Incident Report: Fake Google Authenticator Infection Analysis

***Date:** December 27, 2025* ***Analyst:** Obioma Felicity Uzoh* ***Case ID:** MTA-2025-01-22* ***Severity:** High*

1. Executive Summary

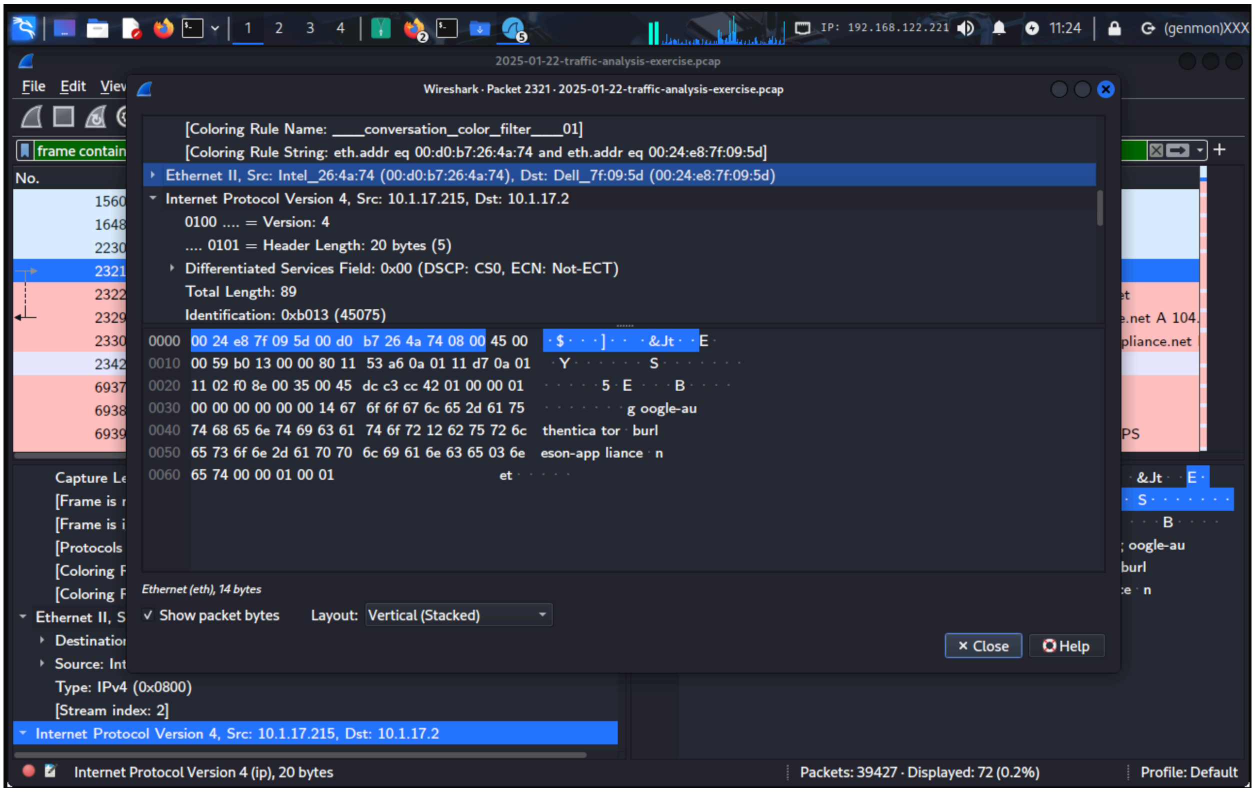
On January 22, 2025, the Security Operations Center (SOC) received a report regarding a potential malware infection. A user reportedly attempted to download "Google Authenticator" but was redirected to a suspicious website.

This report details the forensic analysis of the captured network traffic (PCAP). The investigation confirmed that an internal host visited a fake software site, resulting in the download of a malicious payload and subsequent Command and Control (C2) communication. The infected host has been identified and the malicious domains have been documented for blocking.

2. Technical Analysis

2.1 Incident Scope & Victim Identification

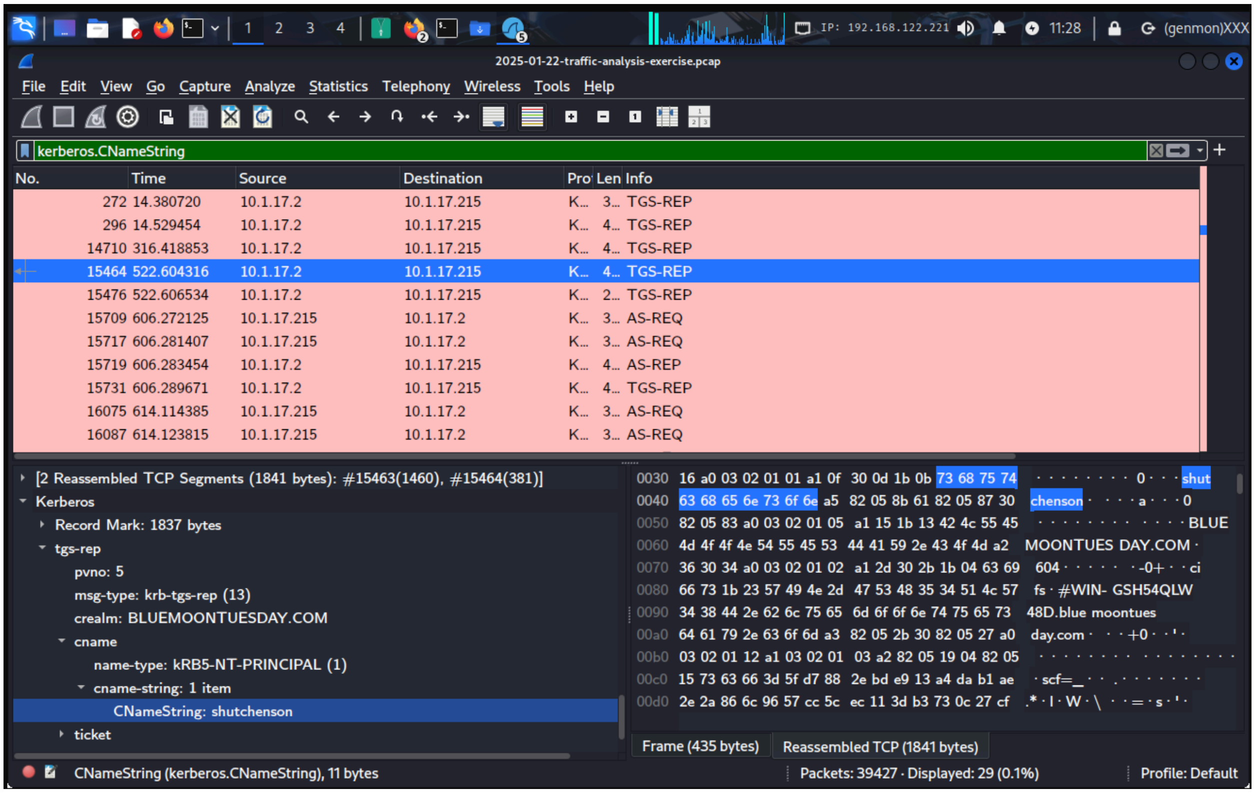
> The investigation began with the detection of anomalous network traffic on the subnet `10.1.17.0/24`. By correlating the alert time with DHCP and Kerberos authentication logs, we successfully isolated the specific endpoint responsible for the activity.
>
> Analysis confirmed the source of the infection was a corporate workstation identified as **DESKTOP-L8C5GSJ**. Using Kerberos traffic (frame 15464), we attributed the session to the user account **`shutchenson`**. The device’s physical address (`00:d0:b7:26:4a:74`) was documented to facilitate isolation at the switch level.



```
2025-01-22-traffic-analysis-exercise.pcap
Wireshark · Packet 2321 · 2025-01-22-traffic-analysis-exercise.pcap

    [Coloring Rule Name: ____conversation_color_filter____01]
    [Coloring Rule String: eth.addr eq 00:d0:b7:26:4a:74 and eth.addr eq 00:24:e8:7f:09:5d]
› Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Dell_7f:09:5d (00:24:e8:7f:09:5d)
˅ Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  › Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 89
    Identification: 0xb013 (45075)

0000  00 24 e8 7f 09 5d 00 d0  b7 26 4a 74 08 00 45 00   ·$···]·· ·&Jt··E·
0010  00 59 b0 13 00 00 80 11  53 a6 0a 01 11 d7 0a 01   ·Y······ S·······
0020  11 02 f0 8e 00 35 00 45  dc c3 cc 42 01 00 00 01   ·····5·E ···B····
0030  00 00 00 00 00 00 14 67  6f 6f 67 6c 65 2d 61 75   ·······g oogle-au
0040  74 68 65 6e 74 69 63 61  74 6f 72 12 62 75 72 6c   thentica tor·burl
0050  65 73 6f 6e 2d 61 70 70  6c 69 61 6e 63 65 03 6e   eson-app liance·n
0060  65 74 00 00 01 00 01                               et·····

Ethernet (eth), 14 bytes
✓ Show packet bytes     Layout: Vertical (Stacked)
✕ Close   Help
```

```
frame contain
No.
1560
1648
2230
2321
2322
2329
2330
2342
6937
6938
6939
    Capture Le
    [Frame is r
    [Frame is i
    [Protocols
    [Coloring F
    [Coloring F
˅ Ethernet II, S
  › Destination
  › Source: Int
    Type: IPv4 (0x0800)
    [Stream index: 2]
˅ Internet Protocol Version 4, Src: 10.1.17.215, Dst: 10.1.17.2

Internet Protocol Version 4 (ip), 20 bytes      Packets: 39427 · Displayed: 72 (0.2%)      Profile: Default
```

Figure 1: Network packet details identifying the victim IP and MAC.



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

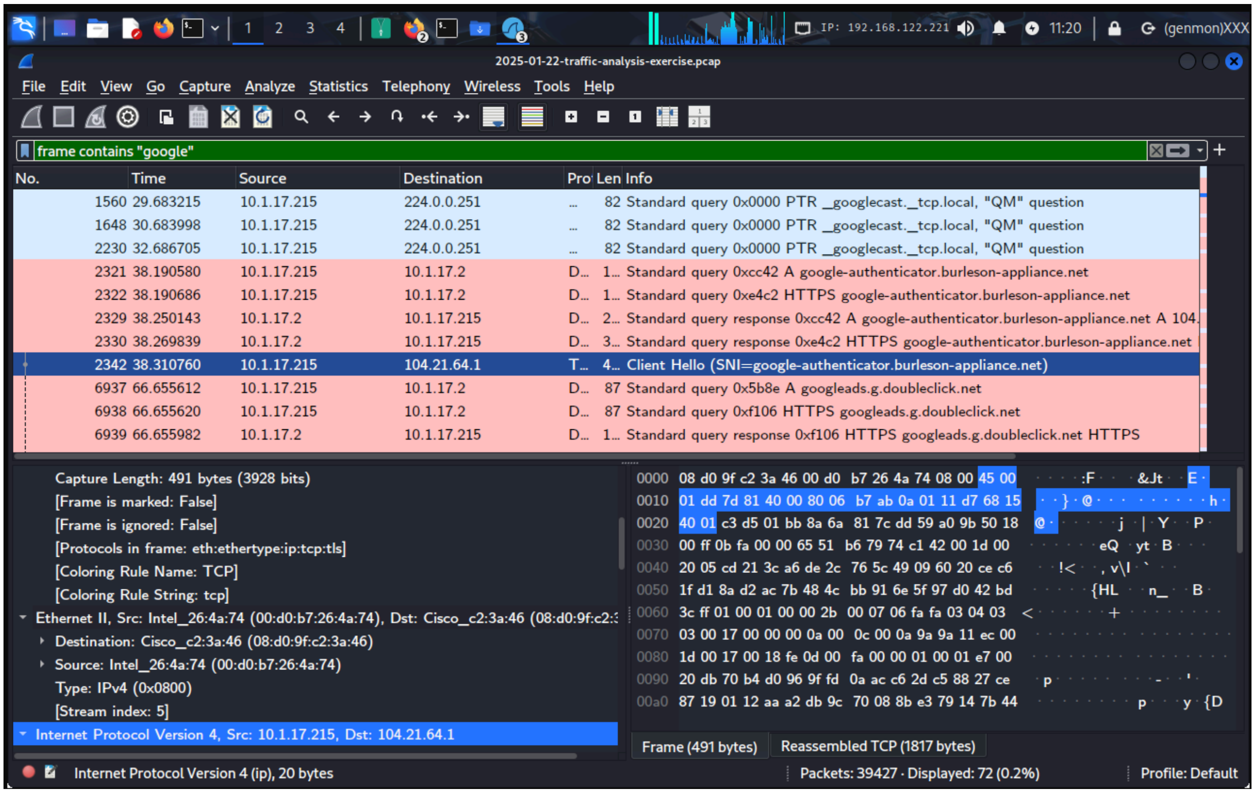
```
2025-01-22-traffic-analysis-exercise.pcap
kerberos.CNameString

No.    Time        Source       Destination  Pro Len Info
  272  14.380720   10.1.17.2    10.1.17.215  K... 3... TGS-REP
  296  14.529454   10.1.17.2    10.1.17.215  K... 4... TGS-REP
14710  316.418853  10.1.17.2    10.1.17.215  K... 4... TGS-REP
15464  522.604316  10.1.17.2    10.1.17.215  K... 4... TGS-REP
15476  522.606534  10.1.17.2    10.1.17.215  K... 2... TGS-REP
15709  606.272125  10.1.17.215  10.1.17.2    K... 3... AS-REQ
15717  606.281407  10.1.17.215  10.1.17.2    K... 3... AS-REQ
15719  606.283454  10.1.17.2    10.1.17.215  K... 4... AS-REP
15731  606.289671  10.1.17.2    10.1.17.215  K... 4... TGS-REP
16075  614.114385  10.1.17.215  10.1.17.2    K... 3... AS-REQ
16087  614.123815  10.1.17.215  10.1.17.2    K... 3... AS-REQ

› [2 Reassembled TCP Segments (1841 bytes): #15463(1460), #15464(381)]
˅ Kerberos
  › Record Mark: 1837 bytes
  ˅ tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: BLUEMOONTUESDAY.COM
    ˅ cname
        name-type: kRB5-NT-PRINCIPAL (1)
      ˅ cname-string: 1 item
          CNameString: shutchenson
    › ticket

0030  16 a0 03 02 01 01 a1 0f  30 0d 1b 0b 73 68 75 74   ·········0···shut
0040  63 68 65 6e 73 6f 6e a5  82 05 8b 61 82 05 87 30   chenson· ···a···0
0050  82 05 83 a0 03 02 01 05  a1 15 1b 13 42 4c 55 45   ········ ····BLUE
0060  4d 4f 4f 4e 54 55 45 53  44 41 59 2e 43 4f 4d a2   MOONTUES DAY.COM·
0070  36 30 34 a0 03 02 01 02  a1 2d 30 2b 1b 04 63 69   604····· ·-0+··ci
0080  66 73 1b 23 57 49 4e 2d  47 53 48 35 34 51 4c 57   fs·#WIN- GSH54QLW
0090  34 38 44 2e 62 6c 75 65  6d 6f 6f 6e 74 75 65 73   48D.blue moontues
00a0  64 61 79 2e 63 6f 6d a3  82 05 2b 30 82 05 27 a0   day.com· ··+0··'·
00b0  03 02 01 12 a1 03 02 01  03 a2 82 05 19 04 82 05   ········ ········
00c0  15 73 63 66 3d 5f d7 88  2e bd e9 13 a4 da b1 ae   ·scf=_·· .·······
00d0  2e 2a 86 6c 96 57 cc 5c  ec 11 3d b3 73 0c 27 cf   .*·l·W·\ ··=·s·'·

Frame (435 bytes)   Reassembled TCP (1841 bytes)
CNameString (kerberos.CNameString), 11 bytes      Packets: 39427 · Displayed: 29 (0.1%)      Profile: Default
```

Figure 2: Kerberos Ticket Granting Service (TGS) request revealing the active user.

2.2 Infection Vector (The "Click")

We reconstructed the user’s browsing history leading up to the infection. At approximately 19:45 UTC, the user performed a DNS lookup for a Google Authenticator download.

Instead of the legitimate Google domain, the user was redirected to a spoofed domain: `google-authenticator.burleson-appliance.net`. This domain hosted a malicious web page that likely utilized social engineering to trick the user into downloading a fake installer. The traffic analysis shows an encrypted HTTPS session (Client Hello) established immediately after the DNS resolution, indicating the payload download was successful.



2025-01-22-traffic-analysis-exercise.pcap

frame contains "google"

```
No.       Time       Source        Destination    Pro Len Info
     1560 29.683215  10.1.17.215   224.0.0.251    ...  82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
     1648 30.683998  10.1.17.215   224.0.0.251    ...  82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
     2230 32.686705  10.1.17.215   224.0.0.251    ...  82 Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
     2321 38.190580  10.1.17.215   10.1.17.2      D... 1... Standard query 0xcc42 A google-authenticator.burleson-appliance.net
     2322 38.190686  10.1.17.215   10.1.17.2      D... 1... Standard query 0xe4c2 HTTPS google-authenticator.burleson-appliance.net
     2329 38.250143  10.1.17.2     10.1.17.215    D... 2... Standard query response 0xcc42 A google-authenticator.burleson-appliance.net A 104.
     2330 38.269839  10.1.17.2     10.1.17.215    D... 3... Standard query response 0xe4c2 HTTPS google-authenticator.burleson-appliance.net
     2342 38.310760  10.1.17.215   104.21.64.1    T... 4... Client Hello (SNI=google-authenticator.burleson-appliance.net)
     6937 66.655612  10.1.17.215   10.1.17.2      D...  87 Standard query 0x5b8e A googleads.g.doubleclick.net
     6938 66.655620  10.1.17.215   10.1.17.2      D...  87 Standard query 0xf106 HTTPS googleads.g.doubleclick.net
     6939 66.655982  10.1.17.2     10.1.17.215    D... 1... Standard query response 0xf106 HTTPS googleads.g.doubleclick.net HTTPS
```

```
    Capture Length: 491 bytes (3928 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:tls]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
▾ Ethernet II, Src: Intel_26:4a:74 (00:d0:b7:26:4a:74), Dst: Cisco_c2:3a:46 (08:d0:9f:c2:3
  ▸ Destination: Cisco_c2:3a:46 (08:d0:9f:c2:3a:46)
  ▸ Source: Intel_26:4a:74 (00:d0:b7:26:4a:74)
    Type: IPv4 (0x0800)
    [Stream index: 5]
▾ Internet Protocol Version 4, Src: 10.1.17.215, Dst: 104.21.64.1
```

```
0000  08 d0 9f c2 3a 46 00 d0  b7 26 4a 74 08 00 45 00   ····:F··&Jt··E·
0010  01 dd 7d 81 40 00 80 06  b7 ab 0a 01 11 d7 68 15   ··}·@·········h·
0020  40 01 c3 d5 01 bb 8a 6a  81 7c dd 59 a0 9b 50 18   @······j·|·Y··P·
0030  00 ff 0b fa 00 00 65 51  b6 79 74 c1 42 00 1d 00   ······eQ·yt·B···
0040  20 05 cd 21 3c a6 de 2c  76 5c 49 09 60 20 ce c6    ··!<··,v\I·`···
0050  1f d1 8a d2 ac 7b 48 4c  bb 91 6e 5f 97 d0 42 bd   ·····{HL··n_··B·
0060  3c ff 01 00 01 00 00 2b  00 07 06 fa fa 03 04 03   <······+········
0070  03 00 17 00 00 00 0a 00  0c 00 0a 9a 9a 11 ec 00   ················
0080  1d 00 17 00 18 fe 0d 00  fa 00 00 01 00 01 e7 00   ················
0090  20 db 70 b4 d0 96 9f fd  0a ac c6 2d c5 88 27 ce    ·p·········-··'·
00a0  87 19 01 12 aa a2 db 9c  70 08 8b e3 79 14 7b 44   ········p···y·{D
```

Frame (491 bytes) | Reassembled TCP (1817 bytes)

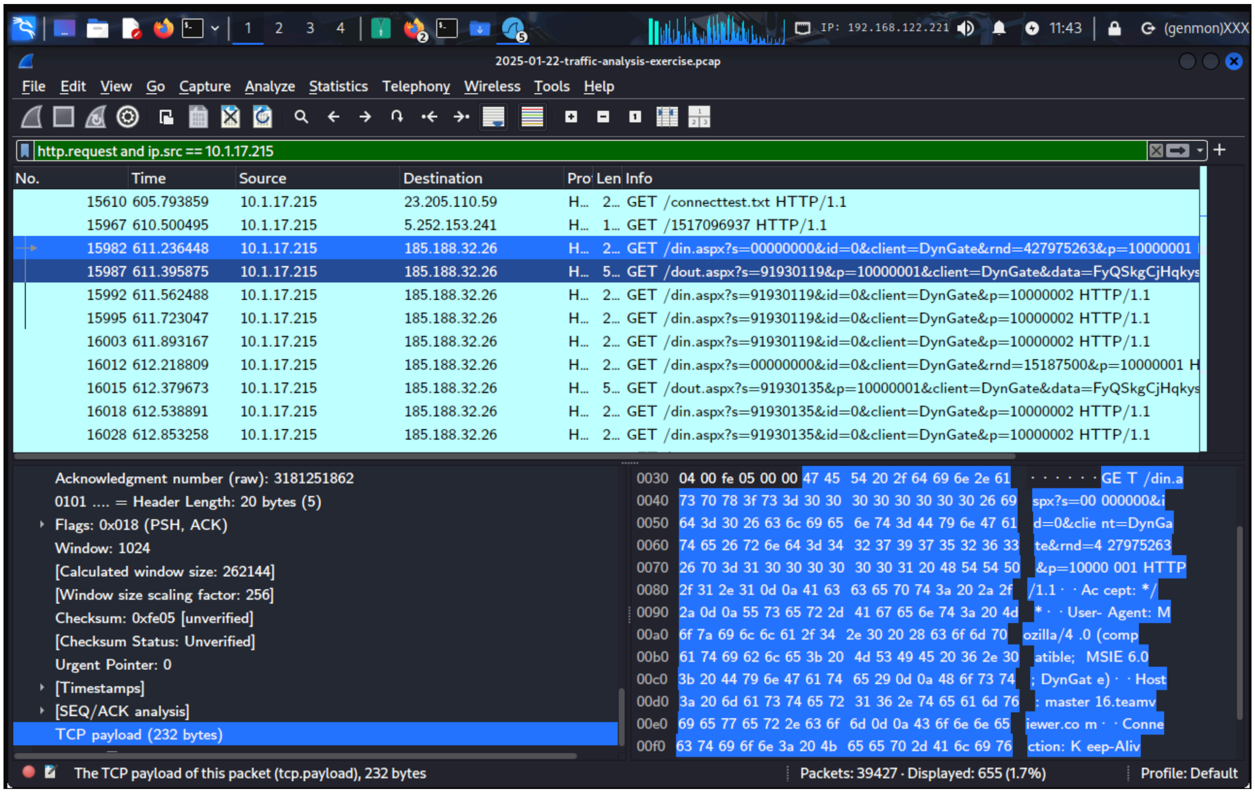
Internet Protocol Version 4 (ip), 20 bytes · Packets: 39427 · Displayed: 72 (0.2%) · Profile: Default

Figure 3: DNS query and subsequent connection to the malicious spoofed domain.

2.3 Post-Infection Activity (The "Call Home")

Approximately 10 minutes after the initial compromise, the infected host began exhibiting Command & Control (C2) behavior. The host initiated multiple HTTP GET requests to the external IP `185.188.32.26`.

Deep packet inspection of this traffic revealed clear Indicators of Compromise (IOCs). The malware utilized a known URL pattern (`/din.aspx` and `/dout.aspx`) associated with **TeamViewer (DynGate)**, a remote access tool often repurposed by attackers as a Remote Access Trojan (RAT). Frame 15987 captures the malware actively exfiltrating encoded data (likely system information) to the attacker's server.



```
http.request and ip.src == 10.1.17.215

No.    Time        Source       Destination     Pro Len Info
 15610 605.793859  10.1.17.215  23.205.110.59   H... 2... GET /connecttest.txt HTTP/1.1
 15967 610.500495  10.1.17.215  5.252.153.241   H... 1... GET /1517096937 HTTP/1.1
 15982 611.236448  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=427975263&p=10000001
 15987 611.395875  10.1.17.215  185.188.32.26   H... 5... GET /dout.aspx?s=91930119&p=10000001&client=DynGate&data=FyQSkgCjHqkys
 15992 611.562488  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=91930119&id=0&client=DynGate&p=10000002 HTTP/1.1
 15995 611.723047  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=91930119&id=0&client=DynGate&p=10000002 HTTP/1.1
 16003 611.893167  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=91930119&id=0&client=DynGate&p=10000002 HTTP/1.1
 16012 612.218809  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=00000000&id=0&client=DynGate&rnd=15187500&p=10000001 H
 16015 612.379673  10.1.17.215  185.188.32.26   H... 5... GET /dout.aspx?s=91930135&p=10000001&client=DynGate&data=FyQSkgCjHqkys
 16018 612.538891  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=91930135&id=0&client=DynGate&p=10000002 HTTP/1.1
 16028 612.853258  10.1.17.215  185.188.32.26   H... 2... GET /din.aspx?s=91930135&id=0&client=DynGate&p=10000002 HTTP/1.1
```

```
    Acknowledgment number (raw): 3181251862
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x018 (PSH, ACK)
    Window: 1024
    [Calculated window size: 262144]
    [Window size scaling factor: 256]
    Checksum: 0xfe05 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
  › [SEQ/ACK analysis]
    TCP payload (232 bytes)
```

```
0030  04 00 fe 05 00 00 47 45  54 20 2f 64 69 6e 2e 61   ······GE T /din.a
0040  73 70 78 3f 73 3d 30 30  30 30 30 30 30 30 26 69   spx?s=00 000000&i
0050  64 3d 30 26 63 6c 69 65  6e 74 3d 44 79 6e 47 61   d=0&clie nt=DynGa
0060  74 65 26 72 6e 64 3d 34  32 37 39 37 35 32 36 33   te&rnd=4 27975263
0070  26 70 3d 31 30 30 30 30  30 30 31 20 48 54 54 50   &p=10000 001 HTTP
0080  2f 31 2e 31 0d 0a 41 63  63 65 70 74 3a 20 2a 2f   /1.1··Ac cept: */
0090  2a 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   *··User- Agent: M
00a0  6f 7a 69 6c 6c 61 2f 34  2e 30 20 28 63 6f 6d 70   ozilla/4 .0 (comp
00b0  61 74 69 62 6c 65 3b 20  4d 53 49 45 20 36 2e 30   atible;  MSIE 6.0
00c0  3b 20 44 79 6e 47 61 74  65 29 0d 0a 48 6f 73 74   ; DynGat e)··Host
00d0  3a 20 6d 61 73 74 65 72  31 36 2e 74 65 61 6d 76   : master 16.teamv
00e0  69 65 77 65 72 2e 63 6f  6d 0d 0a 43 6f 6e 6e 65   iewer.co m··Conne
00f0  63 74 69 6f 6e 3a 20 4b  65 65 70 2d 41 6c 69 76   ction: K eep-Aliv
```

```
The TCP payload of this packet (tcp.payload), 232 bytes    Packets: 39427 · Displayed: 655 (1.7%)    Profile: Default
```

Figure 4: Malicious C2 beacon containing encoded data exfiltration

3. Conclusion & Recommendations

3.1 Incident Summary

The forensic analysis of the captured network traffic confirms that the host `10.1.17.215` was successfully compromised by a "Fake Software" social engineering attack. The attacker achieved code execution and established a persistent command and control (C2) channel using a Remote Access Trojan (TeamViewer/DynGate).

3.2 Immediate Actions Required (Remediation)

Based on these findings, the following actions are recommended to contain and eradicate the threat:

1. **Isolate the Endpoint:** Immediately disconnect `10.1.17.215` (MAC: `00:d0:b7:26:4a:74`) from the corporate network to prevent lateral movement.
2. **Network Blocking:** Implement block rules at the firewall for the identified malicious C2 IP (`185.188.32.26`) and the spoofed domain (`*.burleson-appliance.net`).
3. **Credential Reset:** Force a password reset for the user account `shutchenson`, as their credentials may have been scraped by the malware.
4. **Re-image the Host:** Due to the installation of a Remote Access Tool (RAT), the machine should be considered fully compromised. Do not attempt to "clean" it; wipe and re-image the device from a known good backup.