Honeypot in Linus & Splunk + OSINT Analysis

Threat actors continuously scour the internet for open ports and vulnerable applications. To demonstrate this, I created my own Honeypot using OpenAI/ChatGPT. The honeypot ran for at least 5 days, after logging results I analyzed its output in Splunk.

I chose the following ports at random to expose to the open internet:

Port 3389 (RDP): Remote Desktop Protocol. Allows remote access to a Windows computer's desktop.

Port 34567: Commonly used for video surveillance systems and IP cameras, particularly Chinese brands.

Port 8000: Frequently used for web servers and HTTP-based applications. Can also be used for other services like remote administration or streaming.

Comparison between ports 3389, 34567, and 8000

While these ports serve distinct purposes, they can indirectly interact within a network or system:

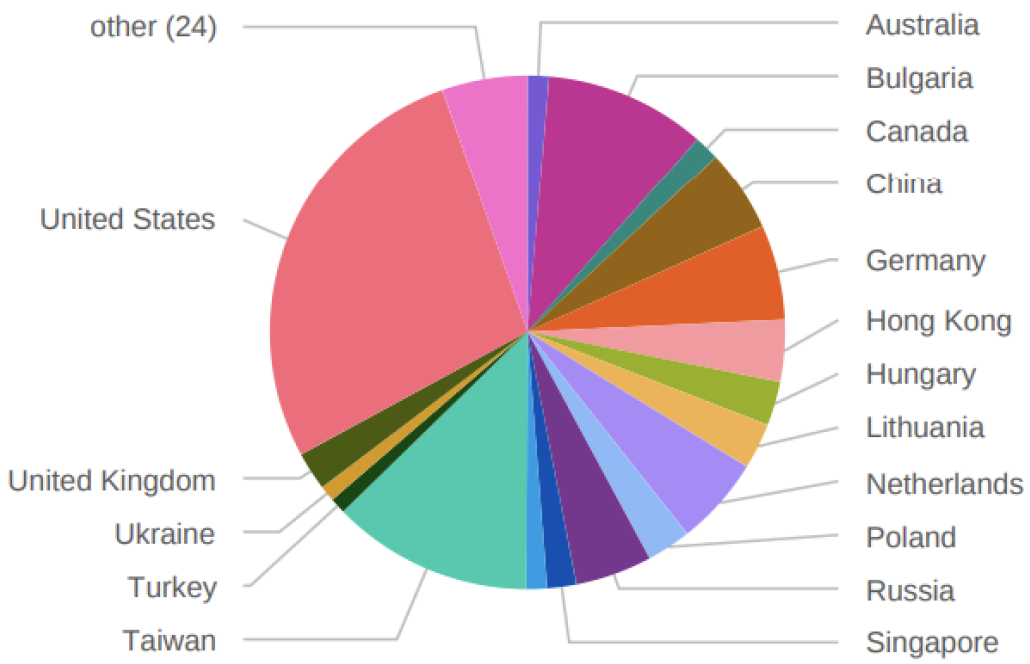
1. **Remote Administration and Monitoring**:
    - Port 3389 (RDP): An administrator could use RDP to remotely access a server or workstation.
    - Port 8000: A web-based monitoring tool could be hosted on port 8000, allowing the administrator to remotely view system logs, performance metrics, or security alerts.
    - Port 34567: In a surveillance scenario, the administrator could use RDP to access a server running surveillance software and then view live feeds or recorded footage through a web interface hosted on port 8000.
2. **Web-Based Access to IP Cameras**:
    - Port 34567: IP cameras typically use this port for streaming video.
    - Port 8000: A web server could be configured to provide a user interface for accessing and controlling these cameras. This interface might be accessible via a web browser, using port 8000.

Key Point: The direct interaction between these ports is limited. However, they often coexist in network environments, especially in scenarios involving remote administration, surveillance, and web-based services. The specific interactions depend on the network configuration and the services running on each port.

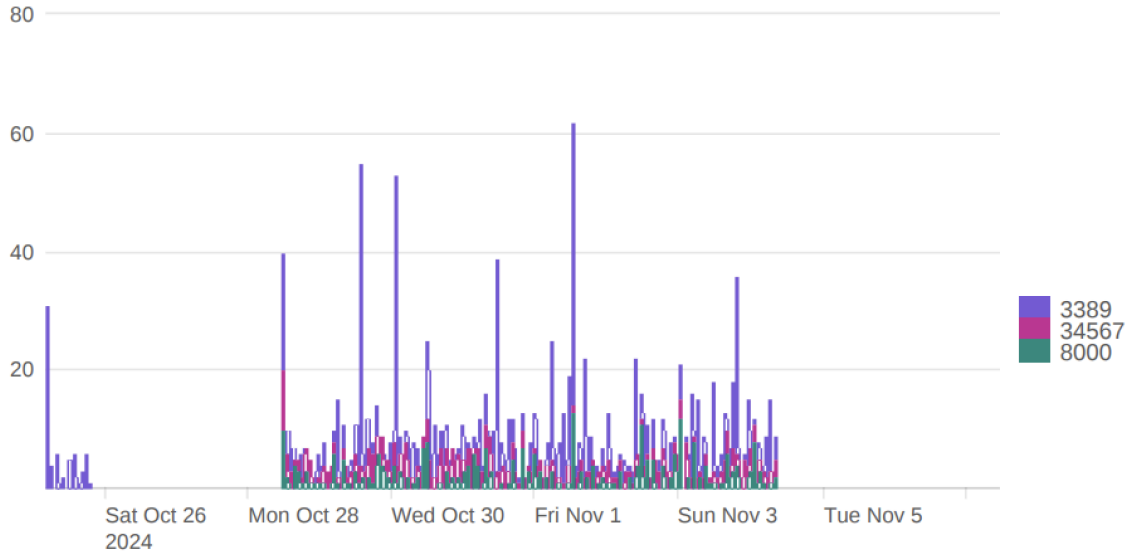
Honeypot Results & Analysis

Using Splunk I was able to visualize number of times each port was targetted, including when and where, and finally I was able to rank each unique IP address by threat count.

Percentage of attacks from Country origin



Ports exposed to the public internet over six days



Source IP by threat count - city, country, region

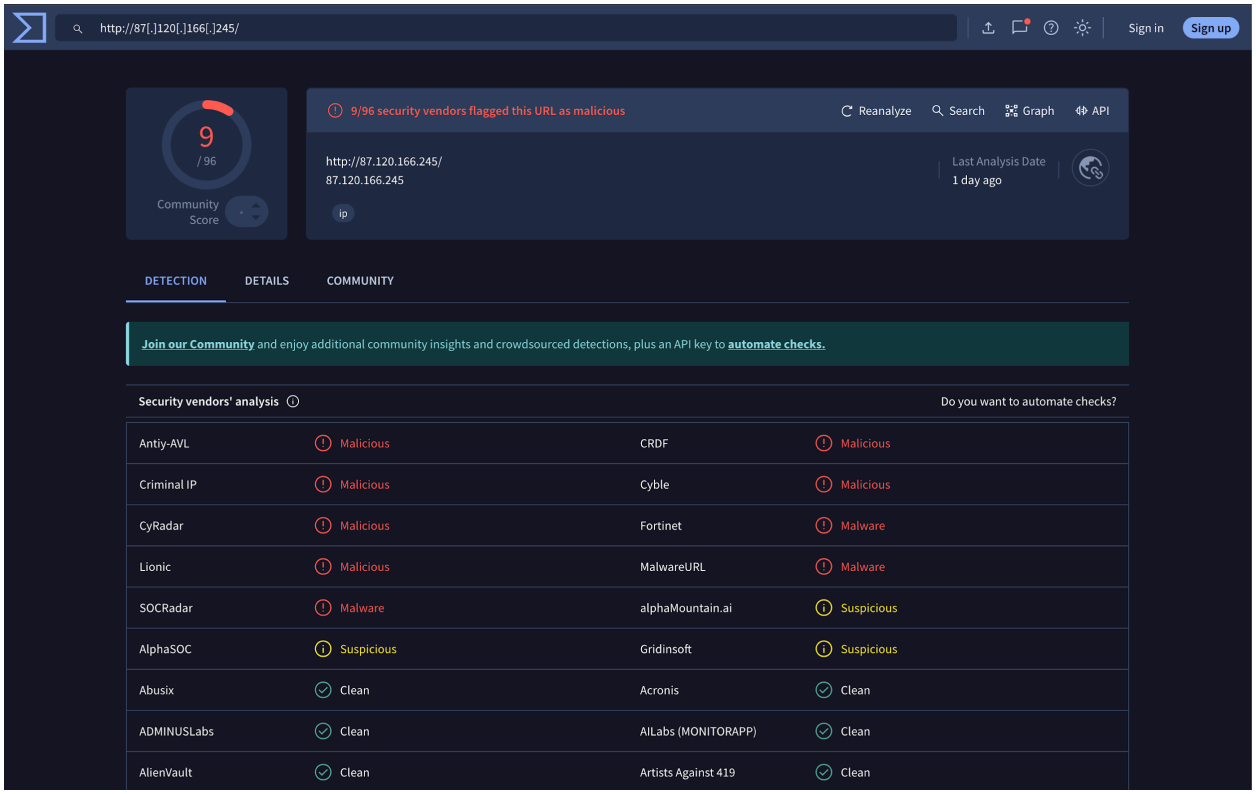
src	count	percent	City	Country	Region	lat	lon
87.120.166.245	161	9.476162	Sofia	Bulgaria	Sofia-grad	42.65070	23.37670
154.213.184.18	41	2.413184	Hong Kong	Hong Kong	Central and Western	22.39640	114.10900
89.183.193.227	40	2.354326	Frankfurt am Main	Germany	Hesse	50.11090	8.68213

I was able to enhance my findings by leveraging open-source intelligence tools, including **VirusTotal**, **AbuseIPDB**, and **GreyNoise**, to gain deeper insights into the IP addresses that connected to my Honeypot. Here are findings for the top three most aggressive unique IP addresses encountered.

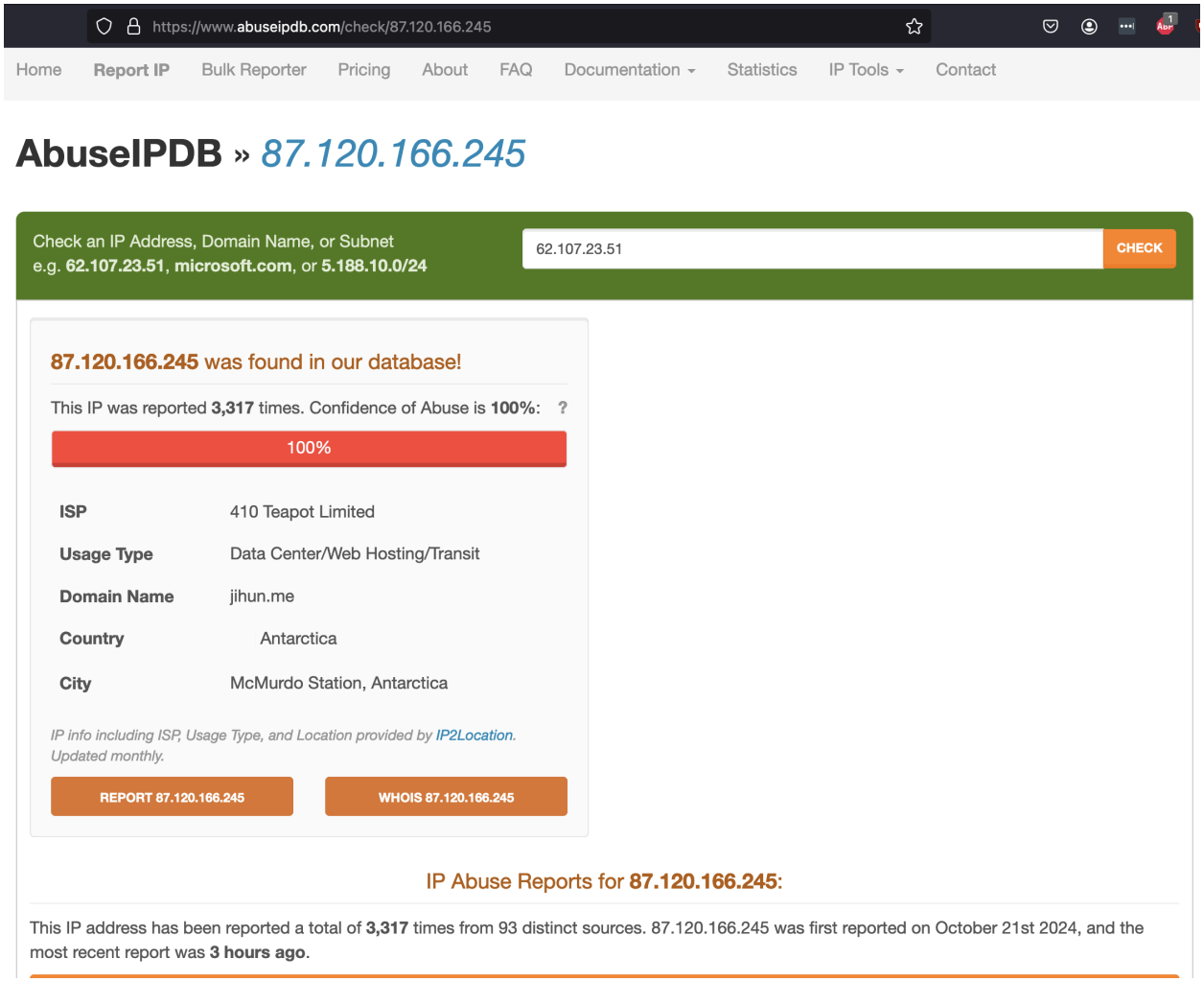
Top 3 Source IPs

1) ***87[.]120[.]166[.]245*** *- malicious*

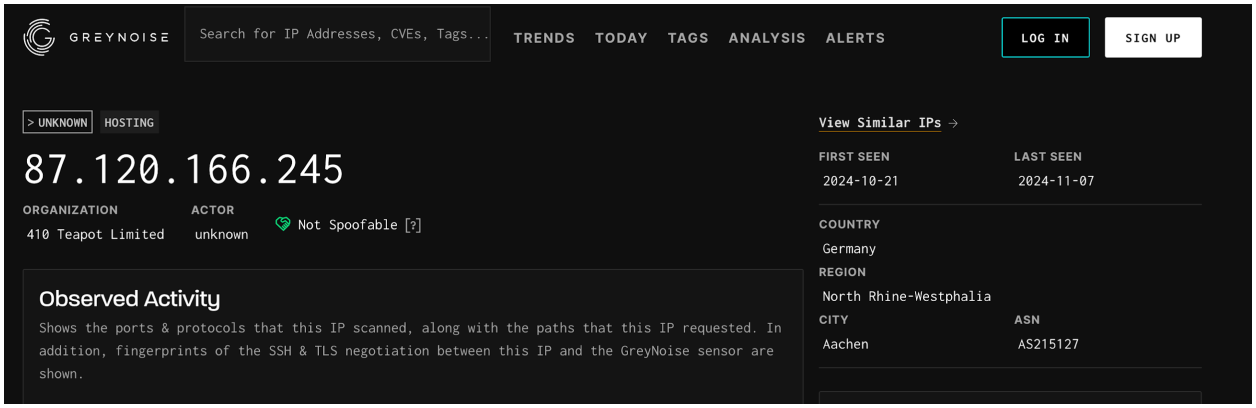
[VirusTotal Community Score](#) = 9/96



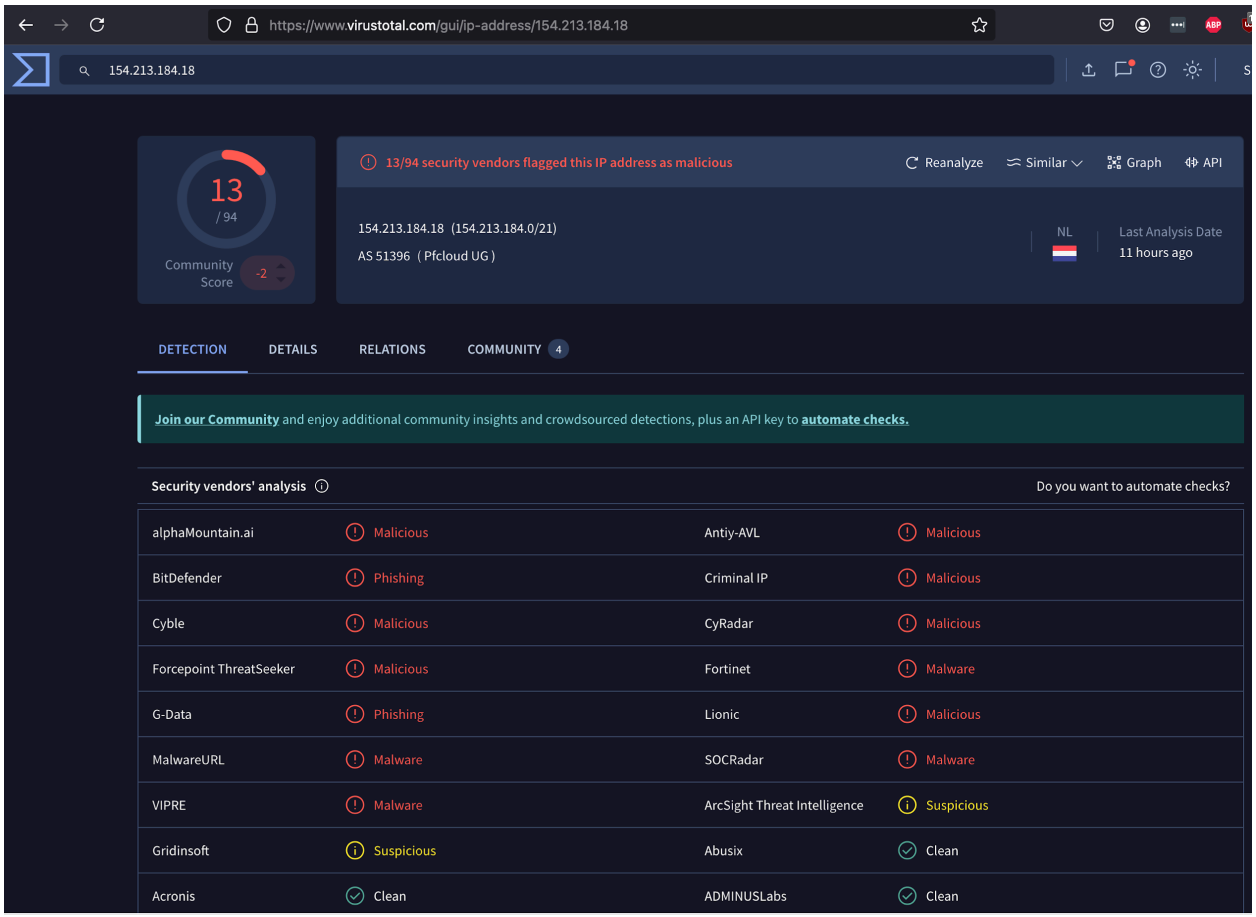
Abuseipdb score = Confidence of Abuse is 100% (This IP was reported 3,317 times)



GreyNoise = “GreyNoise has identified scanning activity from this IP, however we cannot determine its intent. It is still considered internet background noise since it is scanning the entire internet and NOT targeting you specifically.”

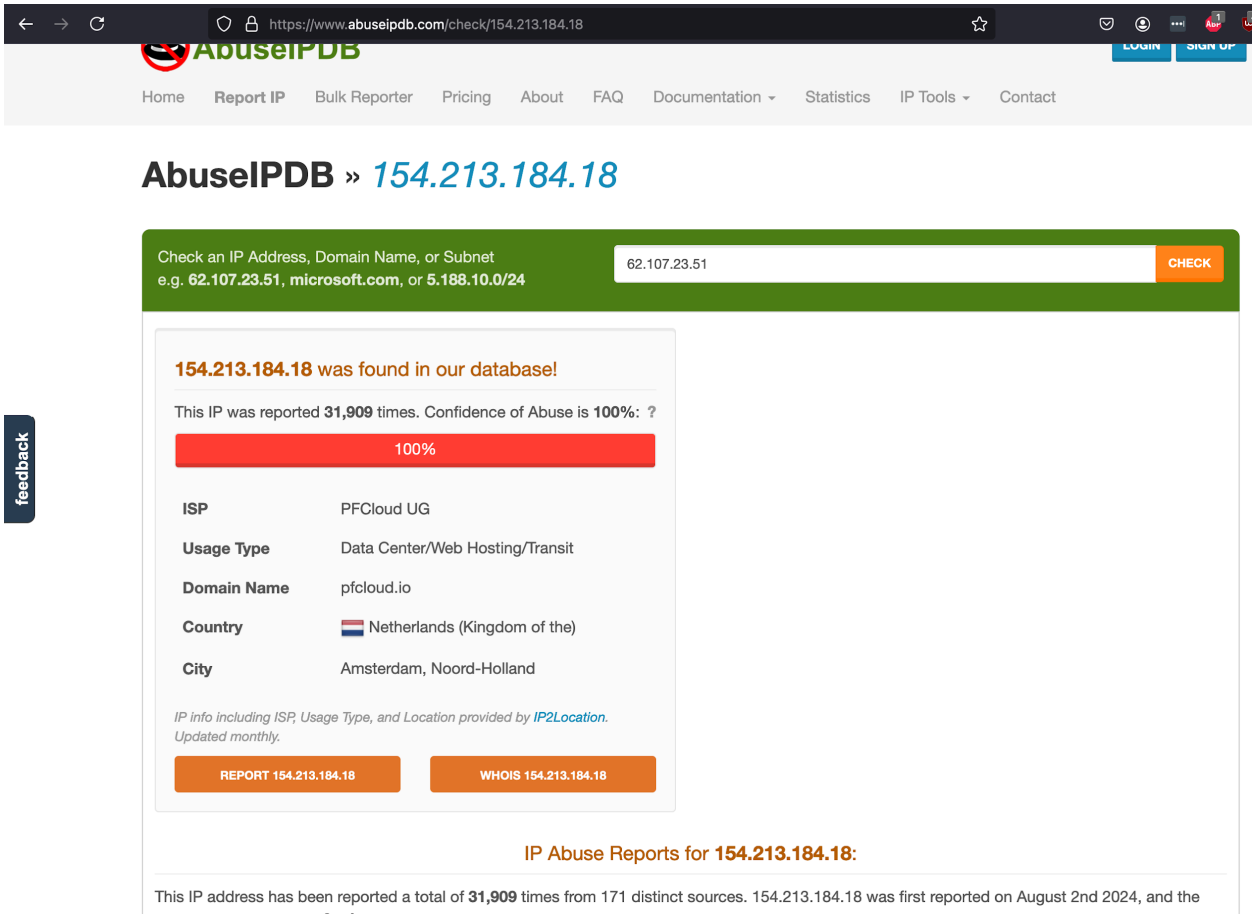


2) ***154[.]213[.]184[.]18*** *- malicious PFCloud UG, Data Center/Web Hosting/Transit possibly involved in a botnet?*



VirusTotal Community Score = 13/96

Abuseipdb score = Confidence of Abuse is 100% (This IP was reported 31,909 times)

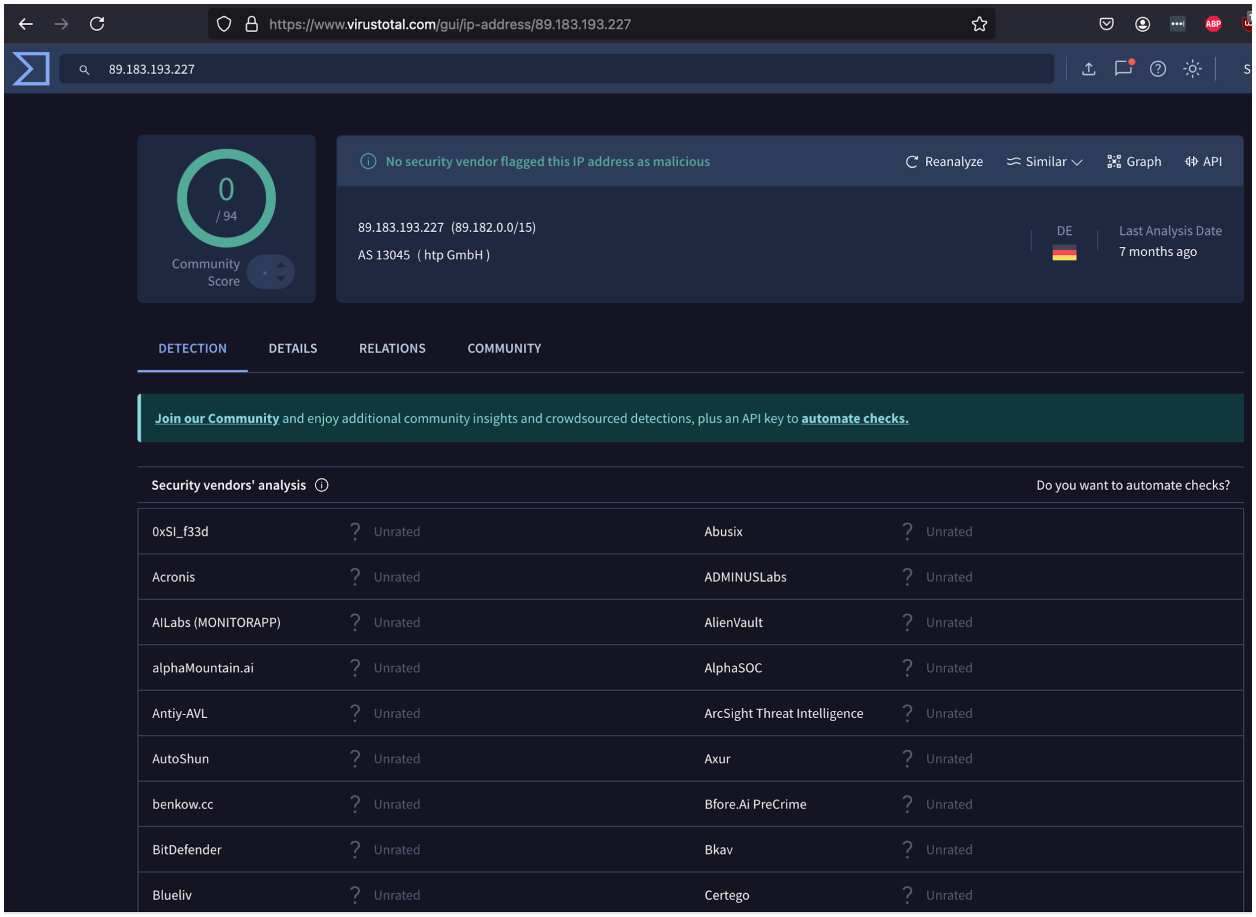


GreyNoise = “GreyNoisehas identified malicious activity from this IP. It is still considered internet background noise since it is scanning the entire internet and NOT targeting you specifically.”

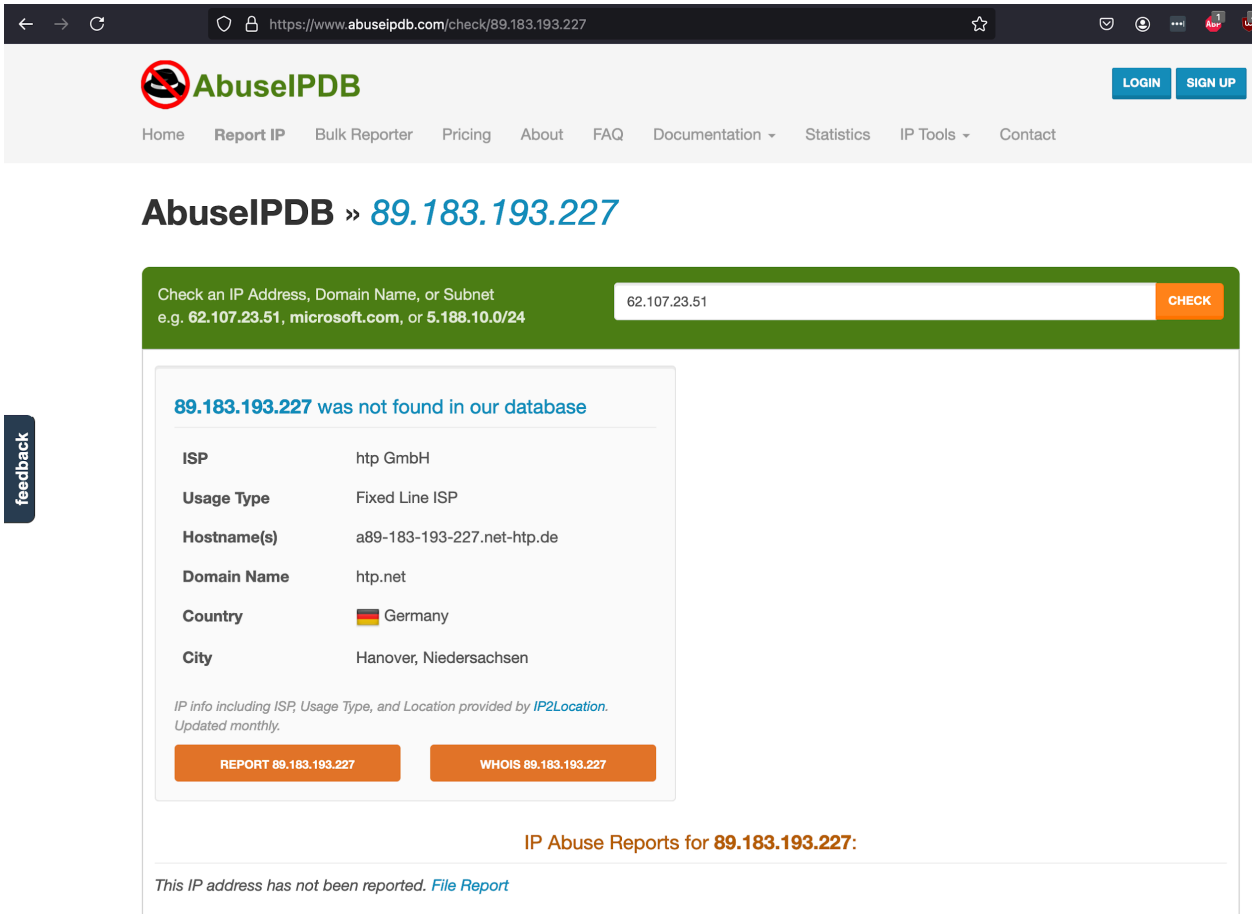
Find imagine

1) ***89[.]183[.]193[.]227*** *- no threat detected, “RIPE NCC,” registry of IPs*

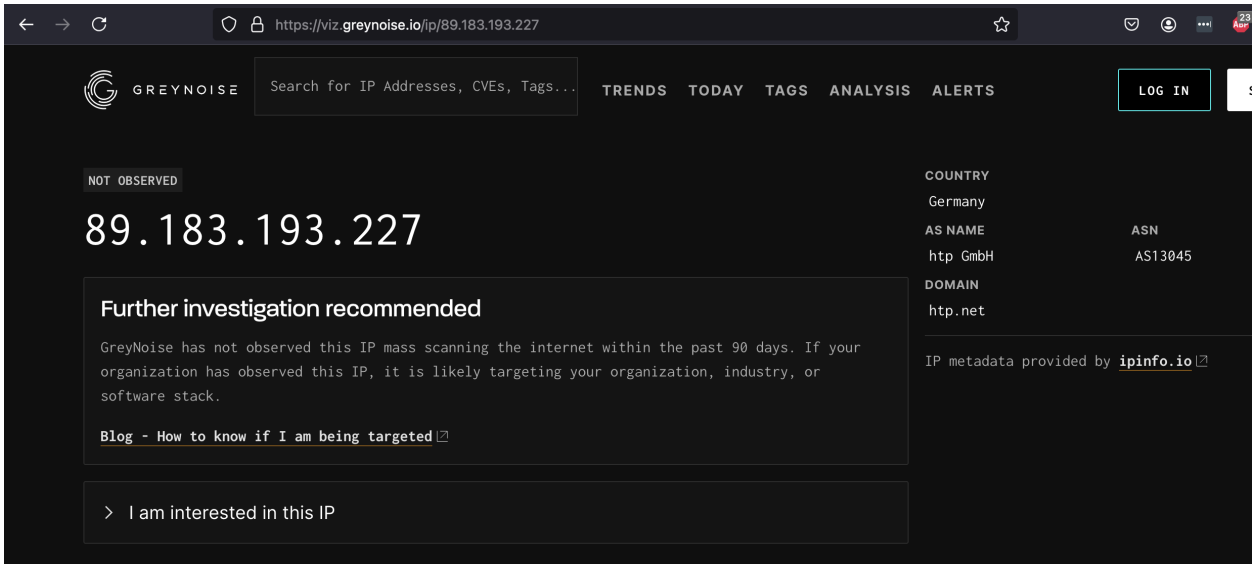
   VirusTotal Community Score = 0/96, no security vender flagged this IP address



Abuseipdb score = 89.183.193.227 was not found in our database



GreyNoise = “GreyNoise has not observed this IP mass scanning the internet within the past 90 days. If your organization has observed this IP, it is likely targeting your organization, industry, or software stack.”



Conclusion

The honeypot experiment demonstrated how threat actors continuously scan the internet for exposed ports and vulnerable systems. The three ports monitored - 3389 (RDP), 34567 (video surveillance), and 8000 (web servers) - are commonly targeted, as they can enable remote access, monitoring, and web-based control of systems.

While these ports serve distinct purposes, they often coexist in network environments and can indirectly interact, for example, in scenarios involving remote administration, surveillance, and web-based services.

The honeypot results, analyzed in Splunk, showed a significant number of connection attempts from various IP addresses, primarily from malicious actors. Further investigation using open-source intelligence tools revealed that the top three most aggressive IP addresses had a history of malicious activity, with high abuse scores and community-reported threats.

This experiment highlights the importance of robust cybersecurity measures, such as carefully managing exposed ports, implementing strong access controls, and continuously monitoring network activity for suspicious behavior. Organizations should stay vigilant and leverage security tools and threat intelligence to protect their systems from unauthorized access and potential exploitation.