

**ANALYSING THE RISK PROFILE OF POPULAR
DOMAINS: USING NSLOOKUP AND IP
REPUTATION DATABASES FOR THREAT
DETECTION**

BY

SOMKENE RICHARD

17th SEPTEMBER, 2024

EXECUTIVE SUMMARY

Domain names and IP addresses are critical targets in cyberattacks, and popular domains are most times targeted for these malicious attacks to lure and exploit users' credentials.

In this analysis, five popular domains were focused to ensure it's IP reputations and detect any possible threat attributed to it. A few IP threats were detected during this analysis.

INTRODUCTION

Several types of cyberattacks are directly related to domain names and IP addresses. These attacks often exploit vulnerabilities in DNS or leverage malicious IP addresses to harm users, networks, and systems. In this analysis, popular domains used are Samsung.com, Microsoft.com, gtbank.com, oandopl.com, and dangote.com.


TOOLS

1. Hp Laptop: device used for the analysis
2. Virustotal: used for ip address analysis and malicious detection
3. Abuseipdb: used for more ip address analysis and reporting of suspicious of malicious IP addresses
3. Pen and paper: used for writing and taking note of details

ANALYSIS

Using the command prompt, the nslookup tool was launched for each of the 5 domains mentioned earlier,

1. Samsung.com



```
C:\Windows\system32\cmd.exe X + v
C:\Users\richa>nslookup samsung.com
Server: Unknown
Address: 192.168.230.169

Non-authoritative answer:
Name:   samsung.com
Address: 211.45.27.231
```

Fig1: nslookup details of samsung.com

2. Microsoft.com

```
C:\Users\richa>nslookup microsoft.com
Server: Unknown
Address: 192.168.230.169

Non-authoritative answer:
DNS request timed out.
    timeout was 2 seconds.
Name:    microsoft.com
Addresses: 20.112.250.133
           20.231.239.246
           20.76.201.171
           20.70.246.20
           20.236.44.162
```

Fig 2: nslookup details of microsoft.com

3. gtbank.com

```
C:\Users\richa>nslookup gtbank.com
Server: Unknown
Address: 192.168.230.169

Non-authoritative answer:
Name:    gtbank.com
Address: 45.60.46.99
```

Fig 4: nslookup details of gtbank.com

4. Oandopl.com

```
C:\Users\richa>nslookup oandopl.com
Server: Unknown
Address: 192.168.230.169

Non-authoritative answer:
Name:    oandopl.com
Addresses: 192.124.249.58
           20.105.232.12
```

Fig 4: nslookup details of oandopl.com

5. Dangote.com

```
C:\Users\richa>nslookup dangote.com
Server: Unknown
Address: 192.168.230.169

Non-authoritative answer:
Name:    dangote.com
Address: 13.69.68.37
```

Fig 5: nslookup details of dangote.com

Checking their IP addresses for any malicious detection:

1. Samsung.com

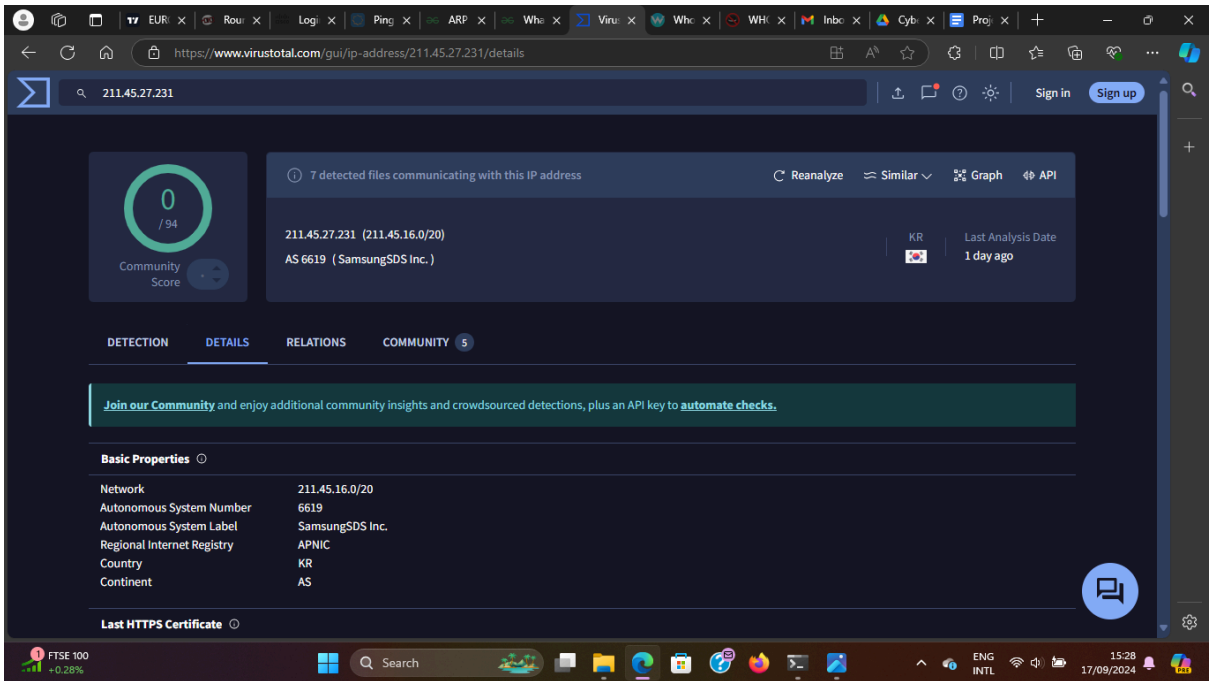


Fig 6: Ip address scanning on virustotal

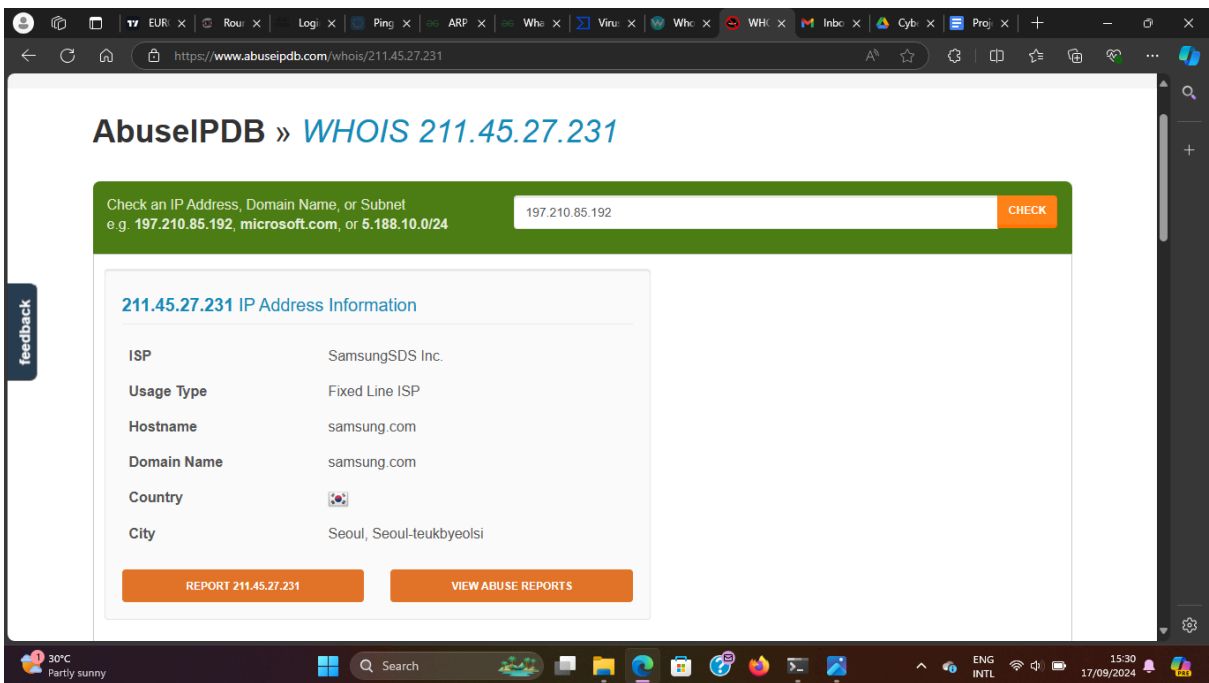


Fig 7: Ip address information on abuseipdb

2. Microsoft

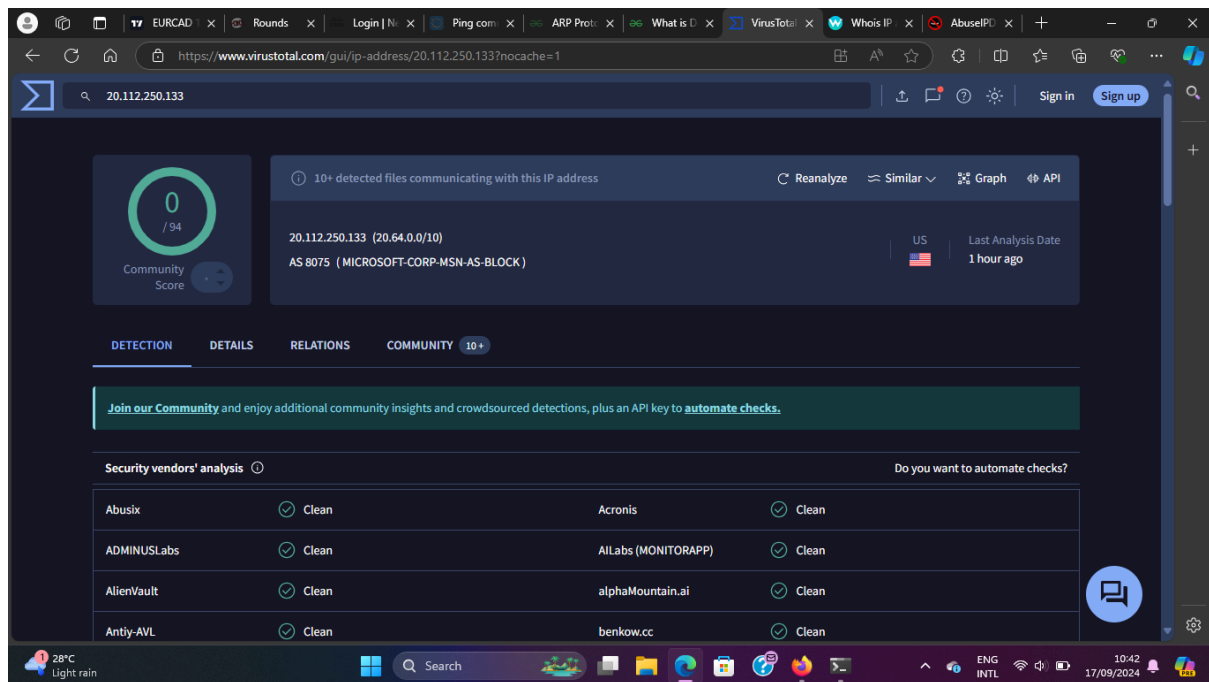


Fig 8: IP address scanning on virustotal

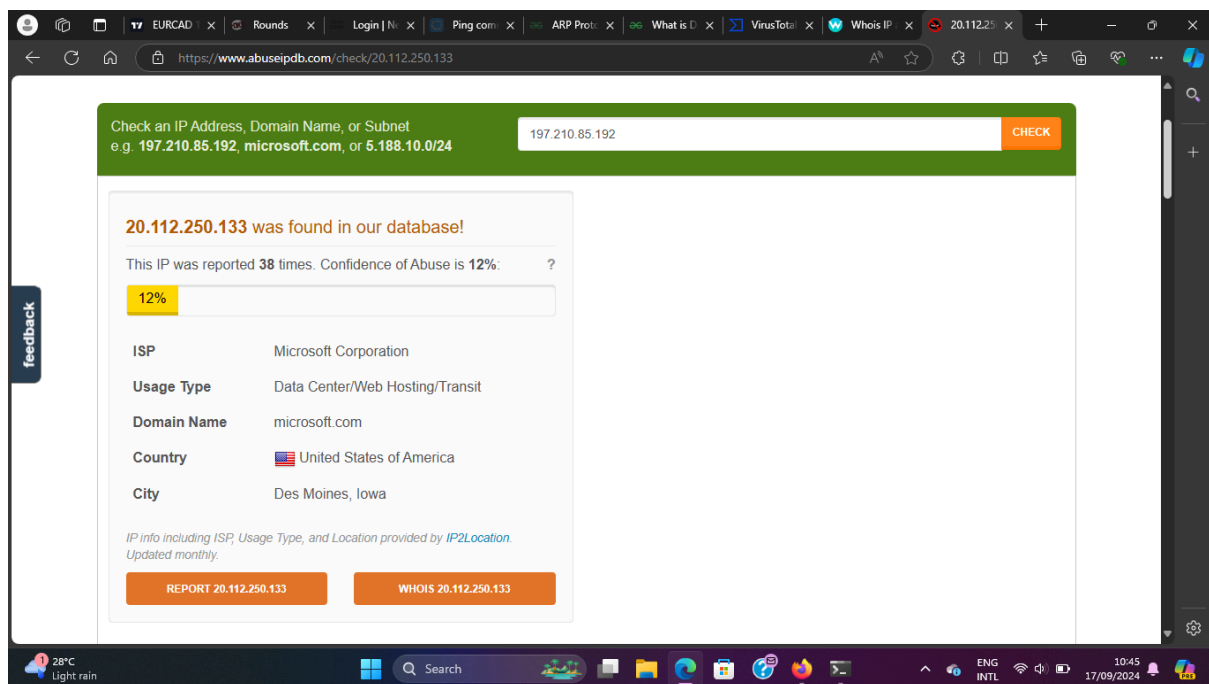


Fig 9: IP address information on abuseipdb

3. gtbank.

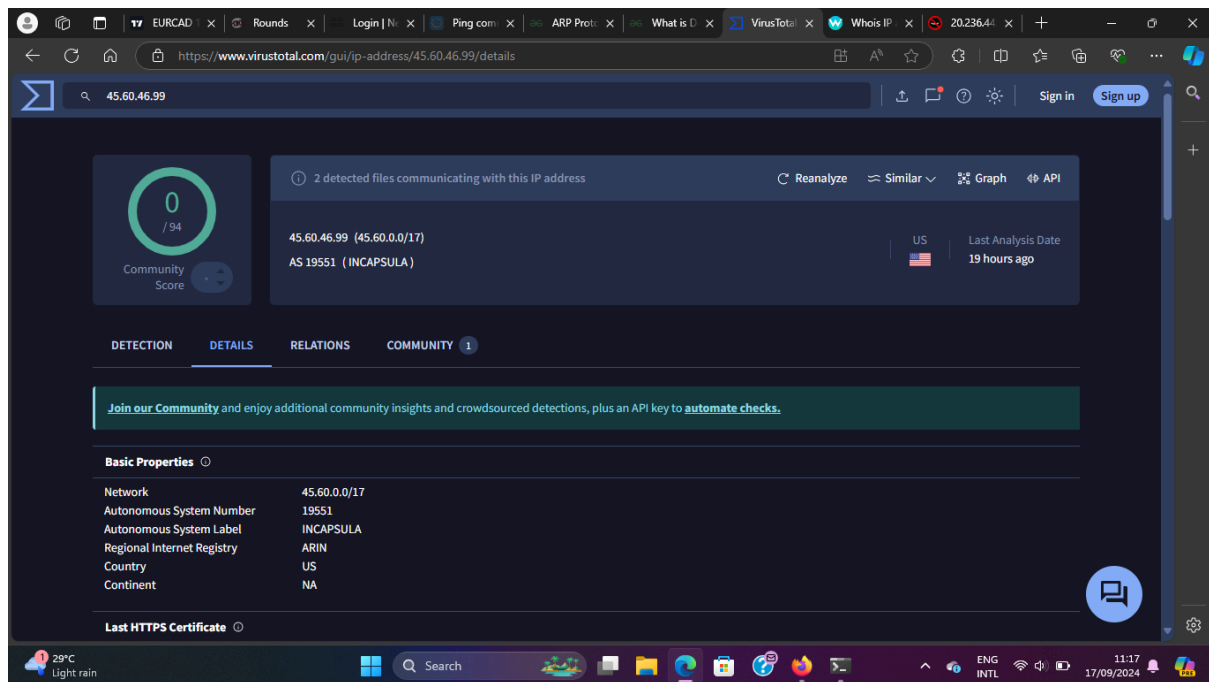


Fig 10: IP address scanning on virustotal

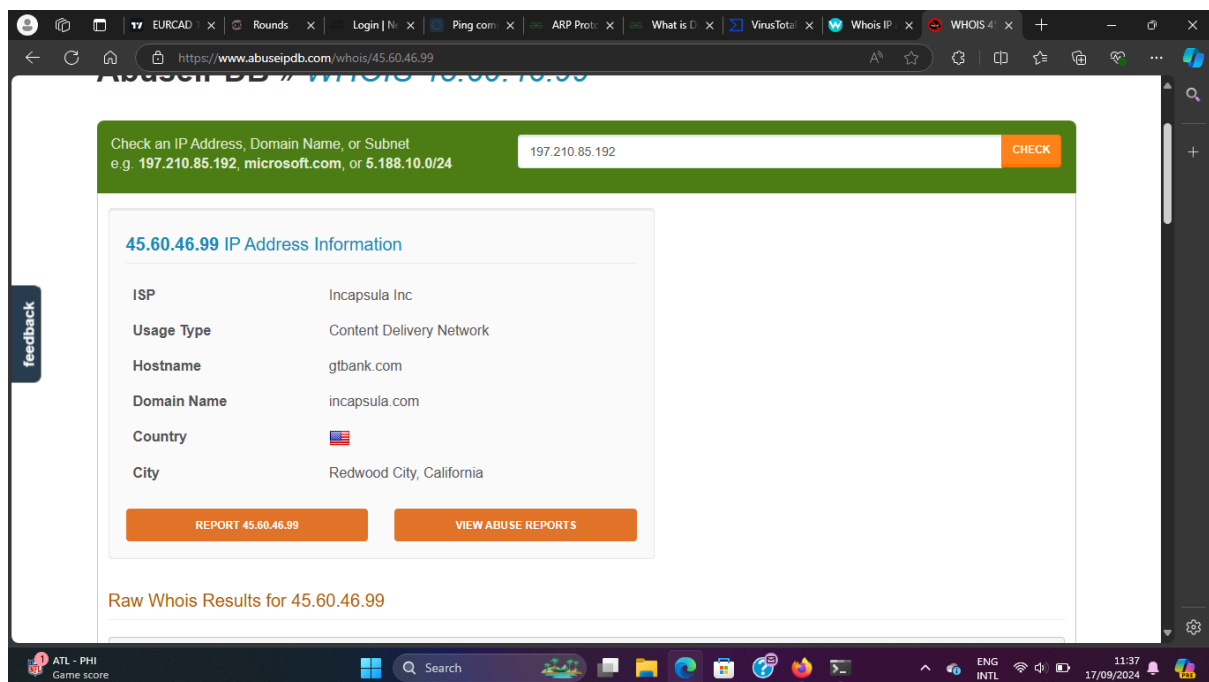


Fig 11: IP address information on abuseipdb

4. Oando

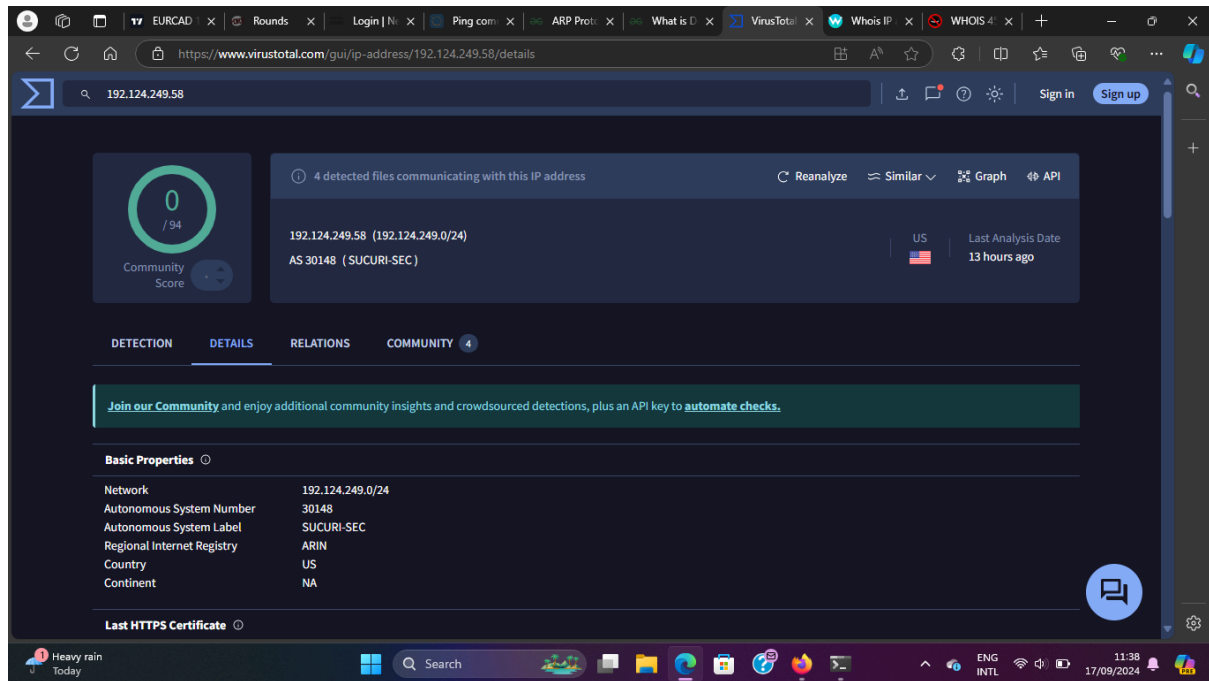


Fig 12: IP address scanning on virustotal

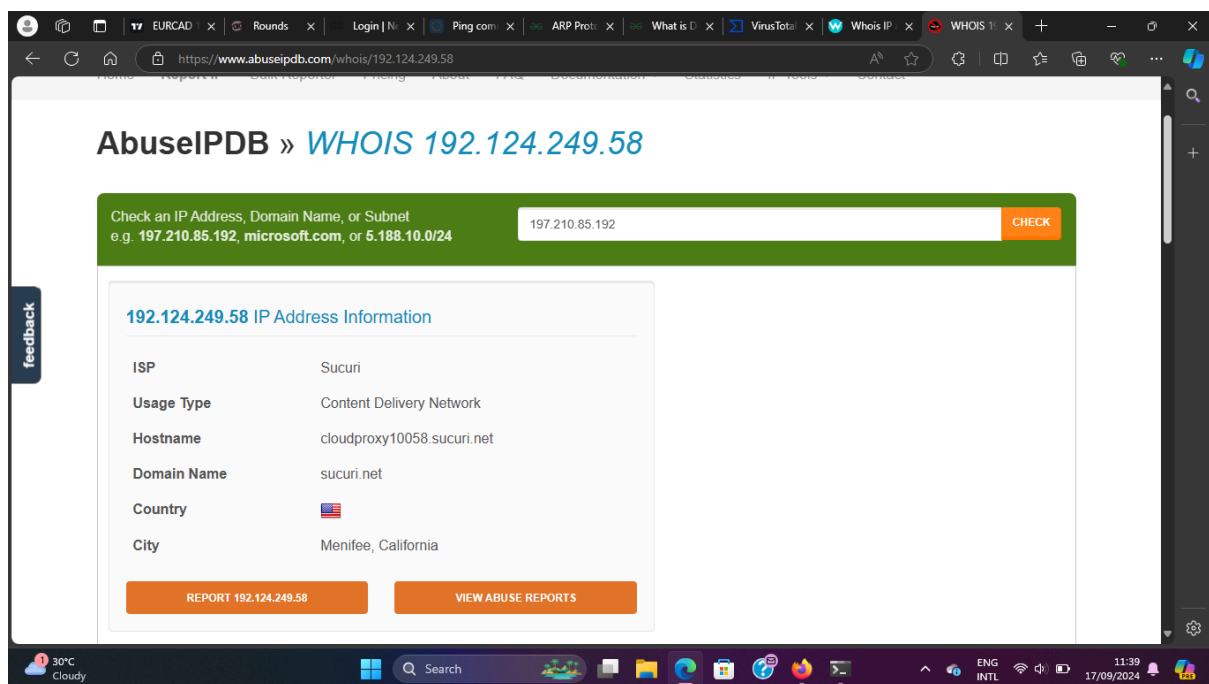


Fig 13: IP address information on abuseipdb

5. Dangote

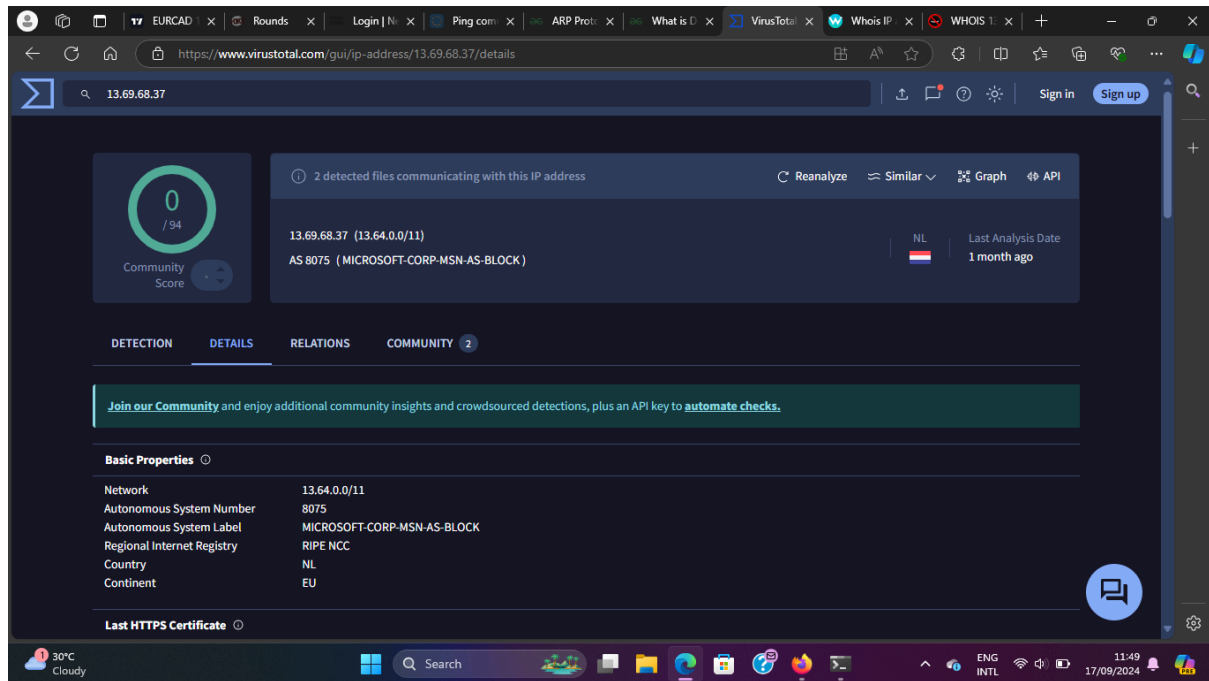


Fig 14: IP address scanning on virustotal

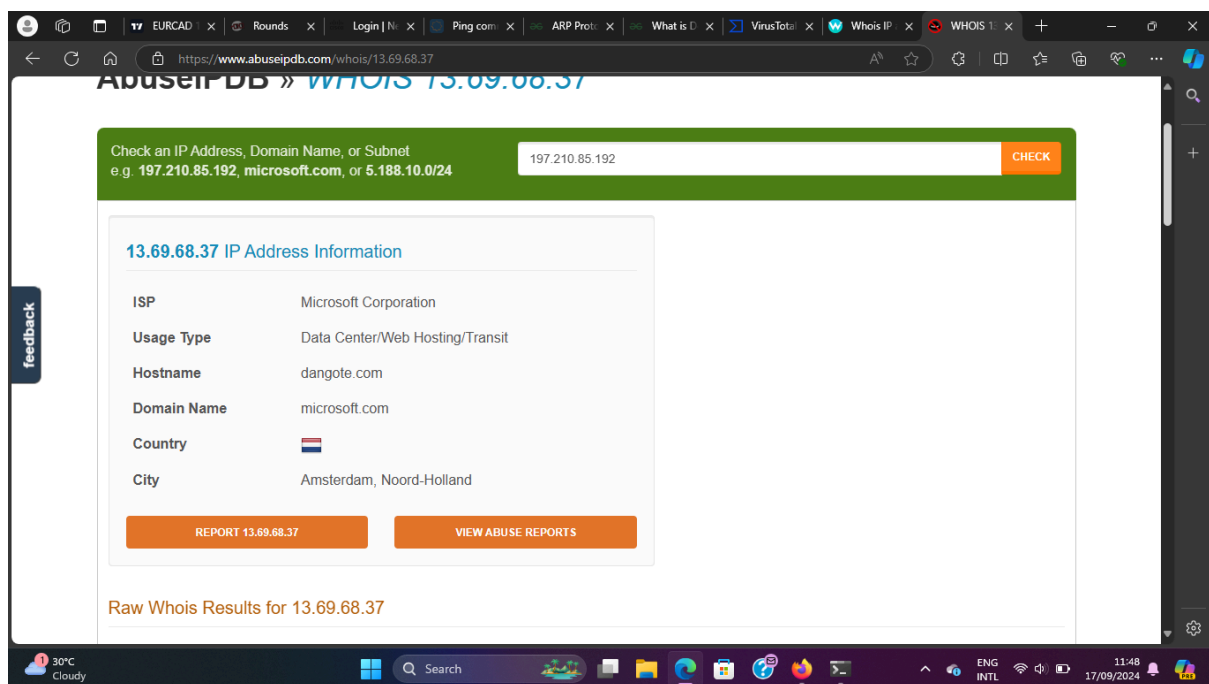


Fig 15: IP address information on abuseipdb

From Virustotal, the IP addresses of the above popular domains were seen to be malicious-free and safe for interaction. Whereas, with the details seen from abuseipdb, all the domains make use of cloud-based ISPs which has been recorded to be cost effective and more efficient in resource allocation.

Samsung.com and Microsoft.com use their own ISPs while gtbank.com, Oando.com, and dangote.com make use of a third-party ISP.

CONCLUSION

With no threat detected from these domain ip addresses It could be seen that the organisations/institutions are conscious in terms of securing their respective data. Regular scanning of the various IPs and networks can also be conducted to avoid any malicious attacks from threat actors, Intrusion Detection and Prevention Systems can also be deployed for more proactive measures.