

Honeybot in Linus & Splunk + OSINT Analysis

Threat actors continuously scour the internet for open ports and vulnerable applications. To demonstrate this, I created my own Honeybot using OpenAI/ChatGPT. The honeybot 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:

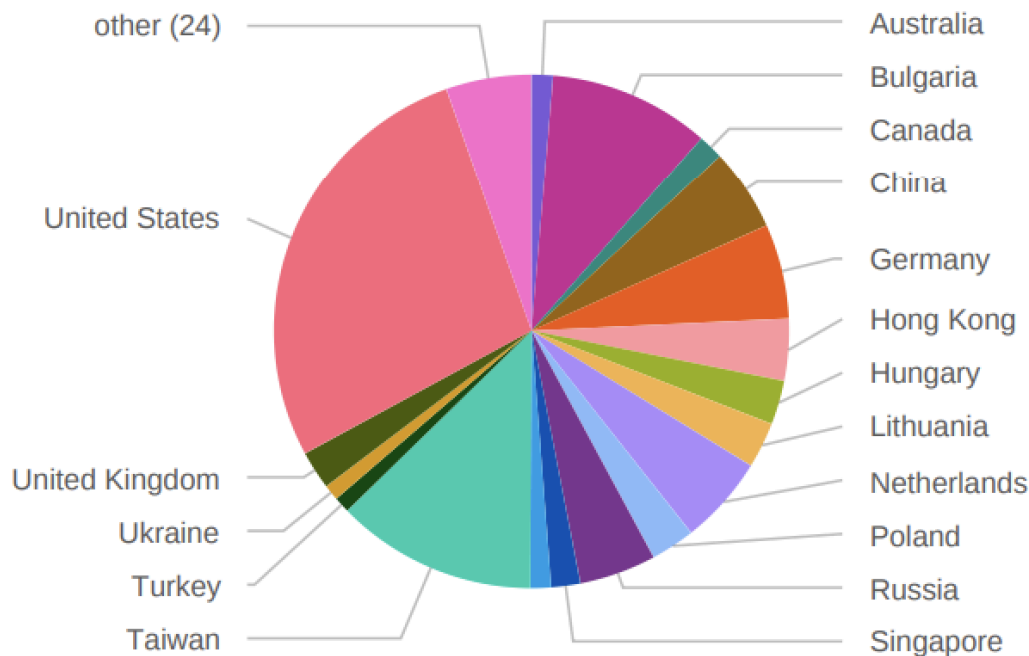
- Port 34567: IP cameras typically use this port for streaming video.
- Port 8000: A web server could be configured to provide a user interface for accessing and controlling these cameras. This interface might be accessible via a web browser, using port 8000.

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.

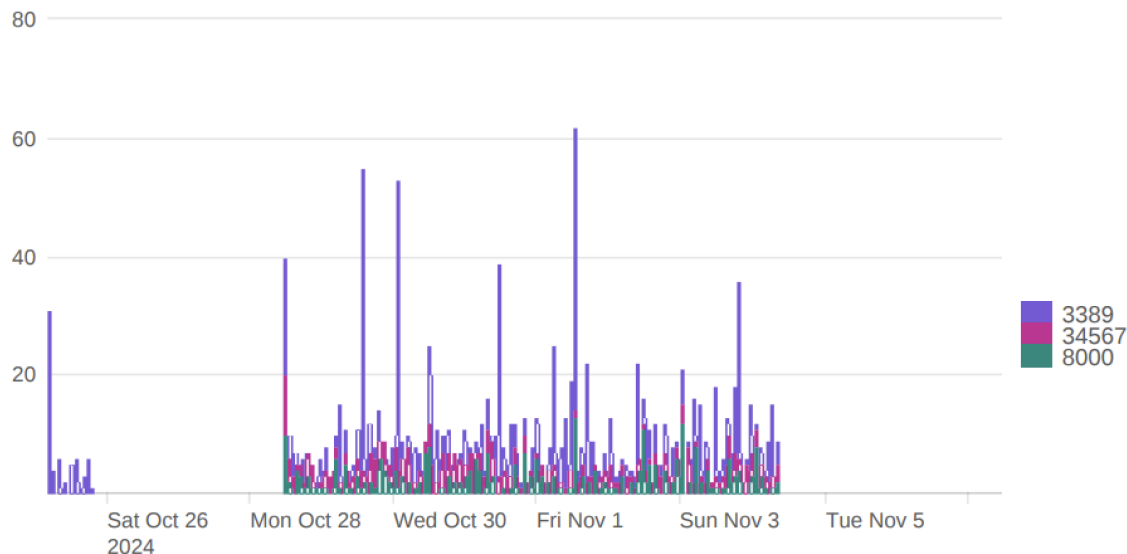
Honeypot Results & Analysis

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

The screenshot shows the VirusTotal interface for the IP address 87.120.166.245. The top section displays a 'Community Score' of 9/96, indicating a malicious status. Below this, a table titled 'Security vendors' analysis' lists 16 different security vendors and their respective classifications for the IP. The vendors are arranged in two columns. The first column includes Antiy-AVL, Criminal IP, CyRadar, Lionix, SOCRadar, AlphaSOC, Abusix, ADMINUSLabs, and AlienVault. The second column includes CRDF, Cyble, Fortinet, MalwareURL, alphaMountain.ai, Gridinsoft, Acronis, AILabs (MONITORAPP), and Artists Against 419. The classifications range from 'Malicious' to 'Clean'.

Security vendors' analysis		Do you want to automate checks?	
Antiy-AVL	Malicious	CRDF	Malicious
Criminal IP	Malicious	Cyble	Malicious
CyRadar	Malicious	Fortinet	Malware
Lionix	Malicious	MalwareURL	Malware
SOCRadar	Malware	alphaMountain.ai	Suspicious
AlphaSOC	Suspicious	Gridinsoft	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	Artists Against 419	Clean

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

https://www.abuseipdb.com/check/87.120.166.245

HomeReport IPBulk ReporterPricingAboutFAQDocumentationStatisticsIP ToolsContact

AbuseIPDB » 87.120.166.245

Check an IP Address, Domain Name, or Subnet
e.g. 62.107.23.51, microsoft.com, or 5.188.10.0/24

62.107.23.51

CHECK

87.120.166.245 was found in our database!

This IP was reported **3,317** times. Confidence of Abuse is **100%**: ?

100%

ISP410 Teapot Limited

Usage TypeData Center/Web Hosting/Transit

Domain Namejihun.me

CountryAntarctica

CityMcMurdo Station, Antarctica

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

REPORT 87.120.166.245

WHOIS 87.120.166.245

IP Abuse Reports for 87.120.166.245:

This IP address has been reported a total of **3,317** times from 93 distinct sources. 87.120.166.245 was first reported on October 21st 2024, and the most recent report was **3 hours ago**.

[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.”

GREYNOISE

Search for IP Addresses, CVEs, Tags...

TRENDS TODAY TAGS ANALYSIS ALERTS

LOG IN

SIGN UP

> UNKNOWNHOSTING

87.120.166.245

ORGANIZATION410 Teapot Limited

ACTORunknown

Not Spoofable [?]

Observed Activity

Shows the ports & protocols that this IP scanned, along with the paths that this IP requested. In addition, fingerprints of the SSH & TLS negotiation between this IP and the GreyNoise sensor are shown.

View Similar IPs →

FIRST SEEN2024-10-21

LAST SEEN2024-11-07

COUNTRYGermany

REGIONNorth Rhine-Westphalia

CITYAachen

ASNAS215127

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

13/94 Community Score

13/94 security vendors flagged this IP address as malicious

154.213.184.18 (154.213.184.0/21)
AS 51396 (Pfccloud UG)

Reanalyze Similar Graph API

154.213.184.18 (154.213.184.0/21)
AS 51396 (Pfccloud UG)

NL Last Analysis Date 11 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

alphaMountain.ai	Malicious	Antiy-AVL	Malicious
BitDefender	Phishing	Criminal IP	Malicious
Cyble	Malicious	CyRadar	Malicious
Forcepoint ThreatSeeker	Malicious	Fortinet	Malware
G-Data	Phishing	Lionic	Malicious
MalwareURL	Malware	SOCradar	Malware
VIPRE	Malware	ArcSight Threat Intelligence	Suspicious
Gridinsoft	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

VirusTotal Community Score = 13/96

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

AbuseIPDB » 154.213.184.18


Check an IP Address, Domain Name, or Subnet
e.g. 62.107.23.51, microsoft.com, or 5.188.10.0/24

62.107.23.51 CHECK

154.213.184.18 was found in our database!

This IP was reported **31,909** times. Confidence of Abuse is **100%**: ?

100%

ISP	PfCloud UG
Usage Type	Data Center/Web Hosting/Transit
Domain Name	pfcloud.io
Country	 Netherlands (Kingdom of the)
City	Amsterdam, Noord-Holland

IP Info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

REPORT 154.213.184.18 WHOIS 154.213.184.18

IP Abuse Reports for 154.213.184.18:

This IP address has been reported a total of **31,909** times from 171 distinct sources. 154.213.184.18 was first reported on August 2nd 2024, and the

[GreyNoise](#) = “GreyNoise has 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 vendor flagged this IP address

← → ↻ https://www.virustotal.com/gui/ip-address/89.183.193.227 ☆

89.183.193.227

Community Score

No security vendor flagged this IP address as malicious

Reanalyze Similar Graph API

89.183.193.227 (89.182.0.0/15)

AS 13045 (htp GmbH)

DE Last Analysis Date 7 months ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ Do you want to automate checks?

0xSI_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AILabs (MONITORAPP)	? Unrated	AlienVault	? Unrated
alphaMountain.ai	? Unrated	AlphaSOC	? Unrated
Antiy-AVL	? Unrated	ArcSight Threat Intelligence	? Unrated
AutoShun	? Unrated	Axur	? Unrated
benkow.cc	? Unrated	Bfore.Ai PreCrime	? Unrated
BitDefender	? Unrated	Bkav	? Unrated
Blueliv	? Unrated	Certego	? Unrated

Abuseipdb score = 89.183.193.227 was not found in our database

AbuseIPDB » 89.183.193.227

Check an IP Address, Domain Name, or Subnet
e.g. 62.107.23.51, microsoft.com, or 5.188.10.0/24

62.107.23.51 CHECK

89.183.193.227 was not found in our database

ISP	htp GmbH
Usage Type	Fixed Line ISP
Hostname(s)	a89-183-193-227.net-htp.de
Domain Name	htp.net
Country	Germany
City	Hanover, Niedersachsen

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

REPORT 89.183.193.227 WHOIS 89.183.193.227

IP Abuse Reports for 89.183.193.227:

This IP address has not been reported. [File Report](#)

feedback

[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.”

GREYNOISE Search for IP Addresses, CVEs, Tags... TRENDS TODAY TAGS ANALYSIS ALERTS LOG IN

NOT OBSERVED

89.183.193.227

Further investigation recommended

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.

[Blog - How to know if I am being targeted](#)

> I am interested in this IP

COUNTRY	Germany
AS NAME	htp GmbH
ASN	AS13045
DOMAIN	htp.net

IP metadata provided by [ipinfo.io](#)

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.