

Incident Analysis Report

1. Alarm Information

- **Alarm ID / Case No:** 003
- **Alarm Source:** SIEM / IDS
- **Alarm Description:** Brute Force detected from IP 194.165.16.165
- **Timestamp:** [e.g., 2025-08-24 13:20 CET]

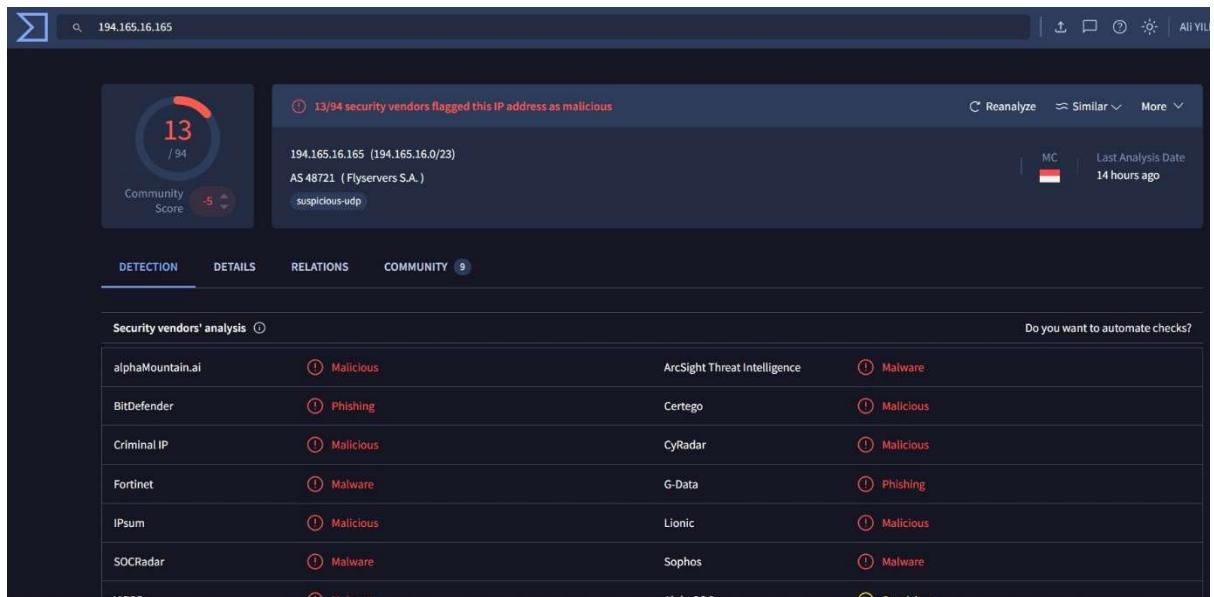
2. IOC Information

- **IOC Type:** IP Address
- **IOC Value:** 194.165.16.165
- **IOC Location:** [Lithuania]

3. OSINT Investigation

VirusTotal

- Result: Detected by 1 AV engine (low confidence).
- <https://www.virustotal.com/gui/ip-address/194.165.16.165/details>



AbuseIPDB

- Result: 100% Abuse Confidence Score – reported for Brute Force activity.
- <https://www.abuseipdb.com/check/194.165.16.165>

The screenshot shows the AbuselPDB website interface. At the top, there is a navigation bar with links for Report IP, Bulk Reporter, Bulk Checker, Pricing, Docs, IP Utilities, Contact, and More. On the far right, there are Login and Sign Up buttons. Below the navigation bar, the URL "AbuselPDB » 194.165.16.165" is displayed. A search bar at the top has placeholder text "Check an IP Address, Domain Name, or Subnet" and contains the value "194.165.16.165". To the right of the search bar is a "CHECK" button. The main content area displays a message: "194.165.16.165 was found in our database!" followed by a note: "This IP was reported 6,934 times. Confidence of Abuse is 100%". A large red progress bar indicates a confidence level of 100%. Below this, a table provides detailed information about the IP address:

ISP	Flyservers S.A.
Usage Type	Data Center/Web Hosting/Transit
ASN	AS48721
Domain Name	flyservers.com
Country	Lithuania
City	Kaunas, Kaunas

4. Analysis & Assessment

- VirusTotal result alone is weak evidence.
- AbuselPDB provides stronger indication of Brute Force with multiple reports.

5. Conclusion / Decision

- **Decision:** True Positive
- **Category:** Brute Force
- **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.