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

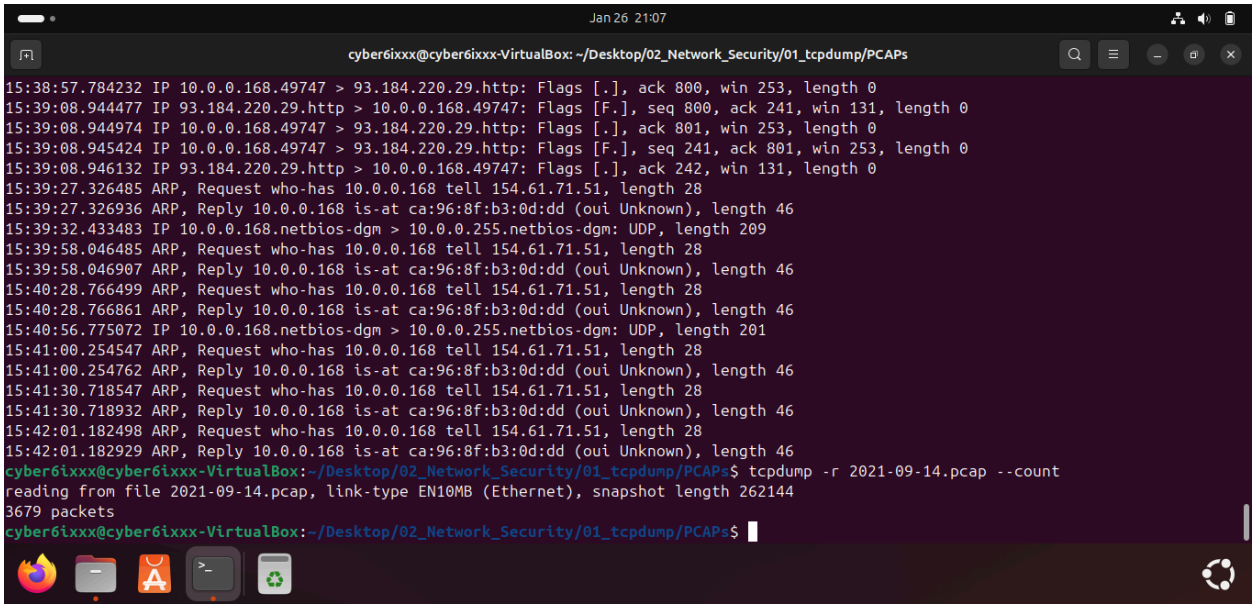
The PCAP file was examined using:

```
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.

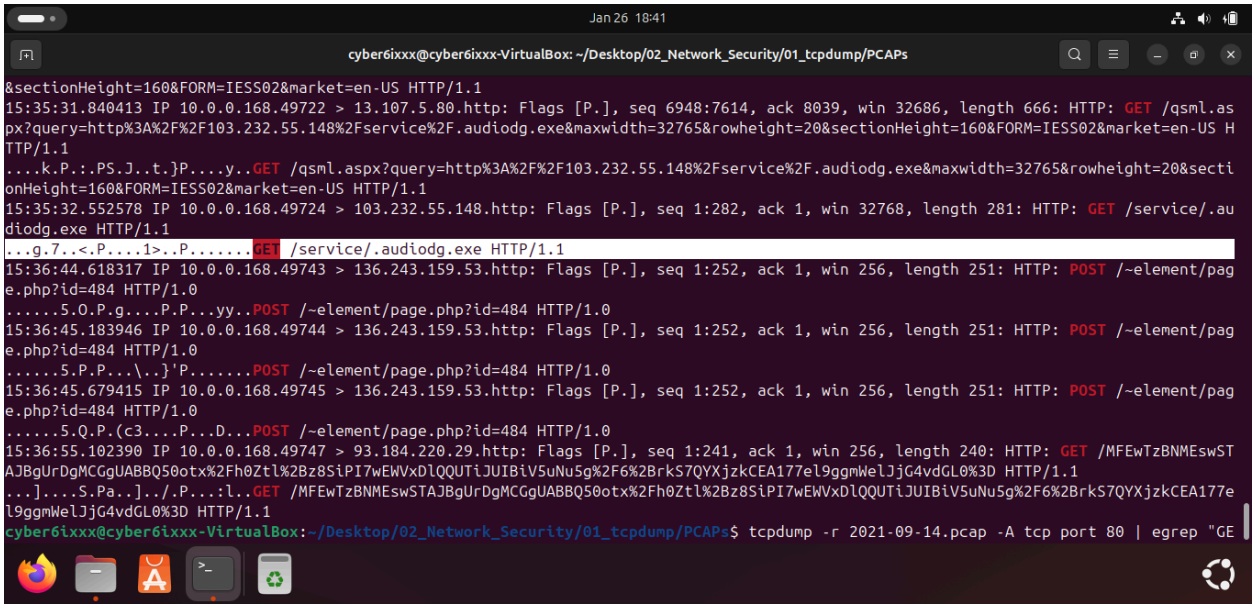


Filtering for Web Traffic

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.



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

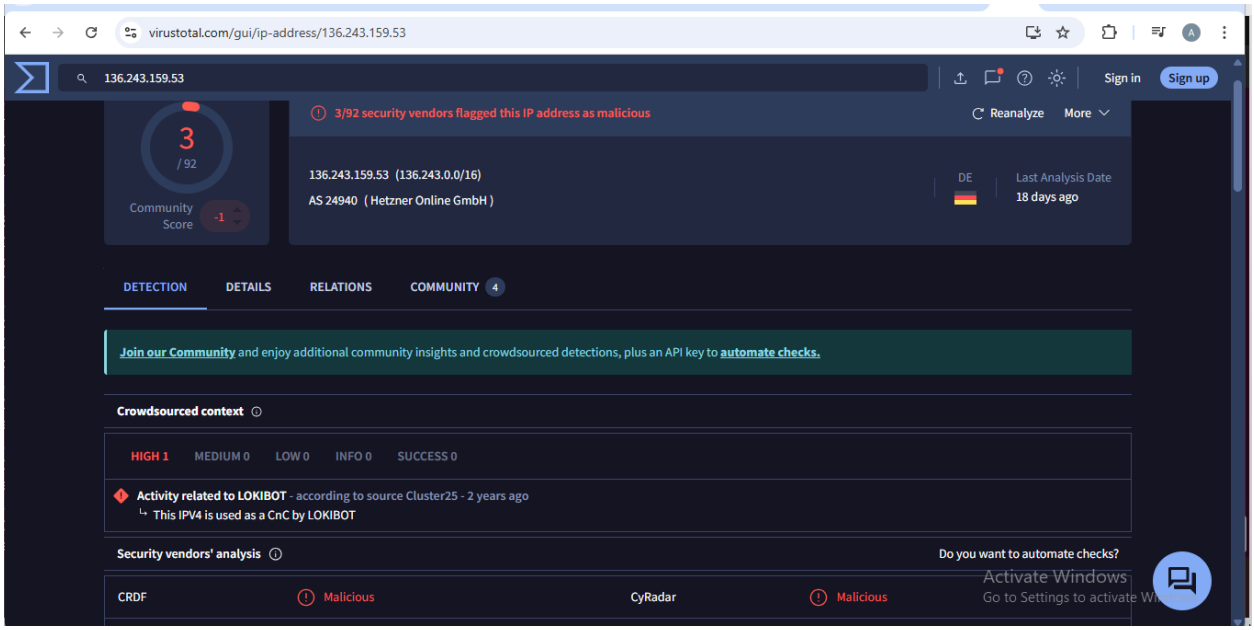
This shows the internal host initiated communication with an unknown external server.

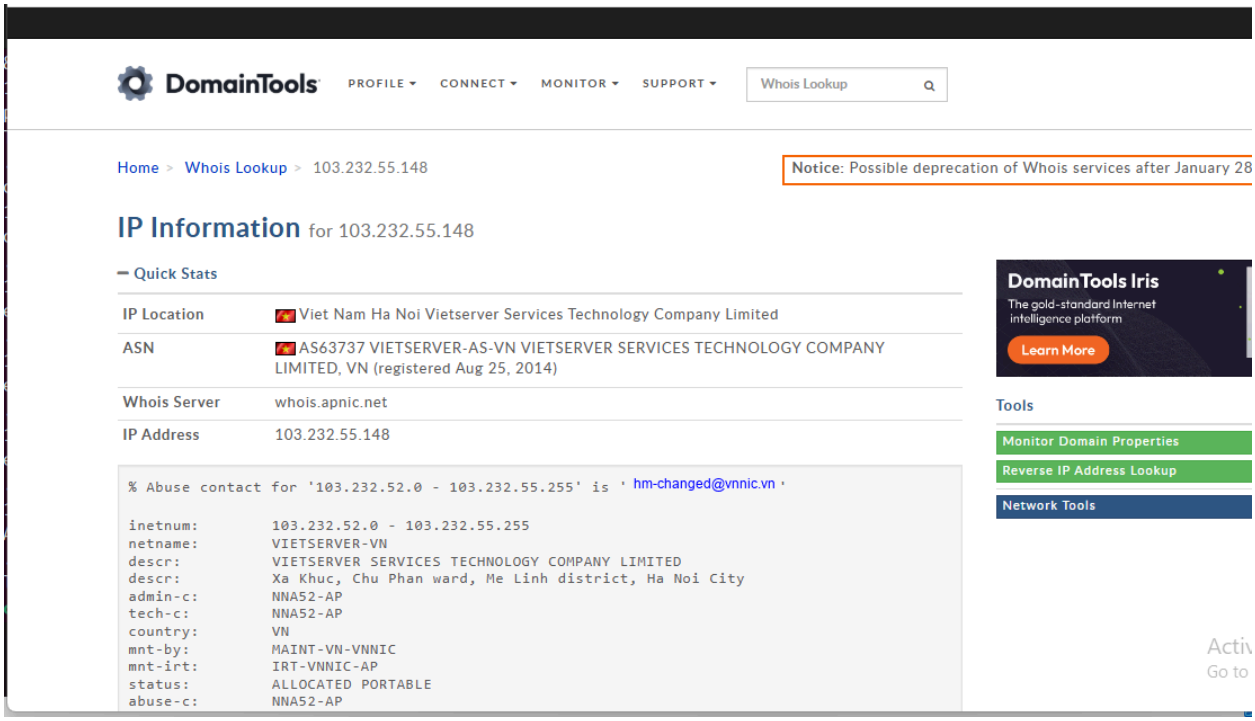
OSINT Investigation

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
Sign in
Sign up
3
/ 92
Community Score
-1
3/92 security vendors flagged this IP address as malicious
Reanalyze
More
136.243.159.53 (136.243.0.0/16)
AS 24940 (Hetzner Online GmbH)
DE
Last Analysis Date
18 days ago
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
Do you want to automate checks?
CRDF
Malicious
CyRadar
Malicious
Activate Windows
Go to Settings to activate Windows.


DomainTools
PROFILE
CONNECT
MONITOR
SUPPORT
Whois Lookup
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

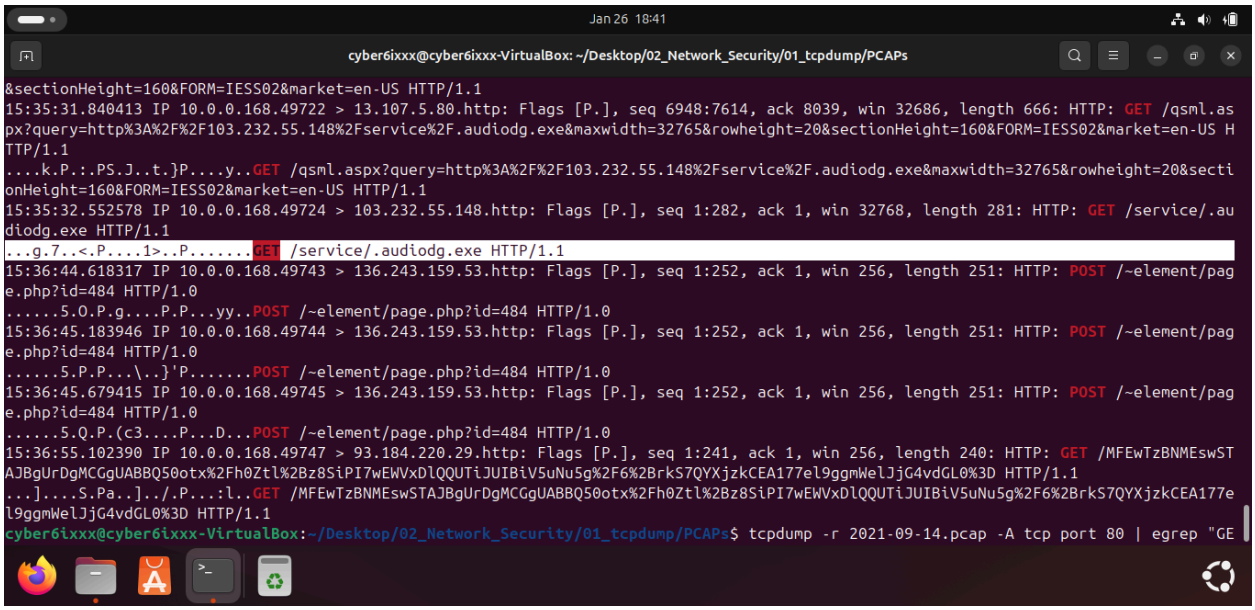
File Download Observed

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



Indicators of Compromise (IOCs)

Type	Value
Malicious IP	103.232.55.148
Suspicious File	.audiodg.exe

Affected Host	10.0.0.168

Conclusion

The analysis identified outbound HTTP communication from an internal host to a suspicious external server, resulting in the download of a potentially malicious executable file. OSINT verification strengthens the likelihood of malicious activity.

These findings support escalation for:

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