WIRESHARK TRAFFIC ANALYSIS REPORT

Prepared by: (Ngah Derick Bongnso)

Date: (11/30/2025)

EXECUTIVE SUMMARY

This report analyzes a packet capture (PCAP) using Wireshark. The capture revealed repeated HTTP transfers of files disguised as JPEG images, which TRiD analysis later confirmed were Windows executable binaries. Additional CAB downloads were observed from Windows Update servers. This behavior indicates possible malware activity, covert data transfer, or command-and-control communication.

ANALYSIS ENVIRONMENT

Tool Used: Wireshark

Additional Tool: TRiD

Protocols Analyzed: HTTP, TCP

Source: Provided PCAP file

KEY FINDINGS

1. Suspicious JPEG Downloads from Host 2.56.57.108

Multiple files were downloaded through HTTP from the same host:

Hostname: 2.56.57.108

Files downloaded as “image/jpeg” but suspicious in size and pattern.

List of extracted objects:

Packet #: 1639

Hostname: 2.56.57.108

Content Type: image/jpeg

Size: 144 kB

Filename: 6.jpg

Packet #: 2239

Hostname: 2.56.57.108

Content Type: image/jpeg

Size: 645 kB

Filename: 1.jpg

Packet #: 2539

Hostname: 2.56.57.108

Content Type: image/jpeg

Size: 334 kB

Filename: 2.jpg

Packet #: 3052

Hostname: 2.56.57.108

Content Type: image/jpeg

Size: 440 kB

Filename: 4.jpg

Packet #: 4192

Hostname: 2.56.57.108

Content Type: image/jpeg

Size: 1246 kB

Filename: 5.jpg

Packet #: 4273

Hostname: 2.56.57.108

Content Type: image/jpeg

Size: 83 kB

Filename: 7.jpg

Assessment: This repetition indicates abnormal, automated behavior such as:

- Malware staging
- Command-and-control (C2) beaconing
- Steganography (data hidden in images)
- File masquerading
- Suspicious payload delivery

2. CAB Files Downloaded from Windows Update Host

Source Host: download.windowsupdate.com

File Types: application/octet-stream (CAB files)

While some Windows Update traffic is normal, it can also be used to disguise malicious transfers.

Recommendation: Verify hashes and signatures using:

- VirusTotal
- Sigcheck
- Microsoft update catalog

TRiD FILE IDENTIFICATION RESULTS

TRiD revealed that the JPEG files were actually Windows executables:

File: 1.jpg

TRiD result: 32% (.EXE) Microsoft Visual C++ Executable

File: 2.jpg

TRiD result: 47.3% (.EXE) Win64 Executable (MS Visual C++)

File: 3.jpg

TRiD result: 32% (.EXE) Win64 Executable

File: 4.jpg

TRiD result: 47.3% (.EXE) Win32 Executable (Visual C++)

File: 5.jpg

TRiD result: 32.2% (.EXE) Win64 Executable

File: 7.jpg

TRiD result: 47.3% (.EXE) Win32 Executable

Interpretation:

- Files disguised as images = classic malware obfuscation.
- Likely malicious payloads downloaded via HTTP.
- Very strong indicators of compromise (IoCs).

INDICATORS OF COMPROMISE (IOCs)

Suspicious Host:

2.56.57.108

Malicious or Suspicious Files:

1.jpg

2.jpg

3.jpg

4.jpg

5.jpg

7.jpg

Behavioral IoCs:

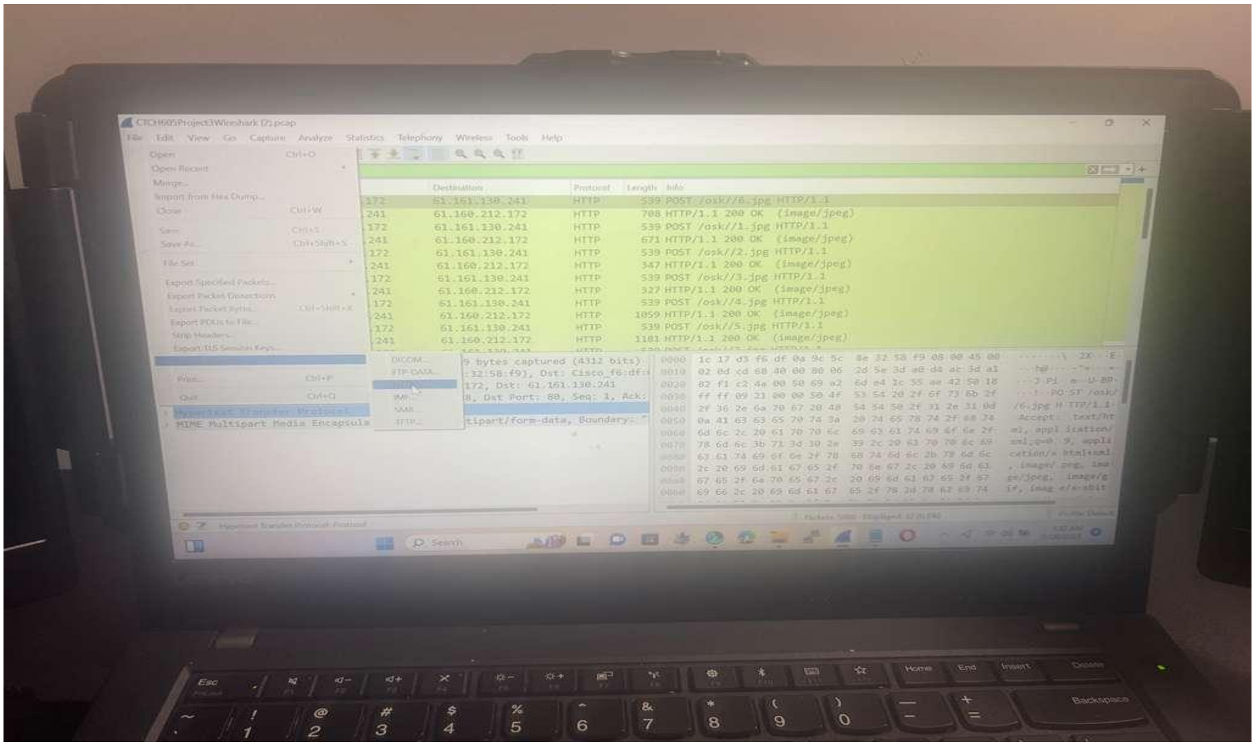
- High-frequency downloads
- Image files that are actually executables
- Repeated contact with a single suspicious IP
- Possible staged payload chain

CONCLUSION

The packet capture provides strong evidence of malicious network activity. The disguised executable files originating from a suspicious IP, combined with repetitive HTTP downloads, strongly suggest malware distribution or C2 activity. Further analysis is highly recommended to confirm if the system was compromised.

RECOMMENDED NEXT STEPS

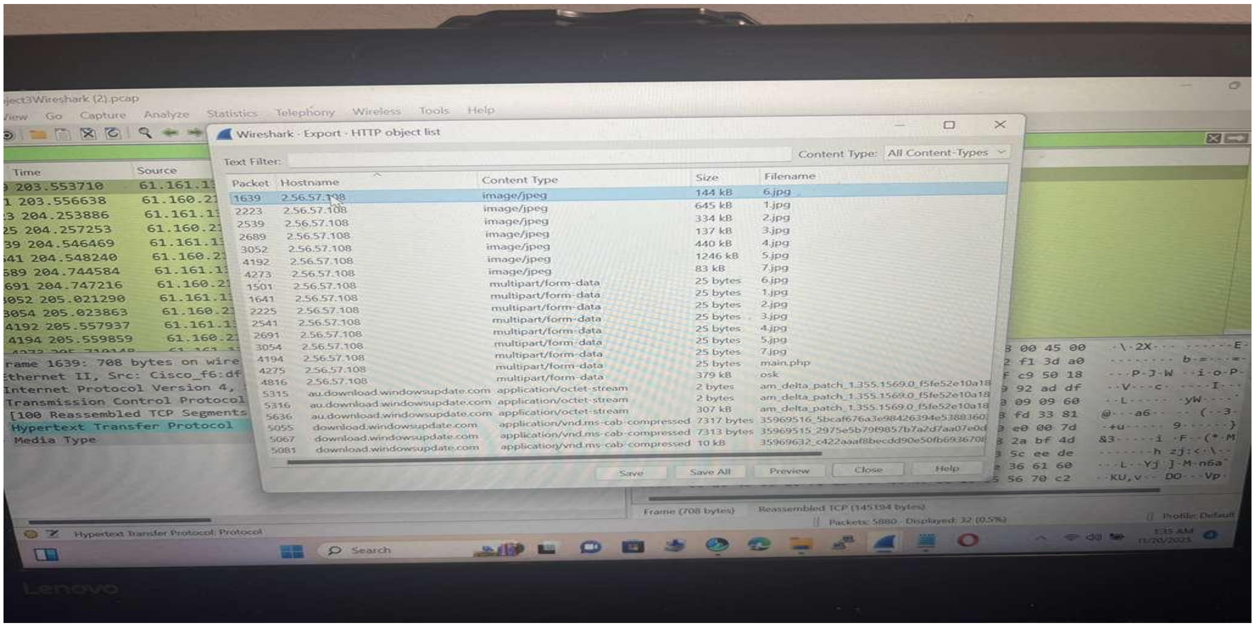
1. Block IP address 2.56.57.108 at the firewall.
2. Upload all suspicious files to VirusTotal.
3. Conduct static and dynamic malware analysis on extracted files.
4. Perform endpoint scans on affected machines.
5. Review logs for additional connections to suspicious IPs.
6. Monitor network for similar traffic patterns.


CTCH605Project3Wireshark (2).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge...
Import from Hex Dump...
Close Ctrl+W
Save Ctrl+S
Save As... Ctrl+Shift+S
File Set
Export Specified Packets...
Export Packet Dissections
Export Packet Bytes... Ctrl+Shift+X
Export PDUs to File...
Strip Headers...
Export TLS Session Keys...
Print... Ctrl+P
Quit Ctrl+Q
DICOM...
FTP-DATA...
HTTP...
IMF...
SMB...
TFTP...

```
     Destination        Protocol  Length Info
.172  61.161.130.241    HTTP       539 POST /osk//6.jpg HTTP/1.1
.241  61.160.212.172    HTTP       708 HTTP/1.1 200 OK  (image/jpeg)
.172  61.161.130.241    HTTP       539 POST /osk//1.jpg HTTP/1.1
.241  61.160.212.172    HTTP       671 HTTP/1.1 200 OK  (image/jpeg)
.172  61.161.130.241    HTTP       539 POST /osk//2.jpg HTTP/1.1
.241  61.160.212.172    HTTP       347 HTTP/1.1 200 OK  (image/jpeg)
.172  61.161.130.241    HTTP       539 POST /osk//3.jpg HTTP/1.1
.241  61.160.212.172    HTTP       327 HTTP/1.1 200 OK  (image/jpeg)
.172  61.161.130.241    HTTP       539 POST /osk//4.jpg HTTP/1.1
.241  61.160.212.172    HTTP      1059 HTTP/1.1 200 OK  (image/jpeg)
.172  61.161.130.241    HTTP       539 POST /osk//5.jpg HTTP/1.1
.241  61.160.212.172    HTTP      1181 HTTP/1.1 200 OK  (image/jpeg)

9 bytes captured (4312 bits)
:32:58:f9), Dst: Cisco_f6:df:
172, Dst: 61.161.130.241
8, Dst Port: 80, Seq: 1, Ack:
Hypertext Transfer Protocol
MIME Multipart Media Encapsula   tipart/form-data, Boundary: "

0000  1c 17 d3 f6 df 0a 9c 5c  8e 32 58 f9 08 00 45 00
0010  02 0d cd 68 40 00 80 06  2d 5e 3d a0 d4 ac 3d a1
0020  82 f1 c2 4a 00 50 69 a2  6d e4 1c 55 ae 42 50 18
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
0080  63 61 74 69 6f 6e 2f 78  68 74 6d 6c 2b 78 6d 6c   cation/x html+xml
```

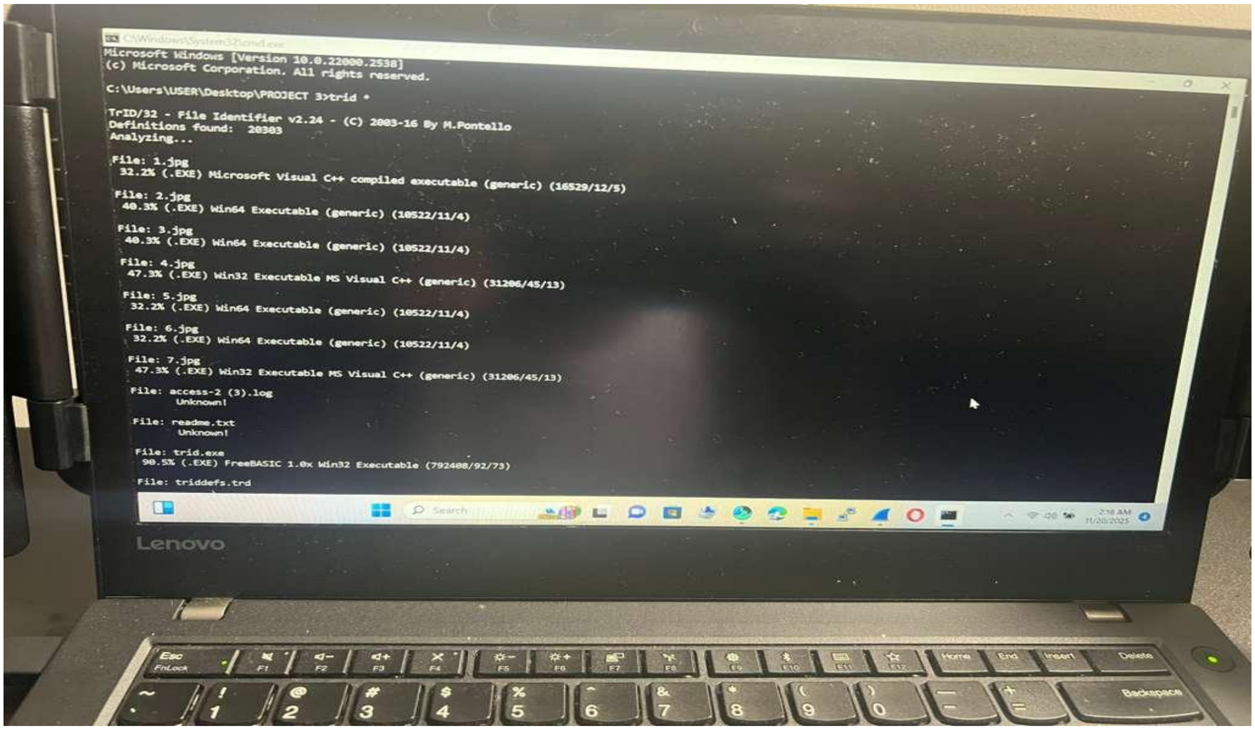

ject3Wireshark (2).pcap
View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
Close
Help
Search
Lenovo

```
Packet Hostname                        Content Type                          Size        Filename
1639   2.56.57.108                     image/jpeg                            144 kB      6.jpg
2223   2.56.57.108                     image/jpeg                            645 kB      1.jpg
2539   2.56.57.108                     image/jpeg                            334 kB      2.jpg
2689   2.56.57.108                     image/jpeg                            137 kB      3.jpg
3052   2.56.57.108                     image/jpeg                            440 kB      4.jpg
4192   2.56.57.108                     image/jpeg                            1246 kB     5.jpg
4273   2.56.57.108                     image/jpeg                            83 kB       7.jpg
1501   2.56.57.108                     multipart/form-data                   25 bytes    6.jpg
1641   2.56.57.108                     multipart/form-data                   25 bytes    1.jpg
2225   2.56.57.108                     multipart/form-data                   25 bytes    2.jpg
2541   2.56.57.108                     multipart/form-data                   25 bytes    3.jpg
2691   2.56.57.108                     multipart/form-data                   25 bytes    4.jpg
3054   2.56.57.108                     multipart/form-data                   25 bytes    5.jpg
4194   2.56.57.108                     multipart/form-data                   25 bytes    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
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
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_c422aaaf8becdd90e50fb6936708
```

```
Time              Source
9 203.553710      61.161.1
1 203.556638      61.160.2
3 204.253886      61.161.1
25 204.257253     61.160.2
39 204.546469     61.161.1
41 204.548240     61.160.2
589 204.744584    61.161.1
691 204.747216    61.160.2
3052 205.021290   61.161.1
3054 205.023863   61.160.2
4192 205.557937   61.161.1
4194 205.559859   61.160.2

rame 1639: 708 bytes on wire
thernet II, Src: Cisco_f6:df
Internet Protocol Version 4,
Transmission Control Protocol
[100 Reassembled TCP Segments
Hypertext Transfer Protocol
Media Type

Frame (708 bytes)   Reassembled TCP (145194 bytes)
Packets: 5880 · Displayed: 32 (0.5%)   Profile: Default
Hypertext Transfer Protocol: Protocol
1:35 AM 11/20/2023
```



```
Microsoft Windows [Version 10.0.22000.2538]
(c) Microsoft Corporation. All rights reserved.

C:\Users\USER\Desktop\PROJECT 3>trid *

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello
Definitions found:  20303
Analyzing...

File: 1.jpg
 32.2% (.EXE) Microsoft Visual C++ compiled executable (generic) (16529/12/5)

File: 2.jpg
 40.3% (.EXE) Win64 Executable (generic) (10522/11/4)

File: 3.jpg
 40.3% (.EXE) Win64 Executable (generic) (10522/11/4)

File: 4.jpg
 47.3% (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13)

File: 5.jpg
 32.2% (.EXE) Win64 Executable (generic) (10522/11/4)

File: 6.jpg
 32.2% (.EXE) Win64 Executable (generic) (10522/11/4)

File: 7.jpg
 47.3% (.EXE) Win32 Executable MS Visual C++ (generic) (31206/45/13)

File: access-2 (3).log
        Unknown!

File: readme.txt
        Unknown!

File: trid.exe
 90.5% (.EXE) FreeBASIC 1.0x Win32 Executable (792408/92/73)

File: triddefs.trd
```