63410 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460  |
| 4218 | 581.504879 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=1 Ack=1 Win=65535 Len=0                |
| 4219 | 581.509907 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 203    | 63410 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=65535 Len=149         |
| 4220 | 581.510000 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 54     | 8080 → 63410 [ACK] Seq=1 Ack=150 Win=64240 Len=0              |
| 4221 | 581.683263 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 144    | 8080 → 63410 [PSH, ACK] Seq=1 Ack=150 Win=64240 Len=90        |
| 4222 | 581.683508 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=150 Ack=91 Win=65535 Len=0             |
| 4223 | 581.685014 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1402   | 8080 → 63410 [PSH, ACK] Seq=91 Ack=150 Win=64240 Len=1348     |
| 4224 | 581.685191 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=150 Ack=1439 Win=65535 Len=0           |
| 4225 | 581.844256 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 367    | 8080 → 63410 [PSH, ACK] Seq=1439 Ack=150 Win=64240 Len=313    |
| 4226 | 581.844488 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=150 Ack=1752 Win=65535 Len=0           |
| 4249 | 583.867600 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 147    | 63410 → 8080 [PSH, ACK] Seq=150 Ack=1752 Win=65535 Len=93     |
| 4250 | 583.867693 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 54     | 8080 → 63410 [ACK] Seq=1752 Ack=243 Win=64240 Len=0           |
| 4251 | 584.039040 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 68     | 8080 → 63410 [PSH, ACK] Seq=1752 Ack=243 Win=64240 Len=6      |
| 4252 | 584.039292 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=150 Ack=243 Win=65535 Len=0            |
| 4253 | 584.208411 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 99     | 8080 → 63410 [PSH, ACK] Seq=243 Ack=1758 Win=64240 Len=45     |
| 4254 | 584.208634 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=243 Ack=1803 Win=65535 Len=0           |
| 4255 | 584.210999 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 449    | 63410 → 8080 [PSH, ACK] Seq=243 Ack=1803 Win=65535 Len=395    |
| 4256 | 584.211071 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 54     | 8080 → 63410 [ACK] Seq=1803 Ack=638 Win=64240 Len=0           |
| 4257 | 584.384719 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 353    | 8080 → 63410 [PSH, ACK] Seq=1803 Ack=638 Win=64240 Len=299    |
| 4258 | 584.384985 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=243 Ack=2102 Win=65535 Len=0           |
| 4259 | 584.385882 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1514   | 8080 → 63410 [ACK] Seq=2102 Ack=638 Win=64240 Len=1460        |
| 4260 | 584.385893 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1290   | 8080 → 63410 [PSH, ACK] Seq=3562 Ack=638 Win=64240 Len=1236   |
| 4261 | 584.386284 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=638 Ack=4798 Win=65535 Len=0           |
| 4262 | 584.386321 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1402   | 8080 → 63410 [PSH, ACK] Seq=4798 Ack=638 Win=64240 Len=1348   |
| 4263 | 584.386423 | 10.9.23.102      | 185.125.204.174 | 63410    | 8080     | 54     | 63410 → 8080 [ACK] Seq=638 Ack=6146 Win=65535 Len=0           |
| 4264 | 584.386635 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1514   | 8080 → 63410 [ACK] Seq=6146 Ack=638 Win=64240 Len=1460        |
| 4265 | 584.386667 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1514   | 8080 → 63410 [ACK] Seq=7606 Ack=638 Win=64240 Len=1460        |
| 4266 | 584.386698 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1178   | 8080 → 63410 [PSH, ACK] Seq=9066 Ack=638 Win=64240 Len=1124   |
| 4267 | 584.386741 | 185.125.204.1... | 10.9.23.102     | 8080     | 63410    | 1402   | 8080 → 63410 [PSH, ACK] Seq=10190 Ack=638 Win=64240 Len=1348  |

Traffic of 185.125.204.174



SNI securitybusinpuff.com

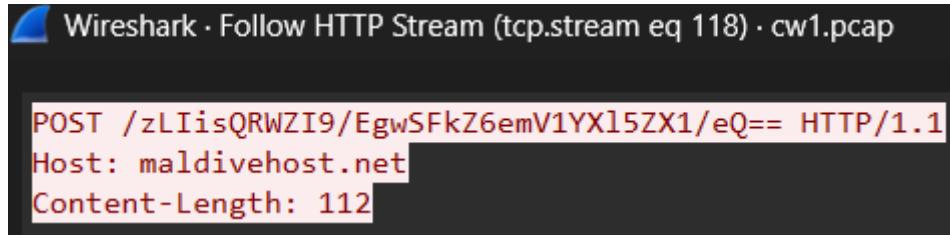
- Post-Infection C2 and Beacon Activity Filtered http.request.method == "POST" to locate active C2 channels. Discovered POST requests to **maldivehost.net** (Frame 3822, 281-byte payload starting zLIisQRWZI9). Server response (Frame 3851) revealed **Apache/2.4.49 (cPanel) OpenSSL/1.1.11 mod\_bwlimited/1.4.**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method == "POST"

| No.                | Time        | ip.src         | ip.dst | src port | dst port | Length   | info |
|--------------------|-------------|----------------|--------|----------|----------|--|------|
| 12426 897.509523   | 10.9.23.102 | 185.106.96.158 | 63516  | 80       | 778      | POST /supprq/sa/dbdhdfdbdfddhdaedc HTTP/1.1  |      |
| + 13205 813.083594 | 10.9.23.102 | 185.106.96.158 | 63533  | 80       | 826      | POST /supprq/sa/dbdhdfdbdfddhdaedc HTTP/1.1  |      |
| 3822 153.653113    | 10.9.23.102 | 208.91.128.6   | 63385  | 80       | 281      | POST /zLii\$QRWZI9/QoSao1xzHgtfjMcGypGenpIdWFSeW9f3k= HTTP/1.1 Continuation                  |      |
| 3908 178.767210    | 10.9.23.102 | 208.91.128.6   | 63386  | 80       | 285      | POST /zLii\$QRWZI9/ASk5xkSPR8l1j5eIg9KnfGyZHI/YXp6eQ== HTTP/1.1 Continuation                 |      |
| 3996 203.829455    | 10.9.23.102 | 208.91.128.6   | 63389  | 80       | 285      | POST /zLii\$QRWZI9/FXMKlgOnkz/Da15DggB10NgfGyZHI/YXp6eQ== HTTP/1.1 Continuation              |      |
| 4006 228.842458    | 10.9.23.102 | 208.91.128.6   | 63390  | 80       | 273      | POST /zLii\$QRWZI9/e0kkAAObInx9Rp6ZxHe1LfX95 HTTP/1.1 Continuation                           |      |
| 4017 254.037243    | 10.9.23.102 | 208.91.128.6   | 63391  | 80       | 293      | POST /zLii\$QRWZI9/lj+J5oqJQ4LB1wiAhr7KngvHgopKbfhfmtkcmJ9eG6R6FH0= HTTP/1.1 Continuation    |      |
| 4027 279.063986    | 10.9.23.102 | 208.91.128.6   | 63392  | 80       | 289      | POST /zLii\$QRWZI9/HD9N9ScAAwPKwEFMwJ/3T15PEZ6emV1YX15ZX1/eQ== HTTP/1.1 Continuation         |      |
| 4037 304.108570    | 10.9.23.102 | 208.91.128.6   | 63393  | 80       | 273      | POST /zLii\$QRWZI9/CsZDz1/Mw9f2VzX58Zxt7fge== HTTP/1.1 Continuation                          |      |
| 4046 329.217819    | 10.9.23.102 | 208.91.128.6   | 63394  | 80       | 285      | POST /zLii\$QRWZI9/DC1zfTsJDga/AicErRgXChsERx57ZJ1fxhken9 HTTP/1.1 Continuation              |      |
| 4090 354.299575    | 10.9.23.102 | 208.91.128.6   | 63396  | 80       | 293      | POST /zLii\$QRWZI9/EgwEcWohMhk+B0ku3BnHQUlI4GLwpfntkcmJ9eG6R6FH0= HTTP/1.1 Continuation      |      |
| 4099 379.469159    | 10.9.23.102 | 208.91.128.6   | 63397  | 80       | 269      | POST /zLii\$QRWZI9/G80tLyck3p8VXkeXhenp5 HTTP/1.1 Continuation                               |      |
| 4109 404.557049    | 10.9.23.102 | 208.91.128.6   | 63398  | 80       | 269      | POST /zLii\$QRWZI9/EgwSFk26emV1YX15ZXL/eQ== HTTP/1.1 Continuation                            |      |
| 4118 429.544248    | 10.9.23.102 | 208.91.128.6   | 63399  | 80       | 285      | POST /zLii\$QRWZI9/CxwglgIIIXhOqKPPHyCOUNgfGyZHI/YXp6eQ== HTTP/1.1 Continuation              |      |
| 4131 454.726221    | 10.9.23.102 | 208.91.128.6   | 63400  | 80       | 277      | POST /zLii\$QRWZI9/fskCegTcg8VvKw950n1/ZXNlfxleit+ HTTP/1.1 Continuation                     |      |
| 4149 479.894757    | 10.9.23.102 | 208.91.128.6   | 63401  | 80       | 265      | POST /zLii\$QRWZI9/TITIYRX572HziFkhken9 HTTP/1.1 Continuation                                |      |
| 4150 505.0809991   | 10.9.23.102 | 208.91.128.6   | 63402  | 80       | 265      | POST /zLii\$QRWZI9/0hpCFx9lc2V+fGV7e34= HTTP/1.1 Continuation                                |      |
| 4162 530.187719    | 10.9.23.102 | 208.91.128.6   | 63404  | 80       | 273      | POST /zLii\$QRWZI9/DCzHSYnBRJFfntkcm39eG6Fh0= HTTP/1.1 Continuation                          |      |
| 4179 555.288708    | 10.9.23.102 | 208.91.128.6   | 63406  | 80       | 289      | POST /zLii\$QRWZI9/mYYFB8/BguIAngKgPAMG0cQ3p8YXjkX9heng5 HTTP/1.1 Continuation               |      |
| 4207 580.475722    | 10.9.23.102 | 208.91.128.6   | 63409  | 80       | 277      | POST /zLii\$QRWZI9/eg17AfENQAQAK7e232ZKh4Yn57eA== HTTP/1.1 Continuation                      |      |
| 4581 605.574149    | 10.9.23.102 | 208.91.128.6   | 63418  | 80       | 269      | POST /zLii\$QRWZI9/QsKykk26emV1YX15ZXL/eQ== HTTP/1.1 Continuation                            |      |
| 4930 630.656018    | 10.9.23.102 | 208.91.128.6   | 63428  | 80       | 289      | POST /zLii\$QRWZI9/fskCegTcg8VvKw950n1/ZXNlfxleit+ HTTP/1.1 Continuation                     |      |
| 5208 655.639495    | 10.9.23.102 | 208.91.128.6   | 63441  | 80       | 265      | POST /zLii\$QRWZI9/Aj1cfX9lc2V+fGV7e34= HTTP/1.1 Continuation                                |      |
| 6227 680.731212    | 10.9.23.102 | 208.91.128.6   | 63444  | 80       | 265      | POST /zLii\$QRWZI9/OsdcFx9lc2V+fGV7e34= HTTP/1.1 Continuation                                |      |
| 6660 705.826232    | 10.9.23.102 | 208.91.128.6   | 63454  | 80       | 297      | POST /zLii\$QRWZI9/HiYfeTpyPng4KCF4Pz8E0ggQ0kg0A0PBuJ7e232ZKh4Yn57eA== HTTP/1.1 Continuation |      |
| 7188 730.806600    | 10.9.23.102 | 208.91.128.6   | 63461  | 80       | 285      | POST /zLii\$QRWZI9/jhANAz16gw8FBhMABRYGcn9cFx91c2V+fGV7e34= HTTP/1.1 Continuation            |      |
| 10017 756.507647   | 10.9.23.102 | 208.91.128.6   | 63482  | 80       | 277      | POST /zLii\$QRWZI9/DRs5e3gJa4w4glik7e232ZKh4Yn57eA== HTTP/1.1 Continuation                   |      |
| 10257 781.698180   | 10.9.23.102 | 208.91.128.6   | 63494  | 80       | 281      | POST /zLii\$QRWZI9/34KJnkbaSUNPzEYigcwQnt7YnZlehhfn4 HTTP/1.1 Continuation                   |      |

active C2 channels



POST requests to **maldivehost.net**

Wireshark · Packet 3822 · cw1.pcap

Frame 3822: Packet, 281 bytes on wire (2248 bits), 281 bytes captured (Encapsulation type: Ethernet (1))  
Arrival Time: Sep 25, 2021 00:46:16.395000000 中國標準時間  
UTC Arrival Time: Sep 24, 2021 16:46:16.395000000 UTC  
Epoch Arrival Time: 1632501976.395000000  
[Time shift for this packet: 0.000000000 seconds]  
[Time delta from previous captured frame: 998.000 microseconds]  
[Time delta from previous displayed frame: 998.000 microseconds]  
[Time since reference or first frame: 2 minutes, 33.653113000 seconds]  
Frame Number: 3822  
Frame Length: 281 bytes (2248 bits)  
Capture Length: 281 bytes (2248 bits)  
[Frame is marked: False]  
[Frame is ignored: False]  
[Protocols in frame: eth:ethertype:ip:tcp:http:data:data]  
Character encoding: ASCII (0)  
[Coloring Rule Name: HTTP]  
[Coloring Rule String: http || tcp.port == 80 || http2]  
Ethernet II, Src: HewlettPacka\_1c:47:ae (00:08:02:1c:47:ae), Dst: Netgear (08:00:27:00:00:00)  
Internet Protocol Version 4, Src: 10.9.23.102, Dst: 208.91.128.6  
Transmission Control Protocol, Src Port: 63385, Dst Port: 80, Seq: 1, A  
Hypertext Transfer Protocol  
POST /zLIisQRWZI9/0QsaDixzHTgtfjMcGypGenpldWF5eWV9f3k= HTTP/1.1\r\nRequest Method: POST  
Request URI: /zLIisQRWZI9/0QsaDixzHTgtfjMcGypGenpldWF5eWV9f3k=  
Protocol Version: HTTP/1.1

Frame 3822

```
Wireshark - Packet 3851 · cw1.pcap

Frame 3851: Packet, 634 bytes on wire (5072 bits), 634 bytes captured (5072 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Sep 25, 2021 00:46:17.143575000 中國標準時間
UTC Arrival Time: Sep 24, 2021 16:46:17.143575000 UTC
Epoch Arrival Time: 1632501977.143575000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 16.274000 milliseconds]
[Time delta from previous displayed frame: 16.274000 milliseconds]
[Time since reference or first frame: 2 minutes, 34.401688000 seconds]
Frame Number: 3851
Frame Length: 634 bytes (5072 bits)
Capture Length: 634 bytes (5072 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:http:data-text-lines]
Character encoding: ASCII (0)
[Coloring Rule Name: HTTP]
[Coloring Rule String: http || tcp.port == 80 || http2]
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_1 (08:00:27:00:00:01)
Internet Protocol Version 4, Src: 208.91.128.6, Dst: 10.9.23.102
Transmission Control Protocol, Src Port: 80, Dst Port: 63385, Seq: 1, Ack: 1
Hypertext Transfer Protocol
HTTP/1.1 200 OK\r\n
    Response Version: HTTP/1.1
    Status Code: 200
    [Status Code Description: OK]
    Response Phrase: OK
    Date: Fri, 24 Sep 2021 16:46:15 GMT\r\n
    Server: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod_bwlimited/1.4\r\n
```

### Frame 3851

6. Reconnaissance and Exfiltration Filtered dns and identified an A query to [api.ipify.org](https://api.ipify.org) at 2021-09-24 17:00:04 UTC (Frame 24149), used by the malware to determine the victim's public IP. Filtered smtp to detect exfiltration attempts. The first MAIL FROM observed was [farshin@mailfa.com](mailto:farshin@mailfa.com). Following the TCP stream revealed AUTH LOGIN credentials for [ho3ein.sharifi@mailfa.com](mailto:ho3ein.sharifi@mailfa.com) (password decoded from base64: 13691369).

Wireshark · Packet 24149 · cw1.pcap

- ▶ Frame 24149: Packet, 299 bytes on wire
- ▶ Ethernet II, Src: Dell\_c2:09:6a (a4:1f:1e:09:c2:09)
- ▶ Internet Protocol Version 4, Src: 10.9.1.100
- ▶ User Datagram Protocol, Src Port: 53, Dst Port: 53
- ▼ Domain Name System (response)
  - Transaction ID: 0xc92c
  - ▼ Flags: 0x8180 Standard query response
    - 1... .... .... .... = Response: Message
    - .000 0... .... .... = Opcode: Standard query
    - .... .0.. .... .... = Authoritative answer
    - .... ..0. .... .... = Truncated: No
    - .... ...1 .... .... = Recursion desired
    - .... .... 1... .... = Recursion available
    - .... .... .0.. .... = Z: reserved
    - .... .... ..0. .... = Answer authenticator
    - .... .... ...0 .... = Non-authentication
    - .... .... .... 0000 = Reply code: No error
  - Questions: 1
  - Answer RRs: 10
  - Authority RRs: 0
  - Additional RRs: 0
- ▼ Queries
  - ▼ api.ipify.org: type A, class IN
    - Name: api.ipify.org
    - [Name Length: 13]
    - [Label Count: 3]
    - Type: A (1) (Host Address)
    - Class: IN (0x0001)

Frame 24149

Wireshark - cw1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

smtp

| No.   | Time        | ip.src        | ip.dst       | src port | dst port | Length   | info |
|-------|-------------|---------------|--------------|----------|----------|--|------|
| 25424 | 1040.310581 | 108.177.15.28 | 10.9.23.102  | 25       | 63602    | 111 S: 220 smtp-relay.gmail.com ESMTP p14sm62724ej |      |
| 25427 | 1040.328900 | 108.177.15.28 | 10.9.23.102  | 587      | 63603    | 111 S: 220 smtp-relay.gmail.com ESMTP v11sm162909w |      |
| 27766 | 1124.990346 | 108.177.15.28 | 10.9.23.102  | 587      | 63655    | 110 S: 220 smtp-relay.gmail.com ESMTP 7sm237060wrz |      |
| 27791 | 1125.174995 | 108.177.15.28 | 10.9.23.102  | 25       | 63652    | 112 S: 220 smtp-relay.gmail.com ESMTP y28sm114321l |      |
| 28158 | 1137.081223 | 108.177.15.28 | 10.9.23.102  | 25       | 63665    | 110 S: 220 smtp-relay.gmail.com ESMTP la2sm66415ej |      |
| 28189 | 1137.432545 | 108.177.15.28 | 10.9.23.102  | 25       | 63666    | 110 S: 220 smtp-relay.gmail.com ESMTP b8sm62981lf  |      |
| 28343 | 1139.976566 | 185.4.29.135  | 10.9.23.102  | 25       | 63678    | 75 S: 220 mail.mailfa.com                          |      |
| 28367 | 1140.408995 | 10.9.23.102   | 185.4.29.135 | 63678    | 25       | 70 C: EHLO localhost                               |      |
| 28395 | 1141.278848 | 185.4.29.135  | 10.9.23.102  | 25       | 63678    | 110 S: 250-mail.mailfa.com   SIZE 30000000   AUTH  |      |
| 28401 | 1141.458745 | 46.16.61.250  | 10.9.23.102  | 25       | 63681    | 96 S: 220 vxsys-smtpclusterma-03.srv.cat ESMTP     |      |
| 28410 | 1141.849946 | 10.9.23.102   | 46.16.61.250 | 63681    | 25       | 70 C: EHLO localhost                               |      |
| 28415 | 1142.013281 | 46.16.61.250  | 10.9.23.102  | 25       | 63681    | 253 S: 250-vxsys-smtpclusterma-03.srv.cat   PIPELI |      |
| 28420 | 1142.054497 | 10.9.23.102   | 185.4.29.135 | 63678    | 25       | 66 C: AUTH LOGIN                                   |      |
| 28448 | 1142.275010 | 10.9.23.102   | 46.16.61.250 | 63681    | 25       | 64 C: STARTTLS                                     |      |
| 28450 | 1142.275468 | 185.4.29.135  | 10.9.23.102  | 25       | 63678    | 72 S: 334 VXNlc5hbWU6                              |      |
| 28457 | 1142.434629 | 46.16.61.250  | 10.9.23.102  | 25       | 63681    | 84 S: 220 2.0.0 Ready to start TLS                 |      |
| 28467 | 1142.706961 | 10.9.23.102   | 185.4.29.135 | 63678    | 25       | 80 C: User: ZmFyc2hpBtYWlsZmEuY29t                 |      |
| 28477 | 1142.941465 | 185.4.29.135  | 10.9.23.102  | 25       | 63678    | 72 S: 334 UGFzc3dvcmQ6                             |      |
| 28480 | 1142.956561 | 185.4.29.135  | 10.9.23.102  | 25       | 63686    | 75 S: 220 mail.mailfa.com                          |      |
| 28504 | 1143.222316 | 10.9.23.102   | 185.4.29.135 | 63678    | 25       | 68 C: Pass: ZGluYW1pdA==                           |      |
| 28506 | 1143.222457 | 10.9.23.102   | 185.4.29.135 | 63686    | 25       | 70 C: EHLO localhost                               |      |
| 28521 | 1143.450341 | 185.4.29.135  | 10.9.23.102  | 25       | 63686    | 110 S: 250-mail.mailfa.com   SIZE 30000000   AUTH  |      |
| 28524 | 1143.456304 | 185.4.29.135  | 10.9.23.102  | 25       | 63678    | 74 S: 235 authenticated.                           |      |
| 28576 | 1144.036130 | 10.9.23.102   | 185.4.29.135 | 63678    | 25       | 86 C: MAIL FROM:<farshin@mailfa.com>               |      |

First mail received [farshin@mailfa.com](mailto:farshin@mailfa.com)

Wireshark · Follow TCP Stream (tcp.stream eq 383) · cw1.pcap

```

220 mail.mailfa.com
EHLO localhost
250-mail.mailfa.com
250-SIZE 30000000
250 AUTH LOGIN

AUTH LOGIN

334 VXNlc5hbWU6
ZmFyc2hpBtYWlsZmEuY29t
334 UGFzc3dvcmQ6
ZGluYW1pdA==

235 authenticated.

MAIL FROM:<farshin@mailfa.com>

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

```

TCP stream of first mail

**Section 3 – Results** The compromised endpoint is workstation 10.9.23.102 (MAC 00:08:02:1c:47:ae). Initial compromise occurred at 2021-09-24 16:44:38 UTC via a drive-by download of **documents.zip** from [attirenepal.com](http://attirenepal.com) (LiteSpeed server). The archive contained **chart-1530076591.xls**, which, upon execution, likely triggered malicious VBA macros or shellcode.

Secondary payloads were delivered over HTTPS (16:45:11 – 16:45:30 UTC) from [finejewels.com.au](http://finejewels.com.au) (GoDaddy-issued certificate), [thietbiagt.com](http://thietbiagt.com), and [new.americold.com](http://new.americold.com).

Persistent C2 was established using Cobalt Strike beacons to 185.106.96.158 (port 80, Host: ocsp.verisign.com, domain: survmeter.live) and 185.125.204.174 (port 443, SNI: securitybusinpuff.com). Post-infection command-and-control occurred over maldivehost.net (Apache/2.4.49 response), with beacon data beginning zLJisQRWZI9 (first packet to C2: 281 bytes).

The malware performed external IP reconnaissance via DNS query to [api.ipify.org](http://api.ipify.org) at 2021-09-24 17:00:04 UTC. Exfiltration was attempted via SMTP using [farshin@mailfa.com](mailto:farshin@mailfa.com) (first MAIL FROM); credentials for [ho3ein.sharifi@mailfa.com](mailto:ho3ein.sharifi@mailfa.com) were exposed as 13691369.

**Type of Infection** — Cobalt Strike beaconing (commercial adversary emulation tool abused for persistence, C2 over HTTP/HTTPS with domain fronting, obfuscated URIs, and credential exfiltration).

**Section 4 – Conclusion & Recommendations** This incident demonstrates a classic multi-stage attack: phishing-driven file download → user execution of macro-enabled document → staged payloads → deployment of Cobalt Strike → persistent C2 and attempted SMTP exfiltration. The use of domain fronting (ocsp.verisign.com) and legitimate-looking infrastructure delayed detection.

## Prevention & Mitigation

- **Endpoint Hardening** — Disable Office macros by default; enforce Protected View and block external content (Group Policy). Deploy EDR with macro/script scanning and Cobalt Strike behavioral detection.
- **Network Controls** — Implement web filtering/proxy to block known C2 domains/IPs (attirenepal.com, maldivehost.net, survmeter.live, securitybusinpuff.com). Monitor DNS for anomalous queries (api.ipify.org, dynamic update patterns).

- **Email & Attachment Security** — Enhance phishing filters; quarantine ZIP/XLS with macros; enforce strict SMTP relay policies and monitor AUTH attempts.
- **User Awareness** — Conduct regular phishing simulations and training on suspicious attachments and macro prompts.
- **Monitoring & Response** — Enable network packet capture with automated IOC matching; use JA3 fingerprinting for Cobalt Strike detection; maintain updated blocklists.

Remaining challenges include encrypted beacon traffic and legitimate domain abuse — requiring advanced behavioral analytics and continuous threat hunting.

## References

- Wireshark Documentation (filters, Follow Stream, Export Objects)
- MITRE ATT&CK: T1204.002, T1071.001, T1566.001
- VirusTotal IOC reports

My Github link: <https://github.com/Patrick-cybersec/COMP3010HK-Security-Operations-Incident-Management/issues>