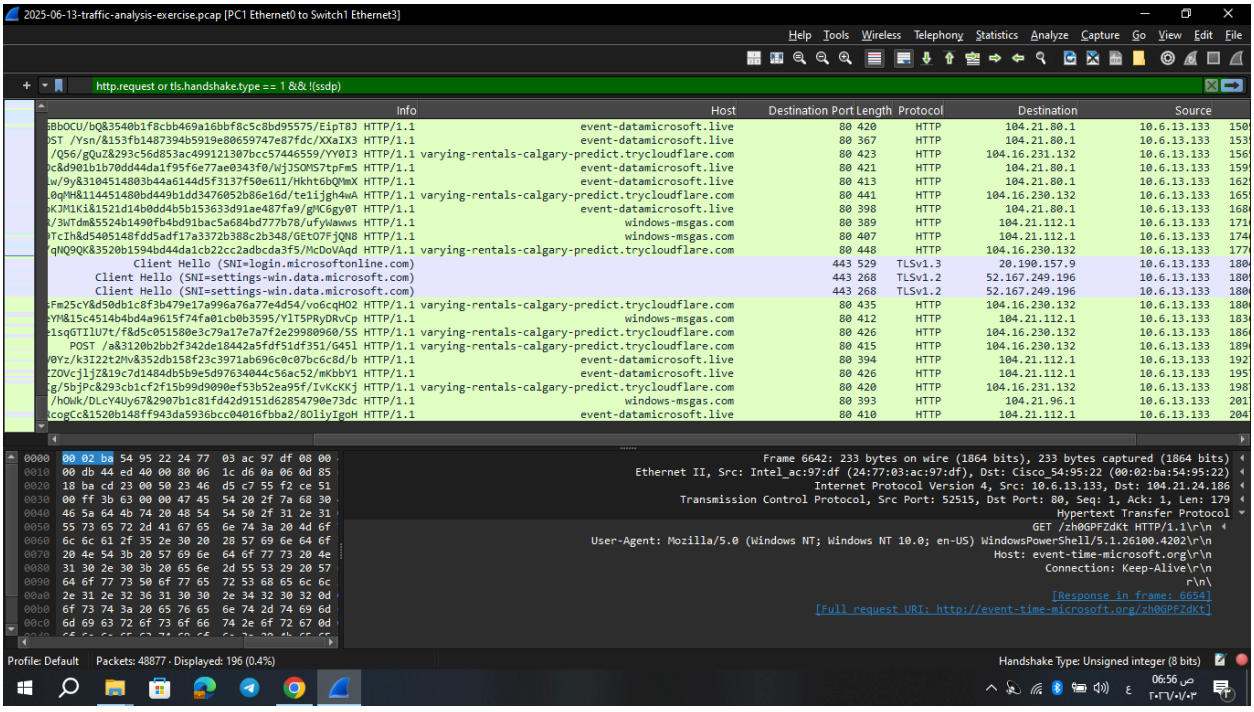
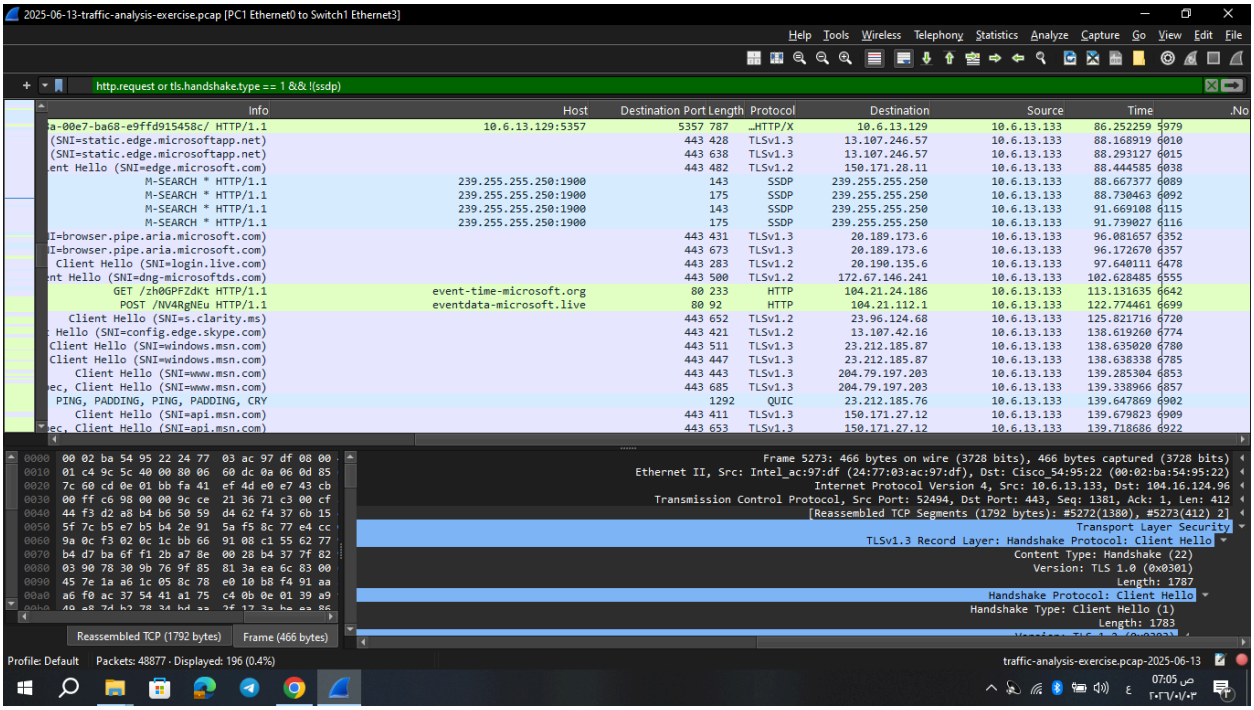
Incident Response Case Study

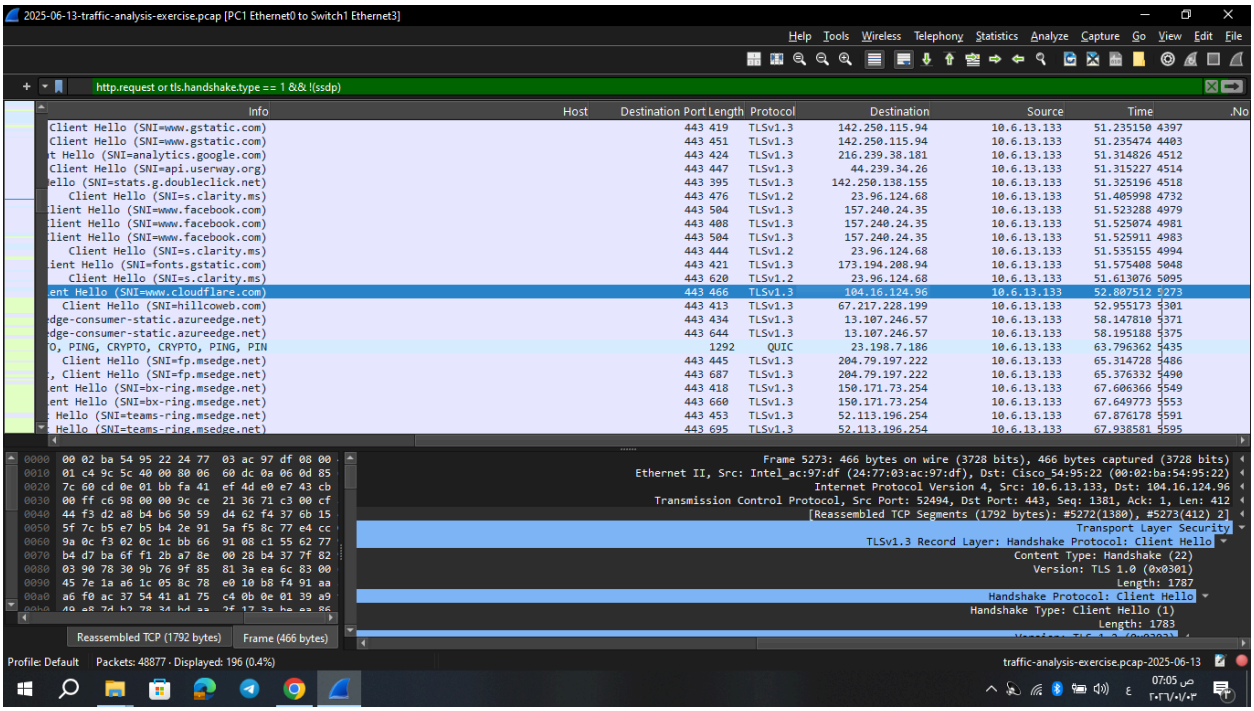
Malicious HTTP/TLS Beaconing Behind Cloudflare.

1 Executive Summary:

During network traffic analysis, suspicious outbound HTTP and TLS traffic was identified from an internal workstation (10.6.13.133) communicating with multiple external IP addresses associated with Cloudflare infrastructure. Further investigation revealed that the traffic was related to a malicious domain used for command-and-control (C2) communication. This report documents the full detection, investigation, and attribution process.




2025-06-13-traffic-analysis-exercise.pcap [PC1 Ethernet0 to Switch1 Ethernet3]
Help Tools Wireless Telephony Statistics Analyze Capture Go View Edit File
http.request or tls.handshake.type == 1 && !(ssdp)
Info Host Destination Port Length Protocol Destination Source Time .No
a-00e7-ba68-e9ffd915458c/ HTTP/1.1 10.6.13.129:5357 5357 787 …HTTP/X 10.6.13.129 10.6.13.133 86.252259 5979
(SNI=static.edge.microsoftapp.net) 443 428 TLSv1.3 13.107.246.57 10.6.13.133 88.168919 6010
(SNI=static.edge.microsoftapp.net) 443 638 TLSv1.3 13.107.246.57 10.6.13.133 88.293127 6015
ent Hello (SNI=edge.microsoft.com) 443 482 TLSv1.2 150.171.28.11 10.6.13.133 88.444585 6038
M-SEARCH * HTTP/1.1 239.255.255.250:1900 143 SSDP 239.255.255.250 10.6.13.133 88.667377 6089
M-SEARCH * HTTP/1.1 239.255.255.250:1900 175 SSDP 239.255.255.250 10.6.13.133 88.730463 6092
M-SEARCH * HTTP/1.1 239.255.255.250:1900 143 SSDP 239.255.255.250 10.6.13.133 91.669108 6115
M-SEARCH * HTTP/1.1 239.255.255.250:1900 175 SSDP 239.255.255.250 10.6.13.133 91.739027 6116
I=browser.pipe.aria.microsoft.com) 443 431 TLSv1.3 20.189.173.6 10.6.13.133 96.081657 6352
I=browser.pipe.aria.microsoft.com) 443 673 TLSv1.3 20.189.173.6 10.6.13.133 96.172670 6357
Client Hello (SNI=login.live.com) 443 283 TLSv1.2 20.190.135.6 10.6.13.133 97.640111 6478
nt Hello (SNI=dng-microsoftds.com) 443 500 TLSv1.2 172.67.146.241 10.6.13.133 102.628485 6555
GET /zh0GPFZdKt HTTP/1.1 event-time-microsoft.org 80 233 HTTP 104.21.24.186 10.6.13.133 113.131635 6642
POST /NV4RgNEu HTTP/1.1 eventdata-microsoft.live 80 92 HTTP 104.21.112.1 10.6.13.133 122.774461 6699
Client Hello (SNI=s.clarity.ms) 443 652 TLSv1.2 23.96.124.68 10.6.13.133 125.821716 6720
Hello (SNI=config.edge.skype.com) 443 421 TLSv1.2 13.107.42.16 10.6.13.133 138.619260 6774
Client Hello (SNI=windows.msn.com) 443 511 TLSv1.3 23.212.185.87 10.6.13.133 138.635020 6780
Client Hello (SNI=windows.msn.com) 443 447 TLSv1.3 23.212.185.87 10.6.13.133 138.638338 6785
Client Hello (SNI=www.msn.com) 443 443 TLSv1.3 204.79.197.203 10.6.13.133 139.285304 6853
ec, Client Hello (SNI=www.msn.com) 443 685 TLSv1.3 204.79.197.203 10.6.13.133 139.338966 6857
PING, PADDING, PING, PADDING, CRY 1292 QUIC 23.212.185.76 10.6.13.133 139.647869 6902
Client Hello (SNI=api.msn.com) 443 411 TLSv1.3 150.171.27.12 10.6.13.133 139.679823 6909
ec, Client Hello (SNI=api.msn.com) 443 653 TLSv1.3 150.171.27.12 10.6.13.133 139.718686 6922
0000 00 02 ba 54 95 22 24 77 03 ac 97 df 08 00
0010 01 c4 9c 5c 40 00 80 06 60 dc 0a 06 0d 85
0020 7c 60 cd 0e 01 bb fa 41 ef 4d e0 e7 43 cb
0030 00 ff c6 98 00 00 9c ce 21 36 71 c3 00 cf
0040 44 f3 d2 a8 b4 b6 50 59 d4 62 f4 37 6b 15
0050 5f 7c b5 e7 b5 b4 2e 91 5a f5 8c 77 e4 cc
0060 9a 0c f3 02 0c 1c bb 66 91 08 c1 55 62 77
0070 b4 d7 ba 6f f1 2b a7 8e 00 28 b4 37 7f 82
0080 03 90 78 30 9b 76 9f 85 81 3a ea 6c 83 00
0090 45 7e 1a a6 1c 05 8c 78 e0 10 b8 f4 91 aa
00a0 a6 f0 ac 37 54 41 a1 75 c4 0b 0e 01 39 a9
Reassembled TCP (1792 bytes)
Frame (466 bytes)
Frame 5273: 466 bytes on wire (3728 bits), 466 bytes captured (3728 bits)
Ethernet II, Src: Intel_ac:97:df (24:77:03:ac:97:df), Dst: Cisco_54:95:22 (00:02:ba:54:95:22)
Internet Protocol Version 4, Src: 10.6.13.133, Dst: 104.16.124.96
Transmission Control Protocol, Src Port: 52494, Dst Port: 443, Seq: 1381, Ack: 1, Len: 412
[Reassembled TCP Segments (1792 bytes): #5272(1380), #5273(412) 2]
Transport Layer Security
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
Content Type: Handshake (22)
Version: TLS 1.0 (0x0301)
Length: 1787
Handshake Protocol: Client Hello
Handshake Type: Client Hello (1)
Length: 1783
Profile: Default
Packets: 48877 · Displayed: 196 (0.4%)
traffic-analysis-exercise.pcap-2025-06-13
07:05 ص
٢٠٢٦/١/٠٣



2️⃣ Environment & Scope

- **Traffic source: Internal workstation (10.6.13.133)**
  - **Data analyzed: PCAP network capture**
  - **Tools used:**
- **Wireshark**
- **VirusTotal**
- **urlscan.io**
- **InfoSec Exchange**
  - **Objective:**
- **Identify malicious activity**
- **Determine attacker infrastructure**
- **Extract IOCs**

Initial Detection (PCAP Analysis):

Suspicious Network Pattern

> Repeated outbound HTTP POST requests were observed at fixed intervals (~30 seconds).
> Requests contained randomized URI paths and small payload sizes.

example :

`POST /gS1jCqsFm25cY&d50db1c8f3b479e17a996a76a77e4d54/vo6cqHO2 HTTP/1.1`

why suspicious ?

- Randomized paths
- Beacon-like timing
- No legitimate User-Agent behavior

Cloudflare Evasion Identified

> Destination IP addresses varied across multiple packets butall belongedto Cloudflare ASN.

why ?

Attackers intentionally use Cloudflare to mask the real origin server and complicate IP-based attribution.

TLS Analysis & SNI Pivoting

First Suspicious TLS Session

```
TLSClient Hello
SNI: dng-microsoftds.com
```

📌 **why SNI?**

- SNI reveals the real domain requested before encryption
- More reliable than destination IP behind Cloudflare

Domain Pivoting

Additional suspicious domains identified:

```
event-time-microsoft.org
eventdata-microsoft.live
hillcoweb.com
```

📌 Naming pattern:

- Microsoft-themed domains
- Typosquatting / masquerading behavior

Reputation & Infrastructure Analysis VirusTotal

```
hillcoweb.com flaggedas suspiciousby multiple engines.
```

urlscan.io

Findings:

- Domain scanned repeatedly over several days

- Presence of js.php endpoint
- Minimal response sizes
- Single backend IP behavior

📌 **Interpretation:**

> These characteristics are consistent with C2 infrastructure rather than legitimate web hosting.

Behavioral Correlation

TLS session ➜Initial HTTPGET ➜ Repeated HTTP POST beaconing

- Proven kill chain
- Not random traffic
- Full malware lifecycle

Indicators of Compromise (IOCs)

Domains:

publichillcoweb.com
dng-microsoftds.com
event-time-microsoft.org
eventdata-microsoft.live

IPs:

Multiple Cloudflare IPs (intentionally excludedasprimary IOCs)

Network Indicators:

- RepeatedPOSTrequests
- RandomizedURIpaths
- Smallpayloadsizes
- Periodicbeaconintervals

Conclusion

This investigation confirms the presenceof malicious beaconing activityfrom t he affected workstation.
The attacker leveraged Cloudflareto hide the command-and-controlserver, re quiringdomain-based analysis via TLS SNI rather than IP-based detection.