

MALWARE ANALYSIS

Malware analysis is the process of examining malicious software (malware) to understand its functionality, behavior, and purpose. This is done in order to gain insights into how the malware operates, identify its potential risks, and develop effective strategies for detection, prevention, and mitigation.

There are generally three main approaches to malware analysis:

Static Analysis:

This involves examining the malware without executing it. Analysts inspect the code, file structure, and other attributes to identify known patterns or signatures associated with malicious software. Static analysis techniques include examining file headers, disassembling or decompiling code, and looking for suspicious or obfuscated content.

Dynamic Analysis:

In this approach, the malware is executed in a controlled environment, often within a sandbox or virtual machine. Analysts monitor its behavior, such as file system changes, network communications, system calls, and registry modifications. This provides insights into the malware's actions in real-time.

Hybrid Analysis:

Combining elements of both static and dynamic analysis, hybrid analysis seeks to leverage the strengths of each approach. For example, static analysis might reveal certain indicators of compromise (IOCs) before running the malware dynamically for a more comprehensive understanding of its behavior.

❖ STATIC ANALYSIS:

Tools used:

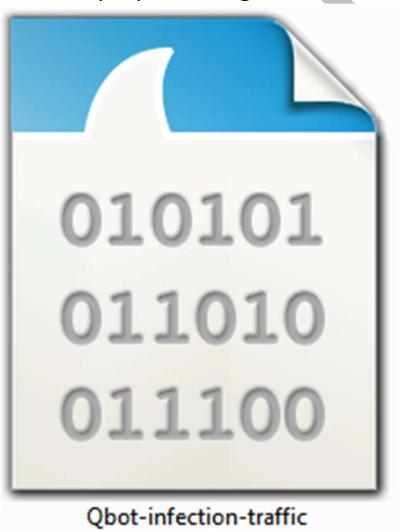
- Wireshark
- Hex editor
- Virus analyzer(virustotal.com)
-

STEPS INVOLVED:

[png file analysis]

1) Capture the traffic analysis:

Obtain a pcap file using Wireshark.



2) Apply a filter to isolate HTTP GET requests (http.request.method == GET) :

Screenshot of Wireshark showing captured traffic from "Qbot-infection-traffic.pcap". A filter has been applied to show only HTTP GET requests.

Selected Filter: http.request.method == GET

Packets: 74404 · Displayed: 13 (0.0%) · Profile: Default

Selected Packet (Frame 19):

```

Frame 19: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Tp-LinkT_27:87:7f (ec:08:6b:27:87:7f), Dst: ASUSTekC_56:33:ea (04:d4:c4:56:33:ea)
Internet Protocol Version 4, Src: 10.1.29.101, Dst: 13.107.4.52
Transmission Control Protocol, Src Port: 49671, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol

```

Selected Bytes (Hex View):

```

0000 04 d4 c4 56 33 ea ec 08 6b 27 87 7f 08 00 45 00 ...V3... k'...E...
0010 00 97 b9 01 40 00 80 06 08 5b 0a 01 1d 65 0d 6b ...@... [...e-k
0020 04 34 c2 07 00 50 fb f0 f5 3b 4b 2d 34 26 50 18 -4...P... ;K-4&P-
0030 02 02 82 4c 00 00 47 45 54 20 2f 63 6f 6e 6e 65 ...L...GE T /conne
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest.t xt HTTP/
0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1-Con nection:
0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 Close... User-Age
0070 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 nt: Micr osoft NC
0080 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 SI- Host : www.ms
0090 66 74 63 6f 6e 6e 65 63 74 74 65 73 74 2e 63 6f ftconnec ttest.co
00a0 6d 0d 0a 0d 0a m...

```

3) Identify files:

Through your filtering, you identified two files (PNG and ZIP).

Screenshot of Wireshark showing captured traffic from "Qbot-infection-traffic.pcap". A filter has been applied to show only HTTP GET requests.

Selected Filter: http.request.method == GET

Packets: 74404 · Displayed: 13 (0.0%) · Profile: Default

Selected Packet (Frame 19):

```

Frame 19: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
Ethernet II, Src: Tp-LinkT_27:87:7f (ec:08:6b:27:87:7f), Dst: ASUSTekC_56:33:ea (04:d4:c4:56:33:ea)
Internet Protocol Version 4, Src: 10.1.29.101, Dst: 13.107.4.52
Transmission Control Protocol, Src Port: 49671, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
Hypertext Transfer Protocol

```

Selected Bytes (Hex View):

```

0000 04 d4 c4 56 33 ea ec 08 6b 27 87 7f 08 00 45 00 ...V3... k'...E...
0010 00 97 b9 01 40 00 80 06 08 5b 0a 01 1d 65 0d 6b ...@... [...e-k
0020 04 34 c2 07 00 50 fb f0 f5 3b 4b 2d 34 26 50 18 -4...P... ;K-4&P-
0030 02 02 82 4c 00 00 47 45 54 20 2f 63 6f 6e 6e 65 ...L...GE T /conne
0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest.t xt HTTP/
0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1-Con nection:
0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 Close... User-Age
0070 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 nt: Micr osoft NC
0080 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 SI- Host : www.ms
0090 66 74 63 6f 6e 6e 65 63 74 74 65 73 74 2e 63 6f ftconnec ttest.co
00a0 6d 0d 0a 0d 0a m...

```

4) Png analysis :

Focused on the PNG file.

Opened the PNG packet and followed the TCP stream.

Observed the presence of "MZ" at the beginning, which is indicative of an executable file.

No.	Time	Source	Destination	Protocol	Length	Info
19	0.165516	10.1.29.101	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
248	25.075751	10.1.29.101	183.91.92.1	HTTP	530	GET /wp-content/uploads/2020/01/ahead/9312.zip HTTP/1.1
2498	107.866461	10.1.29.101		HTTP	222	GET /wp-content/uploads/2020/01/ahead/444444.png HTTP/1.1

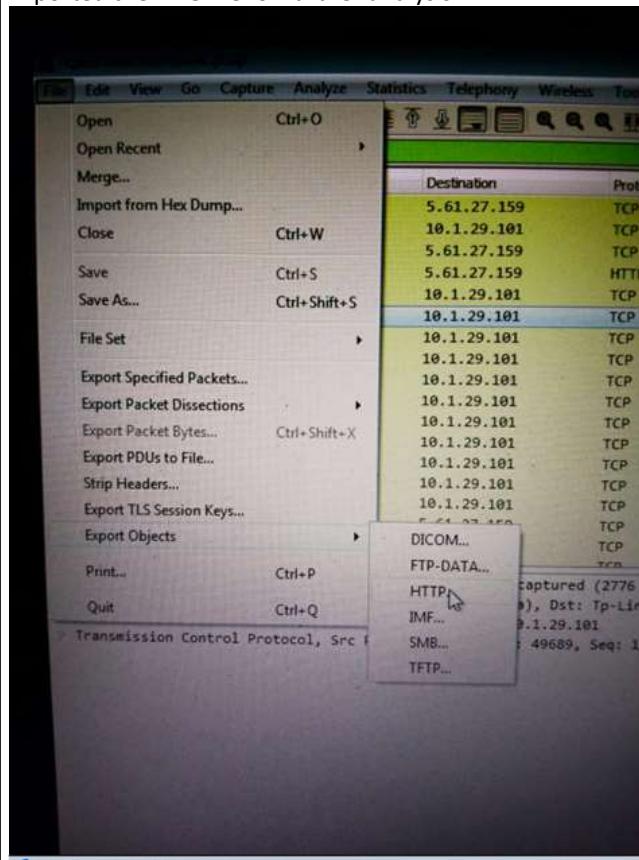
Protocol	Length	Info
HTTP	165	GET /connecttest.txt HTTP/1.1
HTTP	530	GET /wp-content/uploads/2020/01/ahead/9312.zip HTTP/1.1
HTTP	222	GET /wp-content/
HTTP	339	GET /redir_ie.ht
HTTP	268	GET /favicon.ico
HTTP	516	GET /redir_ie.ht
HTTP	456	GET /favicon.ico
HTTP	198	GET /USERTrustEC
HTTP	298	GET /MFEwTzBNMMEs
HTTP	304	GET /ocsp/status
HTTP	341	GET /msdownload/
HTTP	335	GET /msdownload/
HTTP	336	GET /msdownload/

5) Exported objects :

Navigate to the File menu in Wireshark.

Selected "Export Objects" and then "HTTP."

Exported the PNG file for further analysis.



Qbot-infection-traffic.pcap

tcp.stream eq 17

No.	Time	Source
2941	109.728506	5.61.27.159
2942	109.728703	5.61.27.159
2943	109.729084	5.61.27.159
2944	109.729271	5.61.27.159
2945	109.729439	10.1.29.101
2946	109.729440	10.1.29.101
2947	109.729679	5.61.27.159
2948	109.729866	5.61.27.159
2949	109.730256	5.61.27.159
2950	109.730442	5.61.27.159
2951	109.730815	5.61.27.159
2952	109.731003	5.61.27.159
2953	109.731376	5.61.27.159
2954	109.731573	5.61.27.159
2955	109.731749	10.1.29.101
2956	109.731749	10.1.29.101
2957	109.731985	5.61.27.159

Frame 2957: 1396 bytes on wire (1116 bits), 1396 bytes captured (1116 bits) on interface 10.1.29.101
D> Ethernet II, Src: ASUSTekC_56:33: (10:00:0c:00:00:02) [eth0]
D> Internet Protocol Version 4, Src: 10.1.29.101 (10.1.29.101), Dst: 5.61.27.159 (5.61.27.159)
D> Transmission Control Protocol, Src: 10.1.29.101 [47], Dst: 5.61.27.159 [47]
D> Hypertext Transfer Protocol
D> Media Type

Wireshark - Export - HTTP object list

Text Filter: png Content Type: All Content-Types

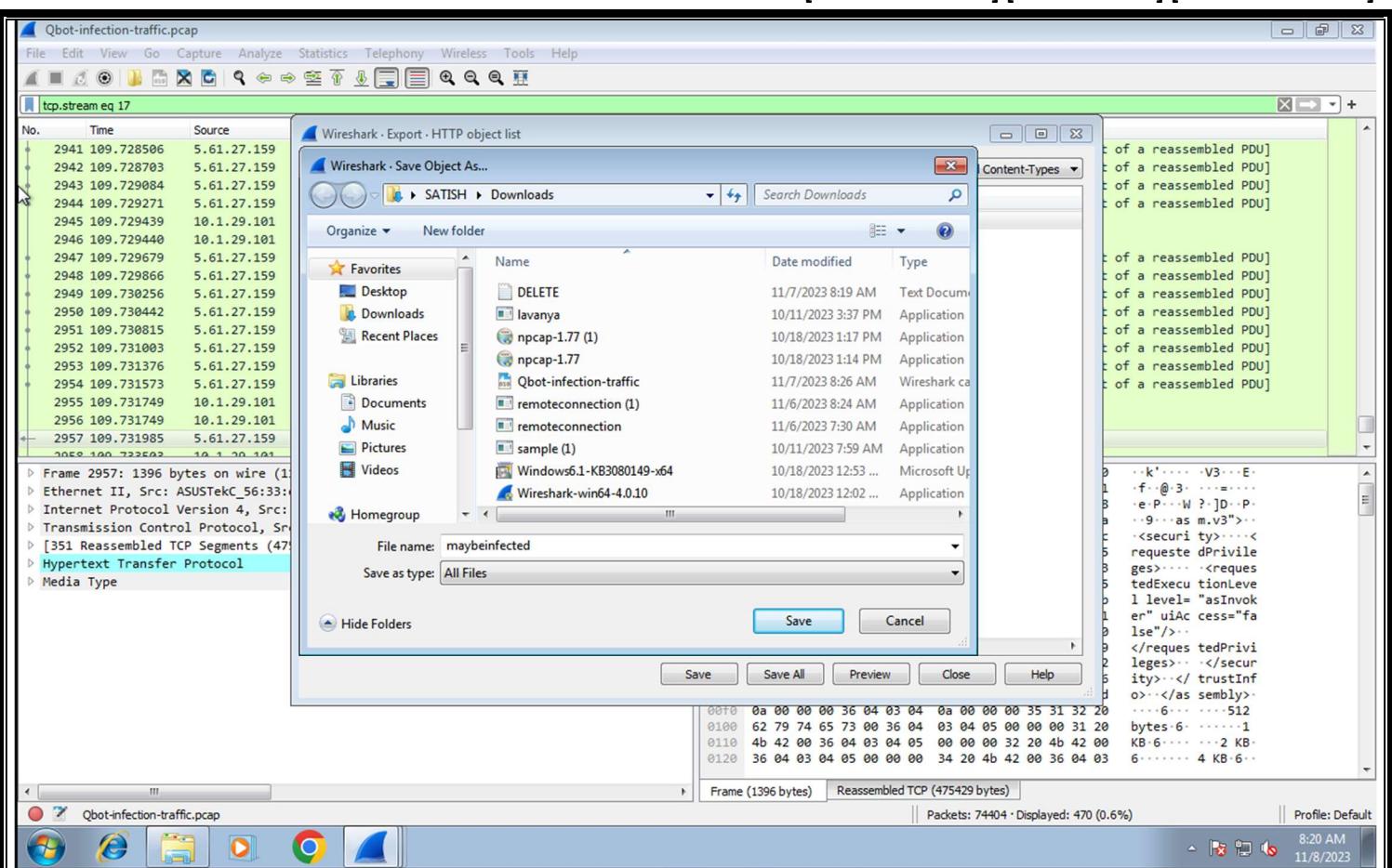
Packet	Hostname	Content Type	Size	Filename
2957	alphaenergyeng.com	image/png	475 kB	444444.png

Frame (1396 bytes) Reassembled TCP (475429 bytes)

Packets: 74404 · Displayed: 470 (0.6%)

Profile: Default

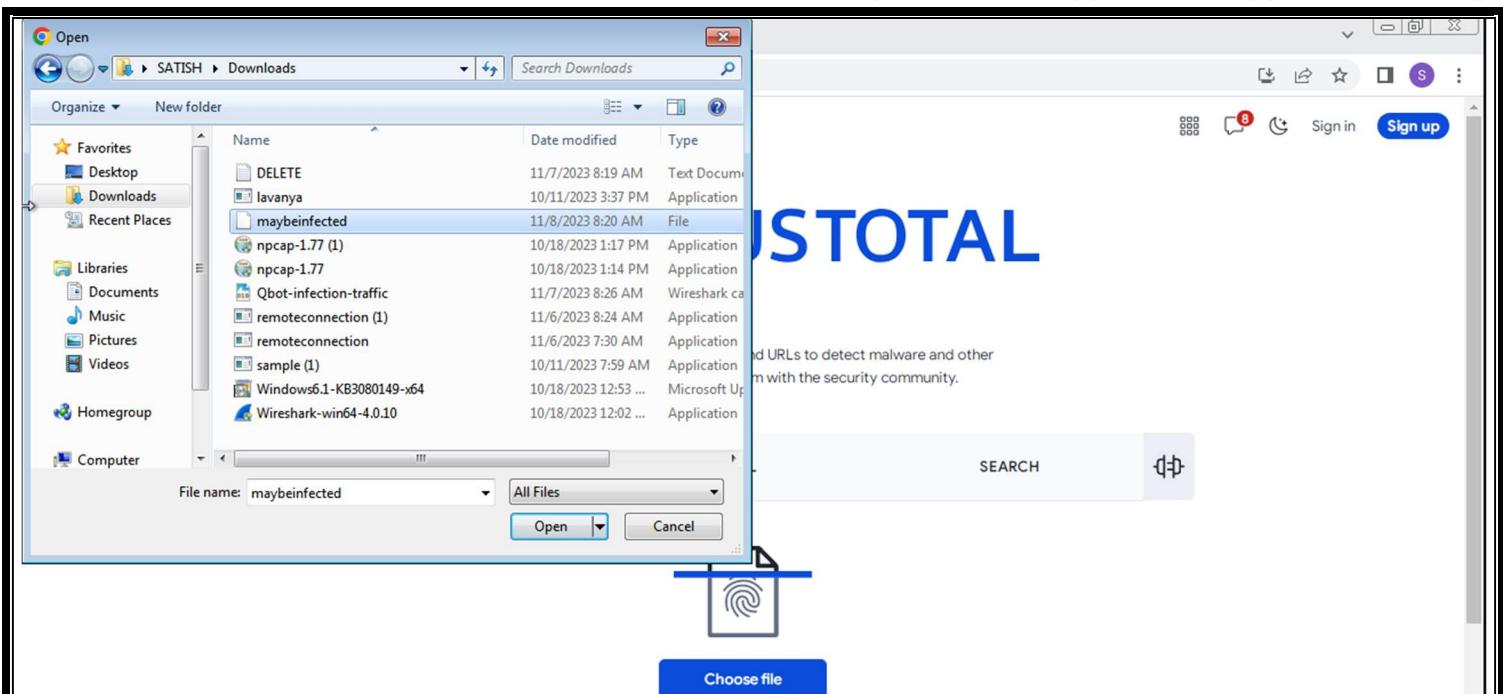
8:19 AM 11/8/2023



6) Virustotal scan:

Uploaded the saved PNG file to VirusTotal.com.

The screenshot shows the VirusTotal website's file upload interface. The main heading is 'VIRUSTOTAL'. Below it, a sub-instruction reads: 'Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.' A large 'FILE' tab is selected, showing a file icon with a blue outline and a 'Choose file' button below it. At the bottom, there is a note about agreeing to the Terms of Service and Privacy Policy, and a sharing disclaimer. The status bar at the bottom indicates 'Establishing secure connection...' and shows the system tray with various icons.



By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the [sharing of your Sample submission with the security community](#). Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).



7) Malicious indication:

VirusTotal.com indicated that the PNG file is potentially malicious.

Detection: 55 / 72

File Details: 56ee803fa903ab477f939b3894af6771aebf0138abe38ae8e3c41cf96bbb0f2a
xsejan.dll
peexe runtime-modules detect-debug-environment long-sleeps checks-user-input spreader executes-dropped-file

Threat Categories: trojan, banker

Family labels: qbot, zusy, qakbot

Security vendors' analysis:

Vendor	Analysis	Notes
AhnLab-V3	Trojan/Win32.RL_Generic.R325764	Alibaba
ALYac	Trojan.Agent.QakBot	Antiy-AVL
Arcabit	Trojan.Zusy.D4D069	Avast
AVG	Win32:BankerX-gen [Trj]	Avira (no cloud)
		TrojanBanker:Win32/Kryptik.e9d7476a
		Trojan[Banker]:Win32.Qbot
		Win32:BankerX-gen [Trj]
		HEUR/AGEN.1351522

[zip file analysis]**1. Capture and Filter Traffic:**

Obtain a pcap file using Wireshark.



Qbot-infection-traffic

2. Apply a filter to isolate HTTP GET requests (http.request.method == GET).

Qbot-infection-traffic.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	Info
19	0.165516	10.1.29.101	13.107.4.52	HTTP	165	GET /connecttest.txt HTTP/1.1
248	25.075751	10.1.29.101	103.91.92.1	HTTP	530	GET /wp-content/uploads/2020/01/ahead/9312.zip HTTP/1.1
2498	107.866461	10.1.29.101	5.61.27.159	HTTP	222	GET /wp-content/uploads/2020/01/ahead/444444.png HTTP/1.1
14837	922.779739	10.1.29.101	89.105.198.119	HTTP	339	GET /redir_ie.html HTTP/1.1
14854	923.063741	10.1.29.101	89.105.198.119	HTTP	268	GET /favicon.ico HTTP/1.1
15082	924.125208	10.1.29.101	89.105.198.119	HTTP	516	GET /redir_ie.html HTTP/1.1
15177	924.323864	10.1.29.101	89.105.198.119	HTTP	456	GET /favicon.ico HTTP/1.1
30215	934.023834	10.1.29.101	91.199.212.52	HTTP	198	GET /USERTrustECCAddTrustCA.crt HTTP/1.1
33777	3601.882311	10.1.29.101	23.61.187.27	HTTP	298	GET /MFEWtBNMEmwSTAJBgUrDgMCggUBBQd1mpyHEqFCSoj4SCu93CBydHAQuR2PiwyqN0hXLgp7xB8ymi0H%2BAdWICEHvU5a...
33829	3604.078863	10.1.29.101	23.61.187.27	HTTP	304	GET /ocsp/status/MFEWtBNMEmwSTAJBgUrDgMCggUBBR8rDZ7XHMv9dleA1%2FfaHn9a2FoQQUwfBYxzw4VJn375XfmIn...
33933	3659.903278	10.1.29.101	72.21.81.240	HTTP	341	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?f325136efe84540c HTTP/1.1
33936	3659.979213	10.1.29.101	72.21.81.240	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?c8e3e86710f90f20 HTTP/1.1
33938	3660.055864	10.1.29.101	72.21.81.240	HTTP	336	GET /msdownload/update/v3/static/trustedr/en/pinrulesstl.cab?86f0075cbaaf7ccc HTTP/1.1

Frame 19: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
 Ethernet II, Src: Tp-LinkT_27:87:7f (ec:08:6b:27:87:7f), Dst: ASUSTekC_56:33:ea (04:d4:
 Internet Protocol Version 4, Src: 10.1.29.101, Dst: 13.107.4.52
 Transmission Control Protocol, Src Port: 49671, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
 Hypertext Transfer Protocol

0000 04 d4 c4 56 33 ea ec 08 6b 27 87 7f 08 00 45 00 ...V3... k'....E-
 0010 00 97 b9 01 40 08 80 06 08 5b 0a 01 1d 65 0d 6b ...@...-[...e-k
 0020 04 34 c2 07 00 50 fb f0 f5 3b 4b 2d 34 26 50 18 -4...P...;K-4&P-
 0030 02 02 82 4c 00 00 47 45 54 20 2f 63 6f 6e 65 ...L..GE T /conne
 0040 63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f cttest.t xt HTTP/
 0050 31 2e 31 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a 1.1.. Con nection:
 0060 20 43 6c 6f 73 65 0d 0a 55 73 65 72 2d 41 67 65 Close.. User-Age
 0070 6e 74 3a 20 4d 69 63 72 6f 73 6f 66 74 20 4e 43 nt: Micr osoft NC
 0080 53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73 SI..Host : www.ms
 0090 66 74 63 6f 6e 65 63 74 74 65 73 74 2e 63 6f ftconnec ttest.co
 00a0 6d 0d 0a 0d 0a m....

Qbot-infection-traffic.pcap

Packets: 74404 · Displayed: 13 (0.0%)

Profile: Default

8:12 AM 11/8/2023

3. Identify files:

Through your filtering, you identified two files (PNG and ZIP).

Frame 19: 165 bytes on wire (1320 bits), 165 bytes captured (1320 bits)
 Ethernet II, Src: Tp-Link_27:87:7f (ec:08:6b:27:87:7f), Dst: ASUSTek_C_56:33:ea (04:d4:
 Internet Protocol Version 4, Src: 10.1.29.101, Dst: 13.107.4.52
 Transmission Control Protocol, Src Port: 49671, Dst Port: 80, Seq: 1, Ack: 1, Len: 111
 Hypertext Transfer Protocol

```

0000  04 d4 c4 56 33 ea ec 08 6b 27 87 7f 08 00 45 00  ...V3... k'...E...
0010  08 97 b9 01 40 00 00 06 08 5b 0a 01 1d 65 0d 6b  ...@... [...e.k
0020  04 34 c2 07 00 50 fb f0 f5 3b 4b 2d 34 26 50 18  ...P... ;K-&P
0030  02 02 82 4c 00 00 47 45 54 20 2f 63 6f 6e 6e 65  ...L...GE T /conne
0040  63 74 74 65 73 74 2e 74 78 74 20 48 54 54 50 2f  cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 6f 6e 65 65 63 74 69 6f 6e 3a  1.1-Con nection:
0060  20 43 6c 6f 73 6d 0a 55 73 65 72 2d 41 67 65  Close.. User-Age
0070  6e 74 3a 20 4d 69 63 72 6f 73 66 74 20 4e 43  nt: Micr osoft NC
0080  53 49 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 6d 73  SI... Host : www.ms
0090  66 74 63 6f 6e 6e 65 63 74 74 65 73 74 2e 63 6f  ftconnec ttest.co
00a0  6d 0d 0a 0d  m...
  
```

4. ZIP File Analysis:

Focused on the ZIP file.

Opened the ZIP file packet and followed the TCP stream.

Mark/Unmark Packet Ctrl+M
 Ignore/Ignore Packet Ctrl+D
 Set/Unset Time Reference Ctrl+T
 Time Shift... Ctrl+Shift+T
 Packet Comments ▶ 1.199.212.52
 Edit Resolved Name 3.61.187.27
 Apply as Filter ▶ 2.21.81.240
 Prepare as Filter ▶ 2.21.81.240
 Conversation Filter
 Colorize Conversation
 SCTP
 Follow
 Copy
 Protocol Preferences
 Decode As...
 Show Packet in New Window

530 bytes captured (4240 bits)
 0: 6b:27:87:7f, Dst: ASUSTek_C_56:33:ea (04:d4:
 10.1.29.101, Dst: 103.91.92.1
 0: 9679, Dst Port: 80, Seq: 1, Ack: 1, Len: 476

```

0000  04 d4 c4 56 33 ea ec 08 6b 27 87 7f 08 00 45 00  ...V3... k'...E...
0010  02 04 a4 8b 40 00 00 06 69 a6 0a 01 1d 65 67 5b  ...@... i...eg[
0020  5c 01 c2 0f 00 50 91 8b c0 6b 6f 22 0c 5b 18  \...p... .".p
0030  02 02 48 96 00 00 47 45 54 20 2f 77 70 2d 63 6f  .H...GE T /wp-co
0040  6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30  ntent/up loads/20
0050  32 30 2f 30 31 2f 61 68 65 61 64 2f 39 33 31 32  0/01/ah ead/9312
0060  2e 7a 69 70 20 48 54 54 50 2f 31 2e 31 0d 0e 48  .zip HTT P/1.1- H
0070  6f 73 74 3a 20 62 68 61 74 6e 65 72 2e 63 6f 6d  ost: bha tner.com
0080  0d 0a 43 6f 6e 65 63 74 69 6f 6e 3a 20 6b 65  -Connec tion: ke
0090  65 70 2d 61 6c 69 76 65 0d 0a 55 70 67 72 61 64  ep-alive ..Upgrad
00a0  65 2d 49 73 65 63 75 72 65 2d 52 65 71 75 65  e-Insecu re-Reque
00b0  73 74 73 3a 20 31 0d 0a 55 73 65 72 2d 41 67 65  sts: 1.. User-Age
00c0  6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20  nt: Mozil lla/5.0
00d0  28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30  (Windows NT 10.0
00e0  3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 41 70 ; Win64; x64) Ap
00f0  70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33 36 pleWebK1 t/537.36
0100  20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47 65 (KHTML, like Ge
0110  63 6b 6f 29 20 43 68 72 6f 6d 65 2f 37 39 2e 30 cko) Chr ome/79.0
0120  2e 33 39 34 35 2e 31 33 30 20 53 61 66 61 72 69 .3945.13 0 Safari
0130  2f 35 33 37 2e 33 36 20 45 64 67 2f 37 39 2e 30 /537.36 Edg/79.0
0140  2e 33 30 39 2e 37 31 0d 0a 41 63 63 65 70 74 3a .309.71 .Accept:
  
```

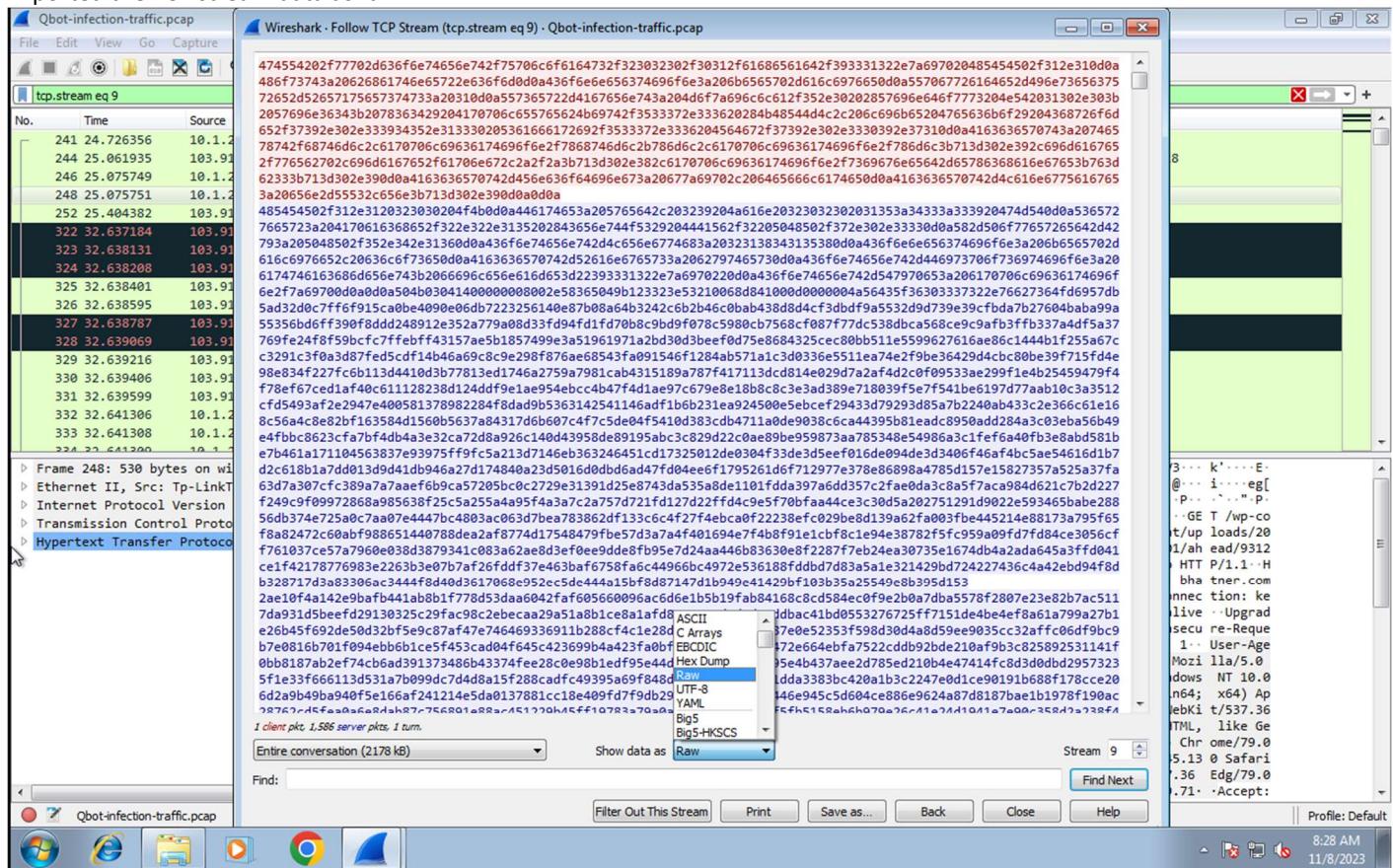
The screenshot shows the Wireshark interface with a list of network captures on the left. A specific packet is selected, and a context menu is open over it. The menu path is 'HTTP > TCP Stream'. The menu items include:

- Mark/Unmark Packet
- Ignore/Unignore Packet
- Set/Unset Time Reference
- Time Shift...
- Packet Comments
- Edit Resolved Name
- Apply as Filter
- Prepare as Filter
- Conversation Filter
- Colorize Conversation
- SCTP
- Follow
- Copy
- Protocol Preferences
- Decode As...
- Show Packet in New Window
- TCP Stream
- UDP Stream
- DCCP Stream
- TLS Stream
- HTTP Stream
- HTTP/2 Stream
- QUIC Stream
- SIP Call

The 'TCP Stream' option is highlighted with a mouse cursor. The main pane displays the selected packet's details, and the bottom pane shows the packet bytes and ASCII dump.

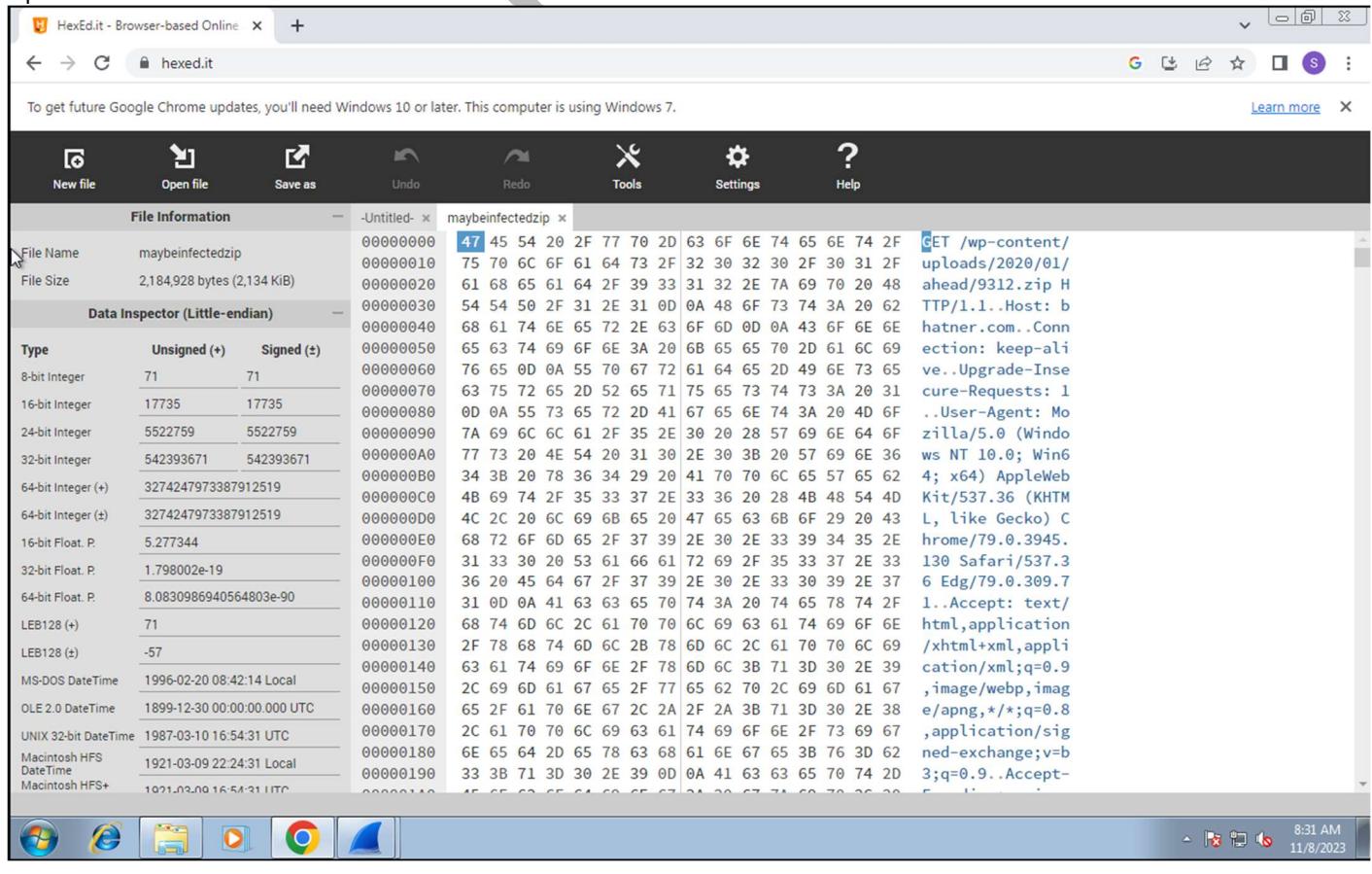
5. Save TCP Stream as Raw:

Exported the TCP stream data as raw.



6. Hexadecimal Editing:

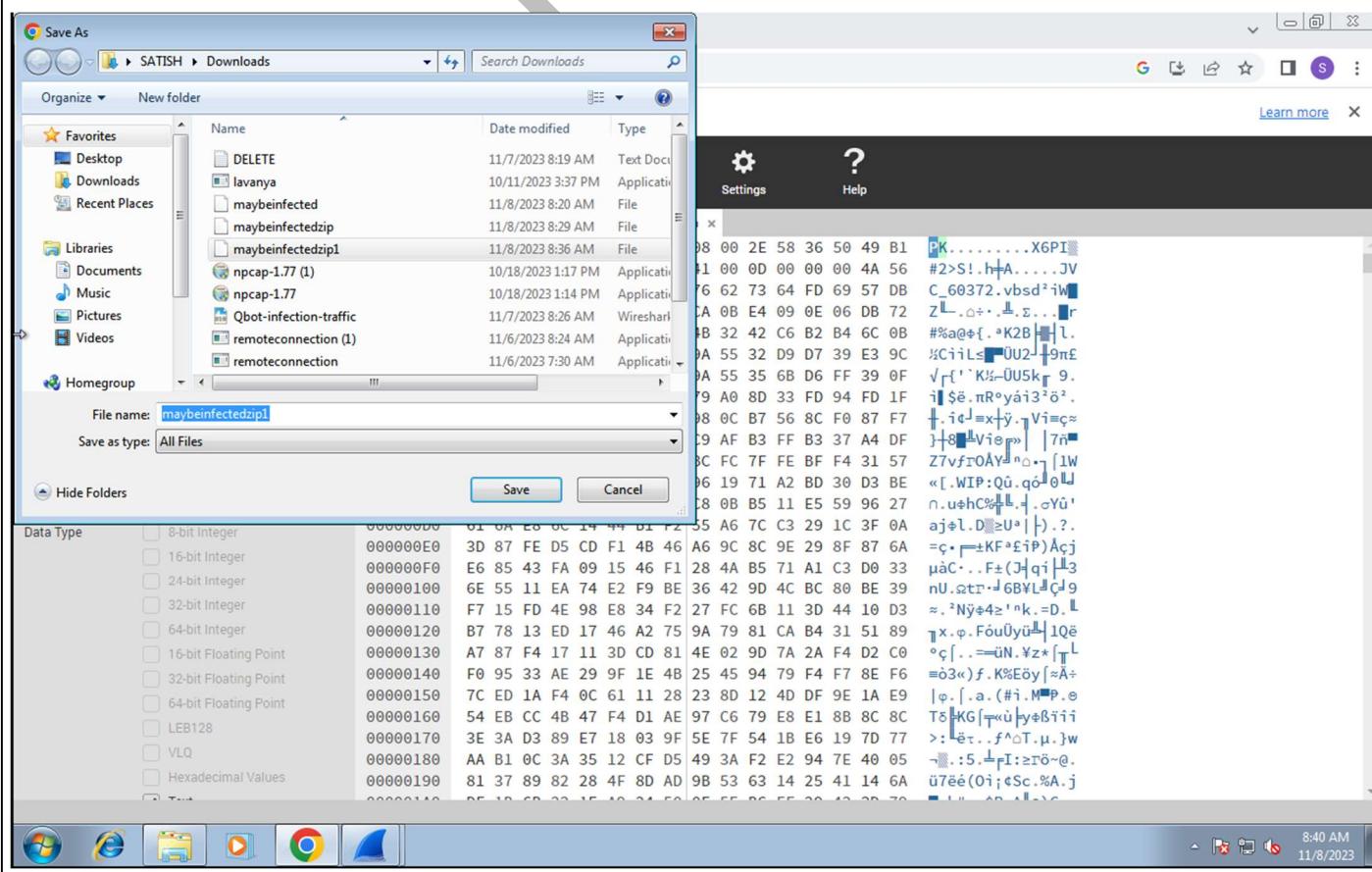
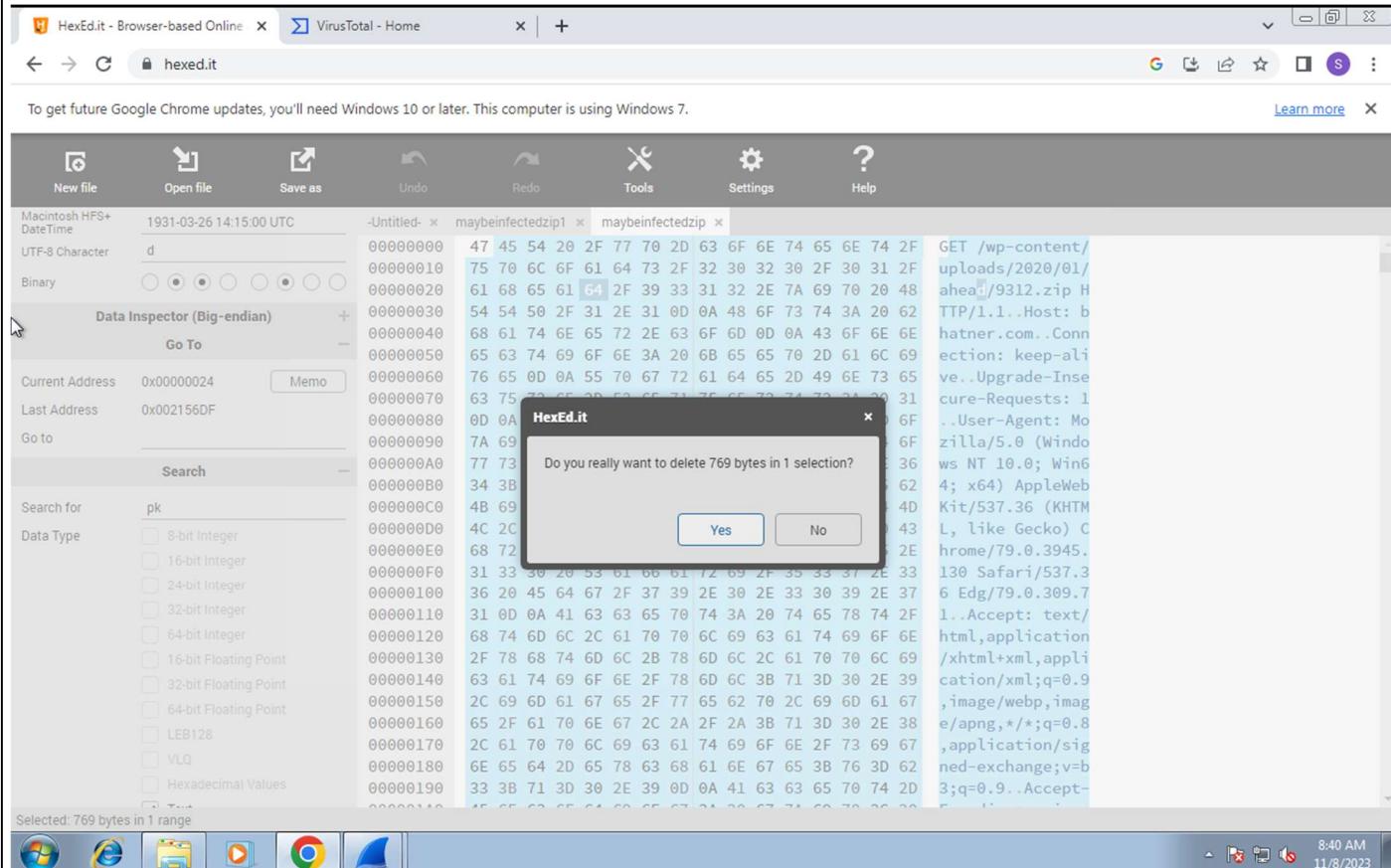
Opened the saved raw file in a hex editor.



7. Trimming and Saving:

Deleted all bytes before the magic bytes "PK" (ZIP file signature).

Saved the edited file.



8. VirusTotal Scan:

Uploaded the edited ZIP file to VirusTotal.com.

File name: maybeinfectedzip1

Open Cancel

SEARCH

Choose file

By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the **sharing of your Sample submission with the security community**. Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. [Learn more](#).

9. Malicious Indication:

VirusTotal.com indicated that the ZIP file is potentially dangerous and infected.

Security vendor	Detection	Action	
Alibaba	TrojanDownloader:VBS/NEMUCOD.c1631...	Arcabit	VBS:Electryon.21
Avast	Other:Malware-gen [Trj]	AVG	Other:Malware-gen [Trj]
BitDefender	VBS:Electryon.21	Emsisoft	VBS:Electryon.21 (B)
eScan	VBS:Electryon.21	ESET-NOD32	VBS/TrojanDownloader.Agent.RKE

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label trojan.electryon/nemucod

Threat categories trojan downloader dropper

Family labels electryon nemucod

Community Score 29 / 60

Community

Do you want to automate checks?

8:37 AM 11/8/2023

8:41 AM 11/8/2023

❖ DYNAMIC ANALYSIS:

Tools used:

- Sandbox environment(ANY.RUN)

The screenshot shows the ANY.RUN homepage with a dark blue background featuring vertical light blue streaks. The logo 'ANY RUN' is prominently displayed on the left. On the right, there is a large call-to-action button with the text 'MALWARE HUNTING WITH LIVE ACCESS TO THE HEART OF AN INCIDENT'. Below it, a subtext reads: 'Watch the epidemic as if it was on your computer, but in a more convenient and secure way, with a variety of monitoring features.' A 'REGISTER FOR FREE' button is also visible. In the center, a screenshot of a browser window shows a WannaCry ransomware sample with the message 'Oops, your files have been encrypted!' and a file list.

The screenshot shows the ANY.RUN malware analysis interface. On the left, a sidebar includes links for 'New task', 'Public tasks', 'Teamwork', 'History', 'Windows 7 32 bit', 'Profile', 'Pricing', 'Contacts', 'FAQ', and 'Log Out'. The main area features a world map with red shading indicating malicious activity. To the right, there are several data visualizations: a 'Statistics for 24 hours' chart showing 'Top submitters rating' with the United States at the top; a 'Tasks ratio' chart with three categories: 2507 Malicious, 1256 Suspicious, and 10416 No threat; and a 'Trending tags' chart listing terms like 'stealer', 'phishing', 'generated-doc', etc., with their respective counts. The bottom of the screen shows a Windows taskbar with various icons and system status indicators.

ANY.RUN - Interactive Online M x Interactive Online Malware Anal... x New Tab x | +

app.any.run/?_gl=1*1wgo8ro*_gcl_au*MTUwODQyNzg4NSxNjk5NDI3MjE*_ga*MTU3Mjg4OTUwNi4xNjkwmJA4NDM2*_ga_53KB74YDZR*MTY5OTQyNzlxNC4zljEuMTY5OTQyODExNC4wLjA...

Malware hunting with live access to the heart of an incident
Analyze a network, file, module, and the registry activity. Interact with the OS directly from a browser. See the feedback from your actions immediately.

Create a new task Pro mode

- Type URL or upload a file

type or copy URL
 Upload

drag and drop a file here

The uploaded file should contain an extension or otherwise use the "Change extension to valid" option in Pro mode.
- Choose an operating system

Windows 7
Windows 8
Windows 10
Windows 11

32 Bit • 64 Bit

Run a public task

Statistics for 24 hours

Top submitters rating

Country	Submissions	Percentage
United States	5336	38%
Germany	1184	8%
India	682	5%
United Kingdom	605	4%
Spain	501	4%
Israel	477	3%
Canada	449	3%
Russian Federation	325	2%
Australia	257	2%
Colombia	225	2%

Tasks ratio

2507 1256 10416

W

Snipping Tool

Screenshot copied to clipboard and saved
Select here to mark up and share the image

Get FREE trial

Search 12:52 PM 11/8/2023

ANY.RUN - Interactive Online M x Analysis https://moviesda8.co/... x TamilRockers 2023 Movies Down... x +

app.any.run/tasks/46257007-e96a-4ec4-90c0-9a45775187b7

TamilRockers 2023 Movies Download TamilRockers Tamil Movies Download - Internet Explorer

Moviesda.Mobi
Name Of Quality

Like our Facebook Fan Page & Get Updates and News!

Moviesda8.Co
(Please Bookmark & Search)

Tamil Mobile Movies

Unstoppable (2023)
VJ Sunny, Septhagiri, Aqsa Khan
Original DVD
Rating: 6.3

Shot Boot Three (2023)
Yogi Babu, Kallash Heet, Sivaangi Krishnakumar
Original DVD
Rating: 8.7

Irugapatur (2023)
Shraddha Srinath, Saniya Iyappan, Vikram Prabhu

No threats detected

https://moviesda8.co/tamilrockers-movies-download/

Win7 32 bit Complete
Open in browser Start: 08.11.2023, 12:57 Total time: 60 s + Add tags

Indicators: IOC MalConf Restart

Text report **Graph** **ATT&CK** ChatGPT **Export**

CPU **RAM**

Processes Filter by PID or name Only important

PID	Process Name	Content
3440	explore.exe	http://ctld.windowupdate.com/msdownl... 4.66 Kb + compressed
3196	explore.exe	http://ctld.windowupdate.com/msdownl... 4.66 Kb + compressed
4181	explore.exe	http://ocsp.pki.goog/gr1/MFEWT2BNME... 1.41 Kb + binary
4182	explore.exe	http://ocsp.pki.goog/gtsr1/ME4WTDBKME... 724 b + binary
4292	explore.exe	http://ocsp.pki.goog/gts1c3/MFIwJD80M... 724 b + binary
4382	explore.exe	http://ocsp.pki.goog/gts1c3/MFEWT2BNM... 472 b + binary
4506	explore.exe	http://ocsp.pki.goog/dts1c3/MFEWT2BNM... 471 b + binary

ANY.RUN

HTTP Requests 15 **Connections** 34 **DNS Requests** 17 **Threats** 0 PCAP

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
1756 ms		?	3196	explore.exe	?	http://ctld.windowupdate.com/msdownl...	4.66 Kb + compressed
1757 ms		?	3196	explore.exe	?	http://ctld.windowupdate.com/msdownl...	4.66 Kb + compressed
4181 ms		?	3196	explore.exe	?	http://ocsp.pki.goog/gr1/MFEWT2BNME...	1.41 Kb + binary
4182 ms		?	3196	explore.exe	?	http://ocsp.pki.goog/gtsr1/ME4WTDBKME...	724 b + binary
4292 ms		?	3196	explore.exe	?	http://ocsp.pki.goog/gts1c3/MFIwJD80M...	724 b + binary
4382 ms		?	3196	explore.exe	?	http://ocsp.pki.goog/gts1c3/MFEWT2BNM...	472 b + binary
4506 ms		?	3196	explore.exe	?	http://ocsp.pki.goog/dts1c3/MFEWT2BNM...	471 b + binary

Get more awesome features with premium access! View more

Info [3888] wmpnscfg.exe Reads the machine GUID from the registry

Search 12:58 PM 11/8/2023


[General](#) [Behavior](#) [MalConf](#) [Static information](#) [Video](#) [Screenshots](#) [System events](#) [Network](#)


General Info

 Add for printing

URL: <https://moviesda8.co/tamilrockers-movies-download/>

Full analysis: <https://app.any.run/tasks/46257007-e96a-4ec4-90c0-9a45775187b7>

Verdict: **No threats detected**

Analysis date: November 08, 2023 at 12:57:25

OS: Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)

Indicators:



SHA1: C933565C40EC8565A7F0599221C2A66B87D61AC1

SHA256: 41BF1E0EA686A71FFA6B2713DAA045C3EF411A1EA21F905016FDE247A8EA496

SSDeep: 3:N8xBR0ISGPwlgbSCn:2t0VGoBbL

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. **ANY.RUN** does not guarantee maliciousness or safety of the content.



Behavior activities

 Add for printing

MALICIOUS

No malicious indicators.

SUSPICIOUS

No suspicious indicators.

INFO

Checks supported languages

- wmpnscfg.exe (PID: 3888)

Manual execution by a user

- wmpnscfg.exe (PID: 3888)

Application launched itself

- iexplore.exe (PID: 3440)

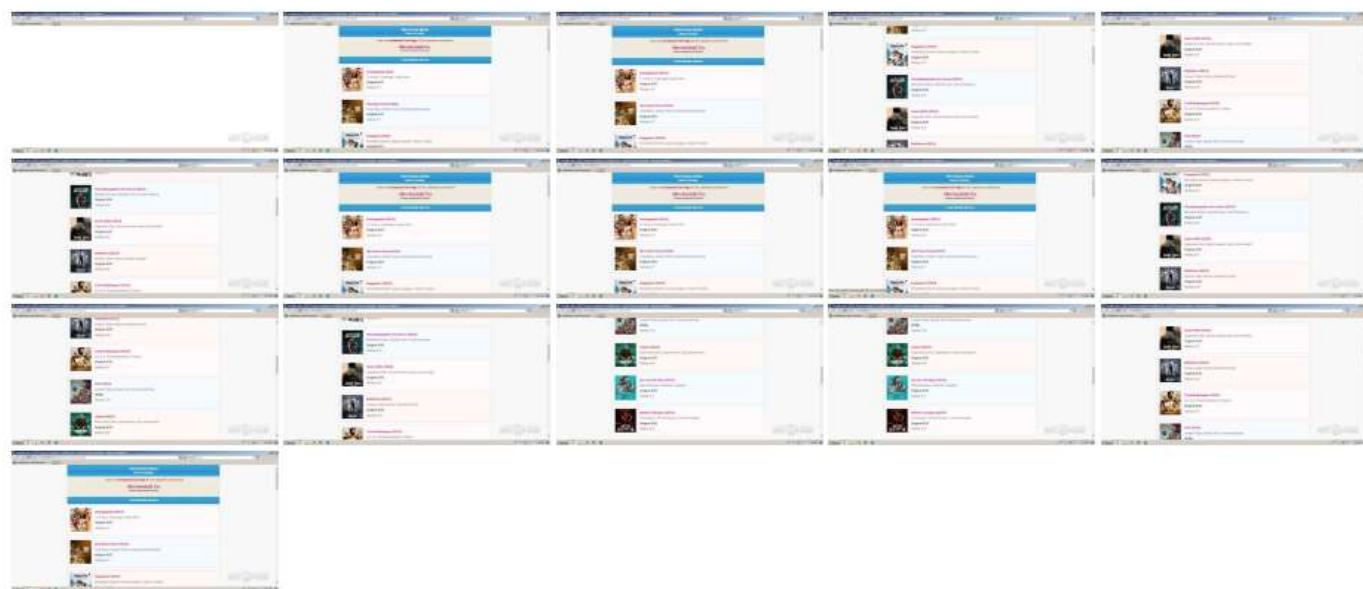
Reads the machine GUID from the registry

- wmpnscfg.exe (PID: 3888)

Reads the computer name

- wmonsco.exe (PID: 3888)

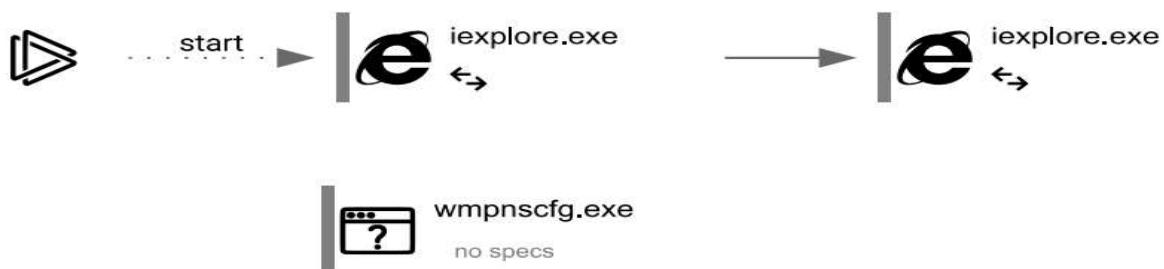
Video and screenshots



Processes

Total processes	Monitored processes	Malicious processes	Suspicious processes
38	3	0	0

Behavior graph



Specs description

	Program did not start		Low-level access to the HDD		Process was added to the startup		Debug information is available
	Probably Tor was used		Behavior similar to spam		Task has injected processes		Executable file was dropped
	Known threat		RAM overrun		Network attacks were detected		Integrity level elevation
	Connects to the network		CPU overrun		Process starts the services		System was rebooted
	Task contains several apps running		Application downloaded the executable file		Actions similar to stealing personal data		Task has apps ended with an error
	File is detected by antivirus software		Inspected object has suspicious PE structure		Behavior similar to exploiting the vulnerability		Task contains an error or was rebooted
	The process has the malware config						

Process information

PID	CMD	Path	Indicators	Parent process
3440	'C:\Program Files\Internet Explorer\iexplore.exe' 'https://moviesda8.co/tamilrockers-movies-download/'	C:\Program Files\Internet Explorer\iexplore.exe		explorer.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Internet Explorer	
Version:	11.00.9600.16428 (winblue_gdr.131013-1700)			
3196				
	'C:\Program Files\Internet Explorer\iexplore.exe'	SCODEF:3440 C:\Program Files\Internet Explorer\iexplore.exe		iexplore.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	LOW	Description:	Internet Explorer	
Version:	11.00.9600.16428 (winblue_gdr.131013-1700)			
3888				
	'C:\Program Files\Windows Media Player\wmpnscfg.exe'	C:\Program Files\Windows Media Player\wmpnscfg.exe		explorer.exe
Information				
User:	admin	Company:	Microsoft Corporation	
Integrity Level:	MEDIUM	Description:	Windows Media Player Network Sharing Service Configuration Application	
Exit code:	0	Version:	12.0.7600.16385 (win7_rtm.090713-1255)	

Registry activity

Total events	Read events	Write events	Delete events
22 613	22 544	66	3

Modification events

(PID) Process: (3440) iexplore.exe Operation: write Value: 0	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing Name: NTPDaysSinceLastAutoMigration
(PID) Process: (3440) iexplore.exe Operation: write Value: 30847387	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TabbedBrowsing Name: NTPLastLaunchHighDateTime
(PID) Process: (3440) iexplore.exe Operation: write Value: 30847437	Key: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\UrlBlockManager Name: NextCheckForUpdateHighDateTime
(PID) Process: (3440) iexplore.exe Operation: write Value: Cookie;	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Cookies Name: CachePrefix
(PID) Process: (3440) iexplore.exe Operation: write Value: Visited:	Key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\History Name: CachePrefix

Files activity

Executable files	Suspicious files	Text files	Unknown types
0	34	39	0

Dropped files

PID	Process	Filename	Type
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\CAF4703619713E3F18D8A9D5D88D6288_F2DAF19C1F776537105D 08FC8D978464	binary
		MD5: 8202A1CD02E7D69597995CABBE8B1A12	SHA256: 58F3B1C3A0A0ACE6321DA22E40BD44A597BD98B9C9390AB9258426B50CF75A7A5
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\CAF4703619713E3F18D8A9D5D88D6288_F2DAF19C1F776537105D 08FC8D978464	binary
		MD5: 0CF5C980C93C66C4757E1A8A99160AC6	SHA256: 4C11B6C36DB881D4E0435BE87B897E89A8090A680797E56E654F5A466A4C49C3
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\F07644E38ED7C9F37D11EEC6D4335E02_17A1BB9C6401DC96520 40571BD192211	binary
		MD5: CAC74099BB8D6CE9C2B8D45A8D29C372	SHA256: 7296F8A6DFE6E0C0046A8E7DA8641913CC892EC47613E56F86B8B75BC5D1DEBD
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\24BD96D5497F70B3F510A6B53CD43F3E_3A89246FB90C5EE662000 4F1AE0EB0EA	binary
		MD5: 16FDB5C10A4DF5AEE308F7FB5F96C679	SHA256: EDF45F72F667717677895170519DB3E6A44EA29DF72FF7BBD7F3DE7134A8708
3196	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\YTOWV792\scam-2003-2023[1].jpg	image
		MD5: 0A20E06237FE1544A37BA1EE21502BF0	SHA256: E0BD56CF52D0BA15A34371EFA2C2FD87ACD27040FEBBA76251A10704452653AB
3196	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\YTOWV792\tamil-kudimagan-2023[1].jpg	image
		MD5: A0AE00E38B7A7FB11C55D7597F87DACP	SHA256: 4D65A0110541162AEADBAE1EF26B5C80CE4E13CE4E3E989BC4B1BD4F71E99AC2
3196	iexplore.exe	C:\Users\admin\AppData\Local\Microsoft\Windows\Temporary Internet Files\Low\Content.IE5\MFAQUS6V\tamilrockers-movies- download[1].htm	html
		MD5: 88213C42E2A1F775F873ACF6CF446C06	SHA256: 8970F90829A80CA63D9BF4069DE059D48FC7872DA5DFB533D2E1B8BCD46AECEE
3196	iexplore.exe	C:\Users\admin\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\57C8EDB95DF3F0AD4EE2DC2B8CFD4157	compressed

Network activity

HTTP(S) requests	TCP/UDP connections	DNS requests	Threats
15	34	17	0

HTTP requests

PID	Process	Method	HTTP Code	IP	URL	CN	Type	Size	Reputation
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gtsr1/ME4wTDBKMEgwRJAJBgUrDgMC GgUABBQwkclLWD4LqGJ7bE7B1XZsEbmfwUAQUSk8rJnEaK0gnhS9SZizv8IkTct4CDQlDvFCj1PwkYA7fE%3D	unknown	binary	724 b	unknown
3196	iexplore.exe	GET	200	23.53.40.41:80	http://ctldl.windowsupdate.com/msdownload/update/v3/sta tic/trusted/en/disallowecertstl.cab?d6bb2ad0af14907d	unknown	compressed	4.66 Kb	unknown
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gtsr1/MFEwTzBNMEswSTAJBgUrDgMC GgUABBS3V7W2nAf4FIMTjpDJKg6%2BMgGgMQQUYHtmGkUN8qJUC99BM00qP%2F8%2FuCEHe9DWzbNvka6iEPxPBY0w0%3D	unknown	binary	1.41 Kb	unknown
3196	iexplore.exe	GET	200	23.53.40.41:80	http://ctldl.windowsupdate.com/msdownload/update/v3/sta tic/trusted/en/authrootstl.cab?86908589b66dbf86	unknown	compressed	61.6 Kb	unknown
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gtsr1/ME4wTDBKMEgwRJAJBgUrDgMC GgUABBQwkclLWD4LqGJ7bE7B1XZsEbmfwUAQUSk8rJnEaK0gnhS9SZizv8IkTct4CDQlDvFNZazTHGPUBUGY%3D	unknown	binary	724 b	unknown
3440	iexplore.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCG gUABBQ50otx%2fh0Zt%2Bz8SP17wEWVxDIQUTLJIBIV5uNu5g%2F6%2BrkS7QYXjkCEAqvpSXKY8RRQeo74ffHUxc%3D	unknown	binary	471 b	unknown
3196	iexplore.exe	GET	200	142.250.181.227:80	http://ocsp.pki.goog/gts1c3/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTHLnmK3f9hNL067UdcLuLvGwCQHYwQUnR%2Fr4XN7XNPZzQ4kYU83E1HSCCEGNkd7zfgP4rEh%2BpCYwNEA%3D	unknown	binary	471 b	unknown
3196	iexplore.exe	GET	200	192.229.221.95:80	http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCG gUABBQ50otx%2fh0Zt%2Bz8SP17wEWVxDIQUTLJIBIV5uNu5g%2F6%2BrkS7QYXjkCEA177e9ggmWelJG4vdGL0%3D	unknown	binary	471 b	unknown

DNS requests

Domain	IP	Reputation
ctldl.windowsupdate.com	23.53.40.41 23.53.40.40 23.53.40.49 23.53.40.83	whitelisted
ocsp.pki.goog	142.250.181.227	whitelisted
nl.yieldedshotter.com	172.255.6.54 23.109.82.219 23.109.248.184 23.109.82.33 23.109.82.94 142.91.159.136 23.109.82.5 23.109.82.239 23.109.150.207 23.109.82.14 23.109.248.177	unknown
fonts.googleapis.com	142.250.186.170	whitelisted
www.clarity.ms	13.107.246.67 13.107.213.67	whitelisted
fonts.gstatic.com	172.217.16.195	whitelisted
api.bing.com	13.107.5.80	whitelisted
ocsp.digicert.com	192.229.221.95	whitelisted

Connections

PID	Process	IP	Domain	ASN	CN	Reputation
2588	svchost.exe	239.255.255.250:1900	—	—	—	whitelisted
3196	iexplore.exe	23.53.40.41:80	ctld.windowsupdate.com	Akamai International B.V.	DE	unknown
4	System	192.168.100.255:137	—	—	—	whitelisted
4	System	192.168.100.255:138	—	—	—	whitelisted
3196	iexplore.exe	142.250.181.227:80	ocsp.pki.goog	GOOGLE	US	whitelisted
1080	svchost.exe	224.0.0.252:5355	—	—	—	unknown
3196	iexplore.exe	188.114.96.9:443	—	CLOUDFLARENET	NL	unknown
3196	iexplore.exe	142.250.186.170:443	fonts.googleapis.com	GOOGLE	US	whitelisted
3196	iexplore.exe	172.255.6.54:443	nl.yieldedshotter.com	SERVERS-COM	NL	unknown
3196	iexplore.exe	13.107.246.67:443	www.clarity.ms	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
3196	iexplore.exe	172.217.16.195:443	fonts.gstatic.com	GOOGLE	US	whitelisted
3196	iexplore.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3440	iexplore.exe	131.253.33.200:443	www.bing.com	MICROSOFT-CORP-MSN-AS-BLOCK	US	whitelisted
3440	iexplore.exe	192.229.221.95:80	ocsp.digicert.com	EDGECAST	US	whitelisted
3196	iexplore.exe	23.212.210.158:80	x1.c.lencr.org	AKAMAI-AS	AU	unknown
3196	iexplore.exe	184.24.77.54:80	r3.o.lencr.org	Akamai International B.V.	DE	unknown
3196	iexplore.exe	68.219.88.97:443	c.clarity.ms	MICROSOFT-CORP-MSN-AS-BLOCK	US	unknown
3440	iexplore.exe	188.114.96.9:443	—	CLOUDFLARENET	NL	unknown

Mitigation techniques of Malware attacks:

- Educate users on malware risks and safe online practices.
- Install and regularly update reputable antivirus software.
- Keep operating systems and software up-to-date for security patches.
- Utilize firewalls to monitor and control network traffic.
- Implement email filtering to detect and block malicious content.
- Secure web browsers and use extensions that enhance security.
- Enforce strong password policies and implement multi-factor authentication.
- Segment networks to limit the impact of potential malware infections.
- Perform regular backups of critical data and store them securely.
- Develop and regularly update an incident response plan for quick and effective action.