

Malware Traffic Analysis Report

Case Overview

A packet capture file (**2021-09-14.pcap**) containing **3,679 packets** was analyzed following reports that an endpoint device may have downloaded malware. The objective of this investigation was to identify suspicious network activity and extract potential **Indicators of Compromise (IOCs)**.

Tools Used

- Kali Linux
 - tcpdump
 - WHOIS lookup
 - VirusTotal
-

Opening the Capture File

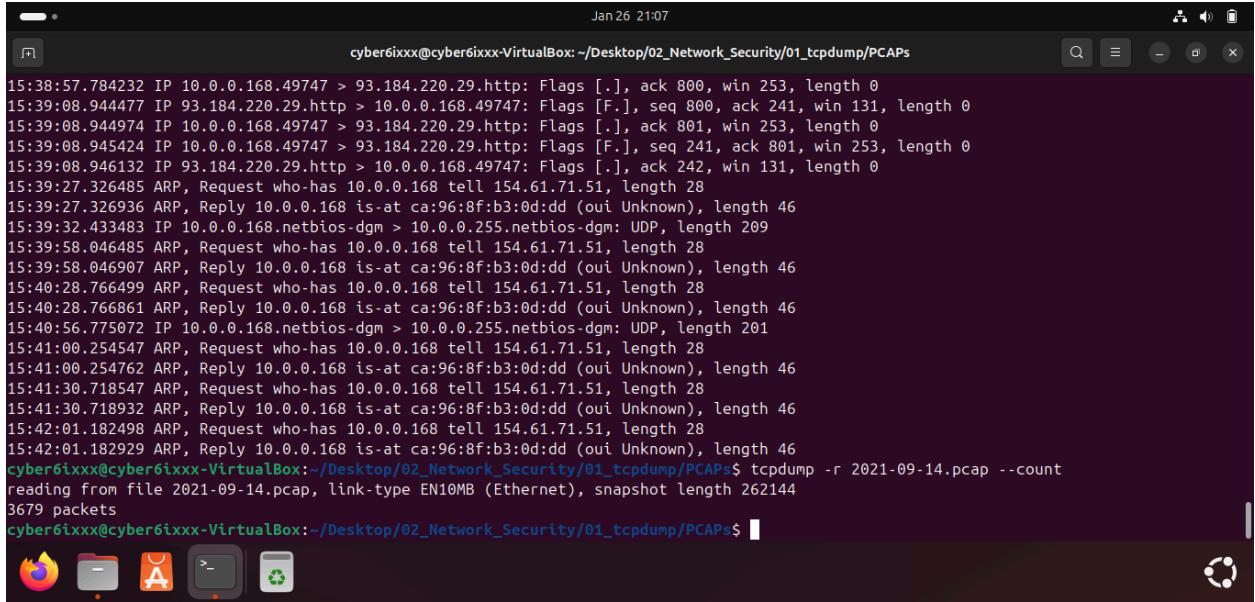
The PCAP file was examined using:

```
tcpdump -r 2021-09-14.pcap
```

To determine the total number of packets in the capture:

```
tcpdump -r 2021-09-14.pcap --count
```

Result: The capture contained **3,679 packets**, indicating significant network activity that required filtering.



A screenshot of a terminal window titled "cyber6ixxx@cyber6ixxx-VirtualBox: ~/Desktop/02_Network_Security/01_tcpdump/PCAPs". The window shows a list of network packets captured from a file named "2021-09-14.pcap". The traffic includes various ARP requests and replies, as well as HTTP requests from IP 10.0.0.168 to 93.184.220.29. The terminal prompt is "tcpdump -r 2021-09-14.pcap --count". The desktop environment includes icons for a browser, file manager, terminal, and system settings.

```
Jan 26 21:07
cyber6ixxx@cyber6ixxx-VirtualBox: ~/Desktop/02_Network_Security/01_tcpdump/PCAPs
15:38:57.784232 IP 10.0.0.168.49747 > 93.184.220.29.http: Flags [..], ack 800, win 253, length 0
15:39:08.944477 IP 93.184.220.29.http > 10.0.0.168.49747: Flags [F.], seq 800, ack 241, win 131, length 0
15:39:08.944974 IP 10.0.0.168.49747 > 93.184.220.29.http: Flags [..], ack 801, win 253, length 0
15:39:08.945424 IP 10.0.0.168.49747 > 93.184.220.29.http: Flags [F.], seq 241, ack 801, win 253, length 0
15:39:08.946132 IP 93.184.220.29.http > 10.0.0.168.49747: Flags [..], ack 242, win 131, length 0
15:39:27.326485 ARP, Request who-has 10.0.0.168 tell 154.61.71.51, length 28
15:39:27.326936 ARP, Reply 10.0.0.168 is-at ca:96:8f:b3:0d:dd (oui Unknown), length 46
15:39:32.433483 IP 10.0.0.168.netbios-dgm > 10.0.0.255.netbios-dgm: UDP, length 209
15:39:58.046485 ARP, Request who-has 10.0.0.168 tell 154.61.71.51, length 28
15:39:58.046907 ARP, Reply 10.0.0.168 is-at ca:96:8f:b3:0d:dd (oui Unknown), length 46
15:40:28.766499 ARP, Request who-has 10.0.0.168 tell 154.61.71.51, length 28
15:40:28.766861 ARP, Reply 10.0.0.168 is-at ca:96:8f:b3:0d:dd (oui Unknown), length 46
15:40:56.775072 IP 10.0.0.168.netbios-dgm > 10.0.0.255.netbios-dgm: UDP, length 201
15:41:00.254547 ARP, Request who-has 10.0.0.168 tell 154.61.71.51, length 28
15:41:00.254762 ARP, Reply 10.0.0.168 is-at ca:96:8f:b3:0d:dd (oui Unknown), length 46
15:41:30.718547 ARP, Request who-has 10.0.0.168 tell 154.61.71.51, length 28
15:41:30.718932 ARP, Reply 10.0.0.168 is-at ca:96:8f:b3:0d:dd (oui Unknown), length 46
15:42:01.182498 ARP, Request who-has 10.0.0.168 tell 154.61.71.51, length 28
15:42:01.182929 ARP, Reply 10.0.0.168 is-at ca:96:8f:b3:0d:dd (oui Unknown), length 46
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/01_tcpdump/PCAPs$ tcpdump -r 2021-09-14.pcap --count
reading from file 2021-09-14.pcap, link-type EN10MB (Ethernet), snapshot length 262144
3679 packets
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/01_tcpdump/PCAPs$
```

Filtering for Web Traffic

Since malware is commonly delivered over HTTP, traffic was filtered to display **GET** and **POST** requests:

```
tcpdump -r 2021-09-14.pcap -A tcp port 80 | egrep "GET|POST"
```

This filter isolates client web requests that could indicate file downloads or data transmission.

```
Jan 26 18:41
cyber6ixxx@cyber6ixxx-VirtualBox: ~/Desktop/02_Network_Security/01_tcpdump/PCAPs
&sectionHeight=160&FORM=IESS02&market=en-US HTTP/1.1
15:35:31.840413 IP 10.0.0.168.49722 > 13.107.5.80.http: Flags [P.], seq 6948:7614, ack 8039, win 32686, length 666: HTTP: GET /qsml.aspx?query=http%3A%2F%2F103.232.55.148%2Fservice%2Faudiodg.exe&maxwidth=32765&rowheight=20&sectionHeight=160&FORM=IESS02&market=en-US H TTP/1.1
....k.P.:.PS.J..t.}P...y..GET /qsml.aspx?query=http%3A%2F%2F103.232.55.148%2Fservice%2Faudiodg.exe&maxwidth=32765&rowheight=20&sectionHeight=160&FORM=IESS02&market=en-US HTTP/1.1
15:35:32.552578 IP 10.0.0.168.49724 > 103.232.55.148.http: Flags [P.], seq 1:282, ack 1, win 32768, length 281: HTTP: GET /service/.audiodg.exe HTTP/1.1
...g.7..<.P...}.P.....GET /service/.audiodg.exe HTTP/1.1
15:36:44.618317 IP 10.0.0.168.49743 > 136.243.159.53.http: Flags [P.], seq 1:252, ack 1, win 256, length 251: HTTP: POST /~element/page.php?id=484 HTTP/1.0
.....5.O.P.g....P.P...yy..POST /~element/page.php?id=484 HTTP/1.0
15:36:45.183946 IP 10.0.0.168.49744 > 136.243.159.53.http: Flags [P.], seq 1:252, ack 1, win 256, length 251: HTTP: POST /~element/page.php?id=484 HTTP/1.0
.....5.P.P...}P.....POST /~element/page.php?id=484 HTTP/1.0
15:36:45.679415 IP 10.0.0.168.49745 > 136.243.159.53.http: Flags [P.], seq 1:252, ack 1, win 256, length 251: HTTP: POST /~element/page.php?id=484 HTTP/1.0
.....5.Q.P.(c3...P...D...POST /~element/page.php?id=484 HTTP/1.0
15:36:55.102390 IP 10.0.0.168.49747 > 93.184.220.29.http: Flags [P.], seq 1:241, ack 1, win 256, length 240: HTTP: GET /MFEwTzBNMEswSTAjBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPi7wEWVxDlQQUTiJUIBiVSuNu5g%2F6%2BrkS7QYXjzkCEA177e19ggmWeljjG4vdGL0%3D HTTP/1.1
.....S.Pa...]./P...:l..GET /MFEwTzBNMEswSTAjBgUrDgMCGgUABBQ50otx%2Fh0Ztl%2Bz8SiPi7wEWVxDlQQUTiJUIBiVSuNu5g%2F6%2BrkS7QYXjzkCEA177el9ggmWeljjG4vdGL0%3D HTTP/1.1
cyber6ixxx@cyber6ixxx-VirtualBox: ~/Desktop/02_Network_Security/01_tcpdump/PCAPs$ tcpdump -r 2021-09-14.pcap -A tcp port 80 | egrep "GE
```

Suspicious HTTP Request Identified

Analysis revealed an HTTP GET request from:

- **Source IP (Client):** 10.0.0.168
- **Destination IP (External Server):** 103.232.55.148

This shows the internal host initiated communication with an unknown external server.

OSINT Investigation

The destination IP was investigated further:

- **WHOIS Lookup:** The IP resolves to infrastructure located in **Vietnam**
- **VirusTotal Check:** The IP was flagged as suspicious by multiple security vendors

This combination suggests possible malicious hosting activity.

virustotal.com/gui/ip-address/136.243.159.53

136.243.159.53

3 / 92 security vendors flagged this IP address as malicious

136.243.159.53 (136.243.0.0/16)
AS 24940 (Hetzner Online GmbH)

DE Last Analysis Date 18 days ago

Community Score -1

DETECTION DETAILS RELATIONS COMMUNITY 4

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

Crowdsourced context

HIGH 1 MEDIUM 0 LOW 0 INFO 0 SUCCESS 0

Activity related to LOKIBOT - according to source Cluster25 - 2 years ago
↳ This IPv4 is used as a CnC by LOKIBOT

Security vendors' analysis

CRDF	Malicious	CyRadar	Malicious	Activate Windows
				Go to Settings to activate W...

Do you want to automate checks?

Activate Windows Go to Settings to activate W...

Home > Whois Lookup > 103.232.55.148

Notice: Possible deprecation of Whois services after January 28

IP Information for 103.232.55.148

Quick Stats

IP Location	Viet Nam Ha Noi Vietserver Services Technology Company Limited
ASN	AS63737 VIETSERVER-AS-VN VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED, VN (registered Aug 25, 2014)
Whois Server	whois.apnic.net
IP Address	103.232.55.148

% Abuse contact for '103.232.52.0 - 103.232.55.255' is 'hm-changed@vnnic.vn'

```

inetnum:      103.232.52.0 - 103.232.55.255
netname:      VIETSERVER-VN
descr:        VIETSERVER SERVICES TECHNOLOGY COMPANY LIMITED
descr:        Xa Khuc, Chu Phan ward, Me Linh district, Ha Noi City
admin-c:      NNA52-AP
tech-c:       NNA52-AP
country:      VN
mnt-by:       MAINT-VN-VNNIC
mnt-irt:      IRT-VNNIC-AP
status:       ALLOCATED PORTABLE
abuse-c:     NNA52-AP
  
```

DomainTools Iris
The gold-standard Internet intelligence platform
[Learn More](#)

Tools

- Monitor Domain Properties
- Reverse IP Address Lookup
- Network Tools

Activ Go to

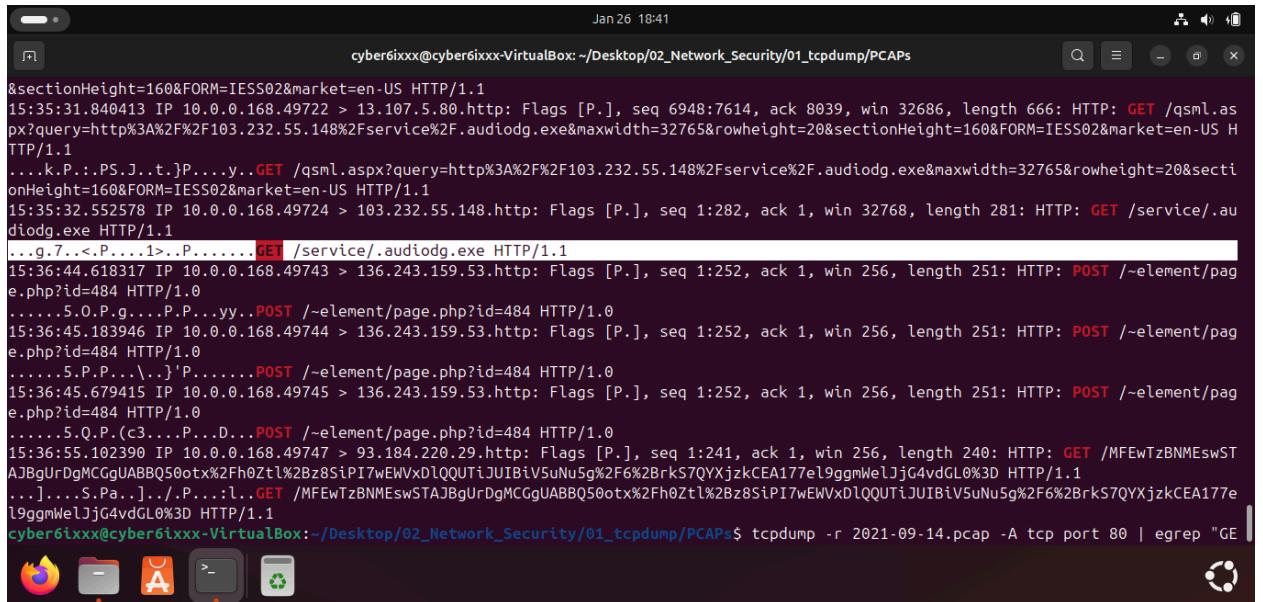
File Download Observed

Traffic analysis indicated the endpoint attempted to download a file named:

.audiodg.exe

Why this is suspicious:

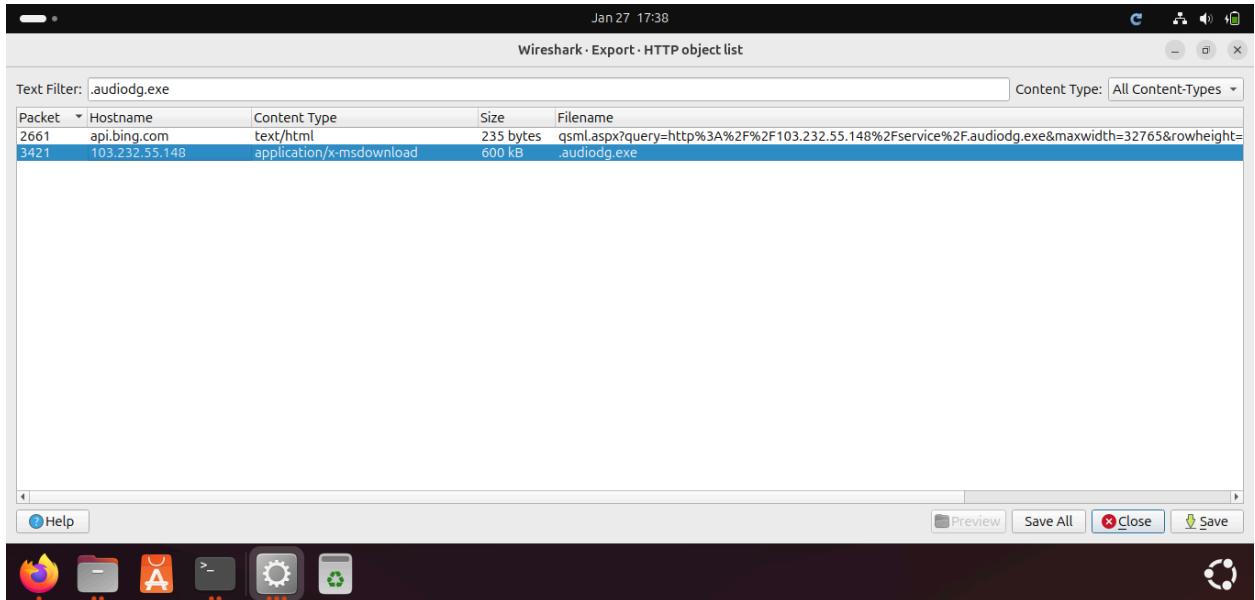
- The file is an **executable (.exe)**
- The naming resembles a legitimate Windows process (**audiodg.exe**), which malware often imitates



```
Jan 26 18:41
cyber6ixxx@cyber6ixxx-VirtualBox: ~/Desktop/02_Network_Security/01_tcpdump/PCAPs
&sectionHeight=160&FORM=IESS02&market=en-US HTTP/1.1
15:35:31.840413 IP 10.0.0.168.49722 > 13.107.5.80.http: Flags [P.], seq 6948:7614, ack 8039, win 32686, length 666: HTTP: GET /qsml.aspx?query=http%3A%2F%2F103.232.55.148%2Fservice%2F.audiogd.exe&maxwidth=32765&rowheight=20&sectionHeight=160&FORM=IESS02&market=en-US HTTP/1.1
....k.P..:PS.J..t.)P....y...GET /qsml.aspx?query=http%3A%2F%2F103.232.55.148%2Fservice%2F.audiogd.exe&maxwidth=32765&rowheight=20&sectionHeight=160&FORM=IESS02&market=en-US HTTP/1.1
15:35:32.552578 IP 10.0.0.168.49724 > 103.232.55.148.http: Flags [P.], seq 1:282, ack 1, win 32768, length 281: HTTP: GET /service/.audiogd.exe HTTP/1.1
...g.7..<.P...1>P.....GET /service/.audiogd.exe HTTP/1.1
15:36:44.618317 IP 10.0.0.168.49743 > 136.243.159.53.http: Flags [P.], seq 1:252, ack 1, win 256, length 251: HTTP: POST /~element/page.php?id=484 HTTP/1.0
.....5.O.P.g...P.P...yy...POST /~element/page.php?id=484 HTTP/1.0
15:36:45.183946 IP 10.0.0.168.49744 > 136.243.159.53.http: Flags [P.], seq 1:252, ack 1, win 256, length 251: HTTP: POST /~element/page.php?id=484 HTTP/1.0
.....5.P.P...\\P.....POST /~element/page.php?id=484 HTTP/1.0
15:36:45.679415 IP 10.0.0.168.49745 > 136.243.159.53.http: Flags [P.], seq 1:252, ack 1, win 256, length 251: HTTP: POST /~element/page.php?id=484 HTTP/1.0
.....5.Q.P.(c3....P...D...POST /~element/page.php?id=484 HTTP/1.0
15:36:55.102390 IP 10.0.0.168.49747 > 93.184.220.29.http: Flags [P.], seq 1:241, ack 1, win 256, length 240: HTTP: GET /MFEwTzBNMEswSTAjBgUrDgMCggUABQ50otx%2Fh0Ztl%2Bz8SiPi7wEWVxDlQQUTiJUIBiVsNu5g%2F6%2BrkS7QYXjkCEA177el9ggmWelJjG4vdGL0%3D HTTP/1.1
[...].....S.Pa...]...P...:l...GET /MFEwTzBNMEswSTAjBgUrDgMCggUABQ50otx%2Fh0Ztl%2Bz8SiPi7wEWVxDlQQUTiJUIBiVsNu5g%2F6%2BrkS7QYXjkCEA177el9ggmWelJjG4vdGL0%3D HTTP/1.1
cyber6ixxx@cyber6ixxx-VirtualBox: ~/Desktop/02_Network_Security/01_tcpdump/PCAPs$ tcpdump -r 2021-09-14.pcap -A tcp port 80 | egrep "GE
```

Safely Download and Investigate Malicious File

The suspicious executable was safely extracted and subjected to static analysis. File hashing and string inspection were performed without execution to avoid system compromise.



Hash Generation

The file's SHA256 hash was calculated:

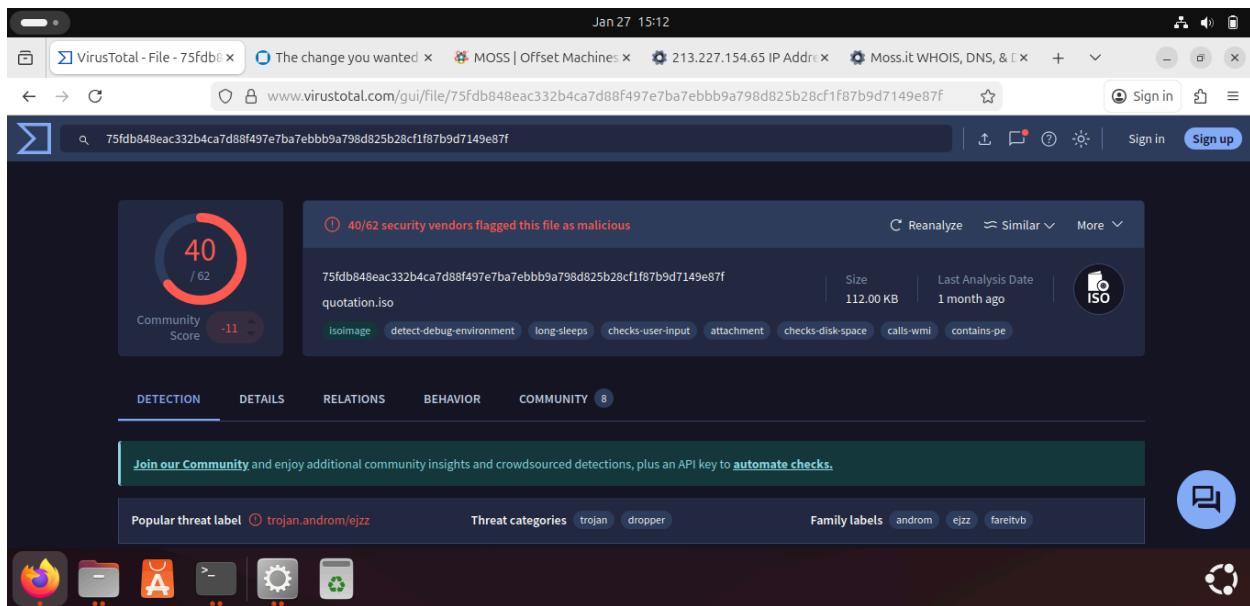
Sha256sum .audiogd.exe

```
Jan 27 15:07
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$ ls
PCAPs
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$ ls -a
. ... .audiogd.exe PCAPs
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$ sha256 .audiogd.exe
Command 'sha256' not found, but can be installed with:
sudo apt install hashalot
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$ sha256sum .audiogd.exe
f485d1a65ccf9f857baa49725d337c15e8aa34515b85c8ef59a72afad7b85249 .audiogd.exe
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$ sha256sum .audiogd.exe && sha1sum .audiogd.exe && md5sum .audiogd.exe
f485d1a65ccf9f857baa49725d337c15e8aa34515b85c8ef59a72afad7b85249 .audiogd.exe
4ff997f6479d3535b093abe1a5e297a3548d959 .audiogd.exe
da4f1a581f73ae0984cc58b61e12bd4c .audiogd.exe
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$ ^C
cyber6ixxx@cyber6ixxx-VirtualBox:~/Desktop/02_Network_Security/02_Wireshark$
```

Threat Intelligence Verification

The SHA256 hash was searched on **VirusTotal**, where the file was flagged as malicious by **40 security vendors**, identifying it as a **Trojan**.

This confirms that the observed HTTP traffic resulted in the download of verified malware.



Indicators of Compromise (IOCs)

Type	Value
Malicious IP	103.232.55.14
	8
Suspicious File	.audiog.exe
Affected Host	10.0.0.168
Sha256 Hash	f485d1a65ccf9f 857baa49725d 337c15e8aa34 515b85c8ef59 a72afad7b852 49

Conclusion

This investigation confirms a successful malware download from a malicious external server. Network evidence, OSINT analysis, and malware hash verification collectively validate the presence of a Trojan infection, supporting escalation for containment and incident response.

These findings support escalation for:

- Host isolation
- Malware scanning
- Log correlation
- Post-incident response procedures