

Incident Analysis Report

1. Alarm Information

- **Alarm ID / Case No:** 002
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** External Port Scan detected from IP 199.45.154.176
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

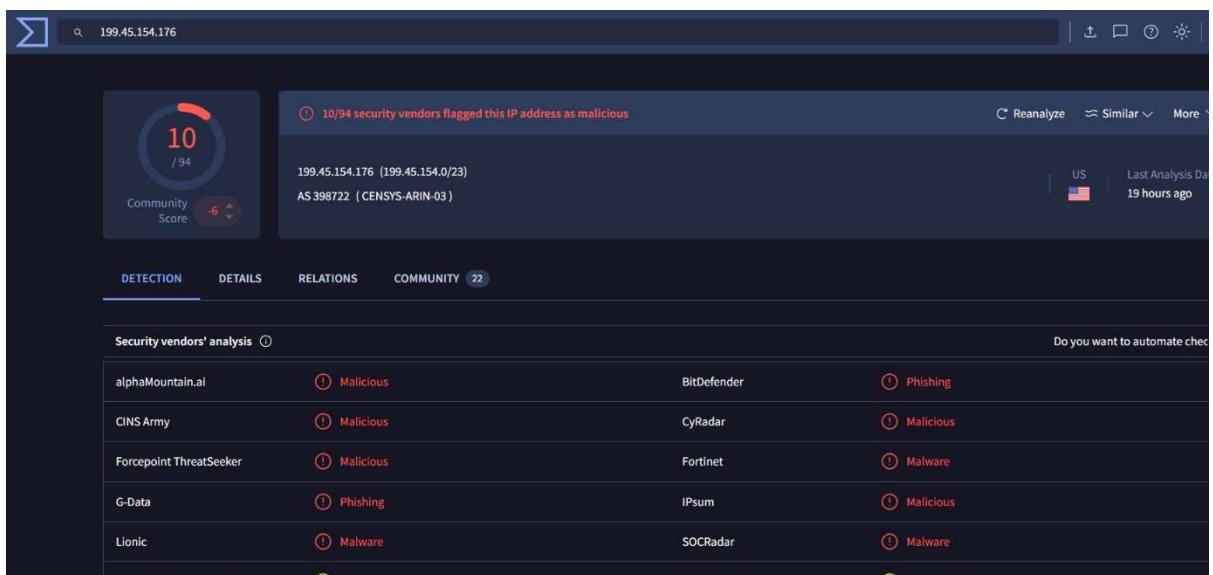
2. IOC Information

- **IOC Type:** IP Address
- **IOC Value:** 199.45.154.176
- **IOC Location:** [USA]

3. OSINT Investigation

VirusTotal

- Result: Detected by 1 AV engine (low confidence).
- <https://www.virustotal.com/gui/ip-address/199.45.154.176>



Comments (18) ○

ObserverPassive 1 day ago

Firewall logs - Blocked inbound connection from 199.45.154.176 from accessing WAN interface over port TCP 3390 (Distributed Service Coordinator)

Nonstop attacks, 24/7, around the clock, for years now, on my home network (see my profile for the rest of the IP addresses attacking my home network daily). Every device of mine is infected with advanced spyware (regardless of reboots, factory reset, buying new devices, the backdoors are persistent, similar to pegasus).

Privacy is NOT a crime just saying, the overreach has gotten so out of control.

Below is a summary of the attackers (government overreach - I am saying this because it's years of research, forensics, logs from the network and devices, and observation. If you are a Trump supporter, you are most likely targeted by these weak cowards that need to team up in groups to make themselves feel powerful, since they have no control over their own lives, they clearly like taking the anger they have with themselves and their life, out on others in order to seek power and control through. All part of the Digital ID and social credit score plan they have been pushing to roll out). People are waking up... Stop the false flags, propaganda, and gaslighting... I recommend checking out the Alex Jones Show on Rumble, The Officer Tatum Show on YT, or Liberal Hiveman on YT, to see what is actually going on.

Show more

ObserverPassive 23 days ago

Firewall Logs - Blocked inbound attempt from 199.45.154.176 from accessing WAN interface over port TCP 9600 (micromuse-ncpw)

Nonstop intrusion attempts - see my profile for the rest of the IPs attacking my home network persistently, for years now. I recommend watching the Alex Jones Show, the people who seek censorship, money, power, and then frame, gaslight, and attack others in order to fulfill their agenda, need to be brought to light.

AbuseIPDB

- Result: 100% Abuse Confidence Score – reported for External Port Scan activity.
- <https://www.abuseipdb.com/check/199.45.154.176>

Check an IP Address, Domain Name, or Subnet
e.g. 2a02:1210:7840:7400:a0d8:8bda:7aa3:162f, microsoft.com, or 5.188.10.0/24

199.45.154.176 **CHECK**

199.45.154.176 was found in our database!

This IP was reported 56,129 times. Confidence of Abuse is **100%**. ?

ISP	Censys, Inc.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS398722
Hostname(s)	scanner-001.hk2.censys-scanner.com
Domain Name	censys.com
Country	Hong Kong

4. Analysis & Assessment

- VirusTotal result alone is weak evidence.
- AbuseIPDB provides stronger indication of External Port Scan with multiple reports.

5. Conclusion / Decision

- Decision:** **True Positive**

- **Category:** External Port Scan
 - **Risk Level:** High (based on organization's classification)
-

6. Recommended Actions

1. Block the IP address on firewall / IPS.
2. Review SIEM logs for additional login attempts from the same source.
3. Correlate failed logins with user accounts for potential compromise attempts.
4. Consider implementing automated blocking rules for IPs with high abuse scores.