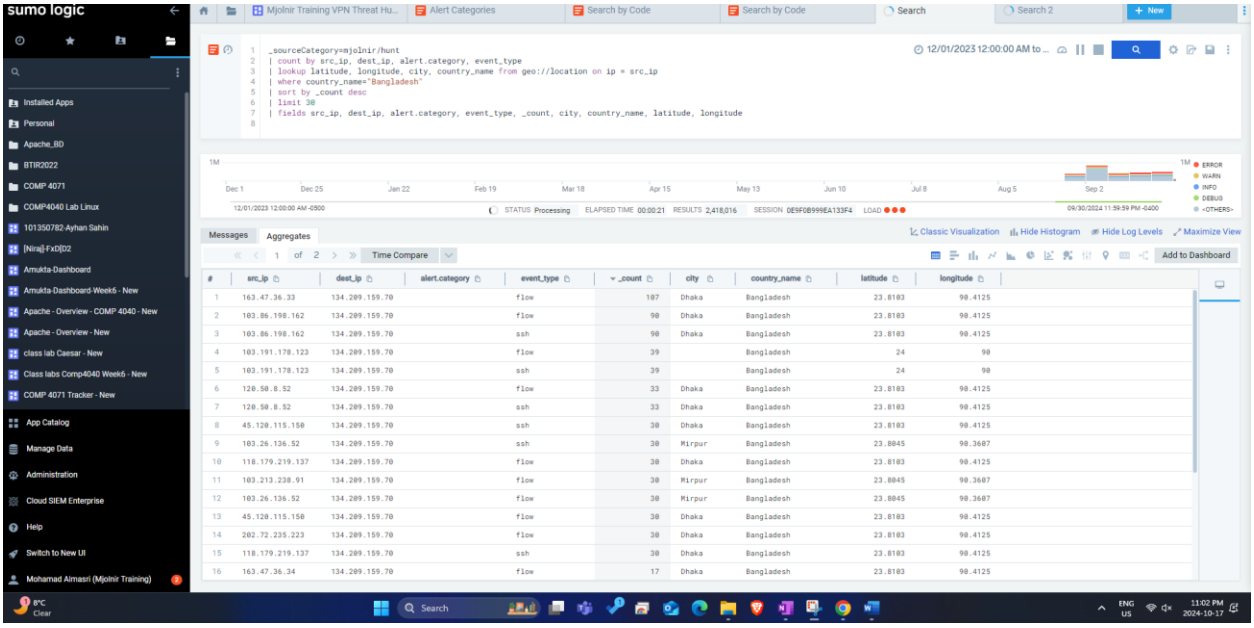
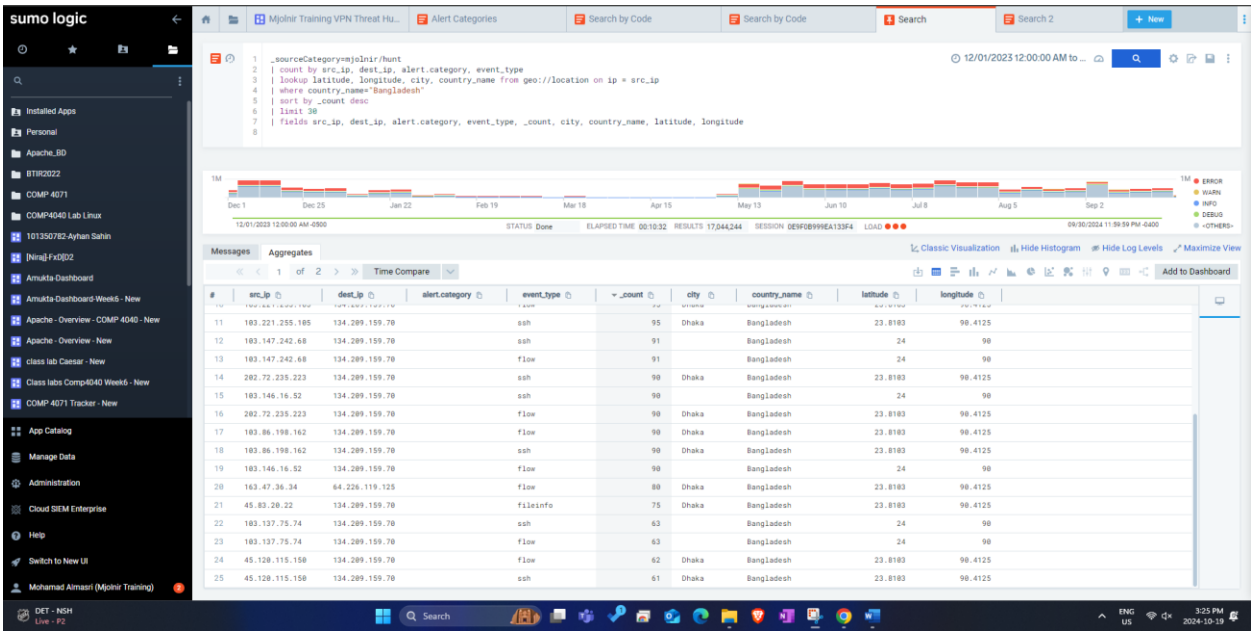
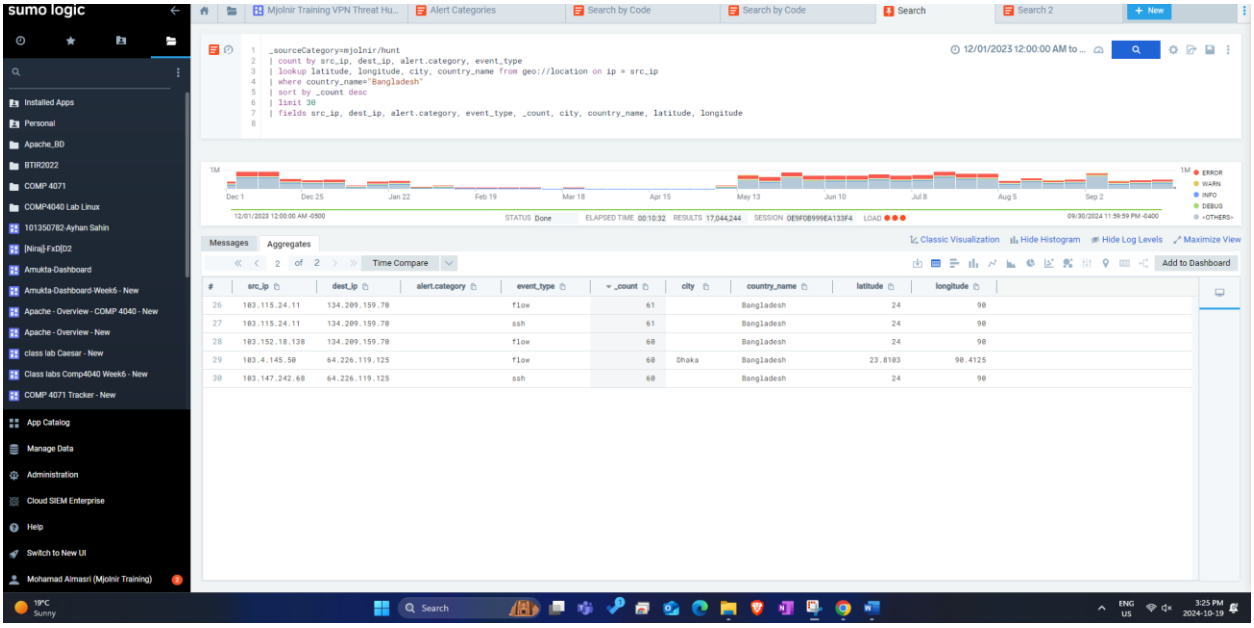
MOHAMAD ALMASRI **ID: 101167438**

DIGITAL FORENSICS&INCID. RESP - COMP 4071

Assignment 1







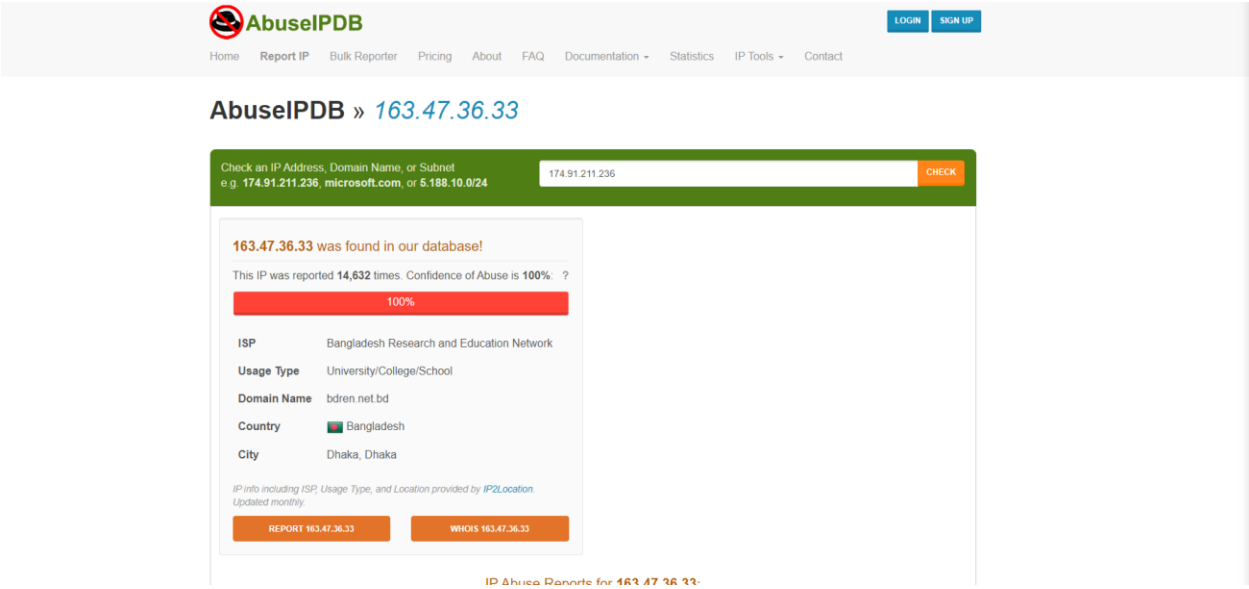
Event 1,2

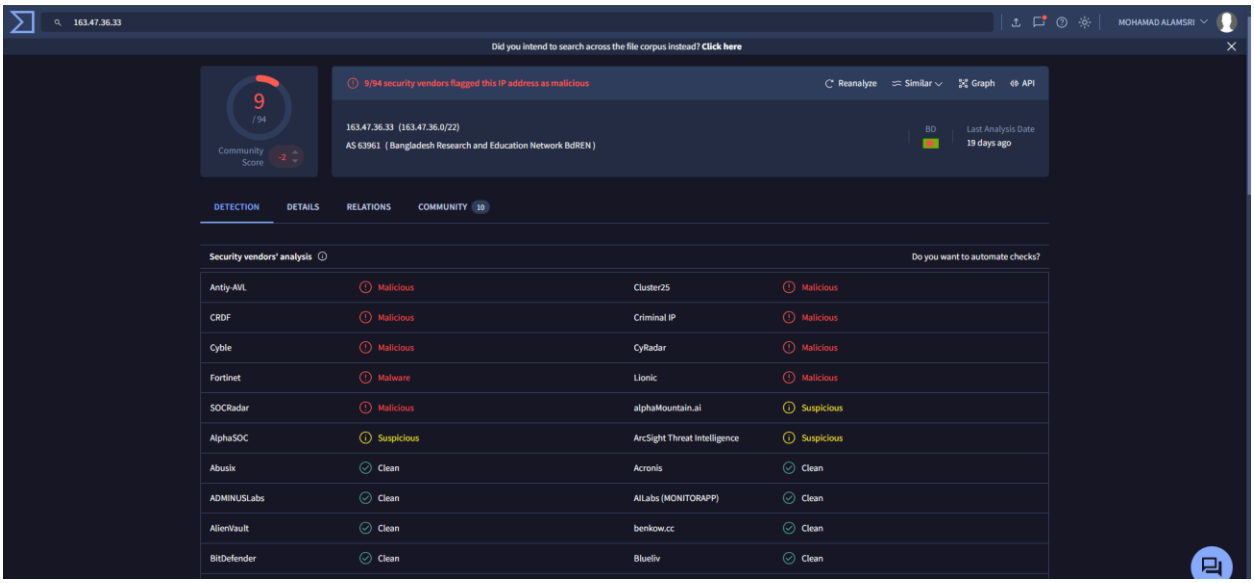
1. what is the source of the attack?

1	163.47.36.33	134.209.159.70	flow	513	Dhaka	Bangladesh	23.8103	90.4125

1	163.47.36.33	134.209.159.70	flow	513	Dhaka	Bangladesh	23.8103	90.4125
2	163.47.36.33	64.226.119.125	flow	317	Dhaka	Bangladesh	23.8103	90.4125

The source IP of the attack is 163.47.36.33, which is located in Dhaka, Bangladesh, as shown by the geolocation lookup.



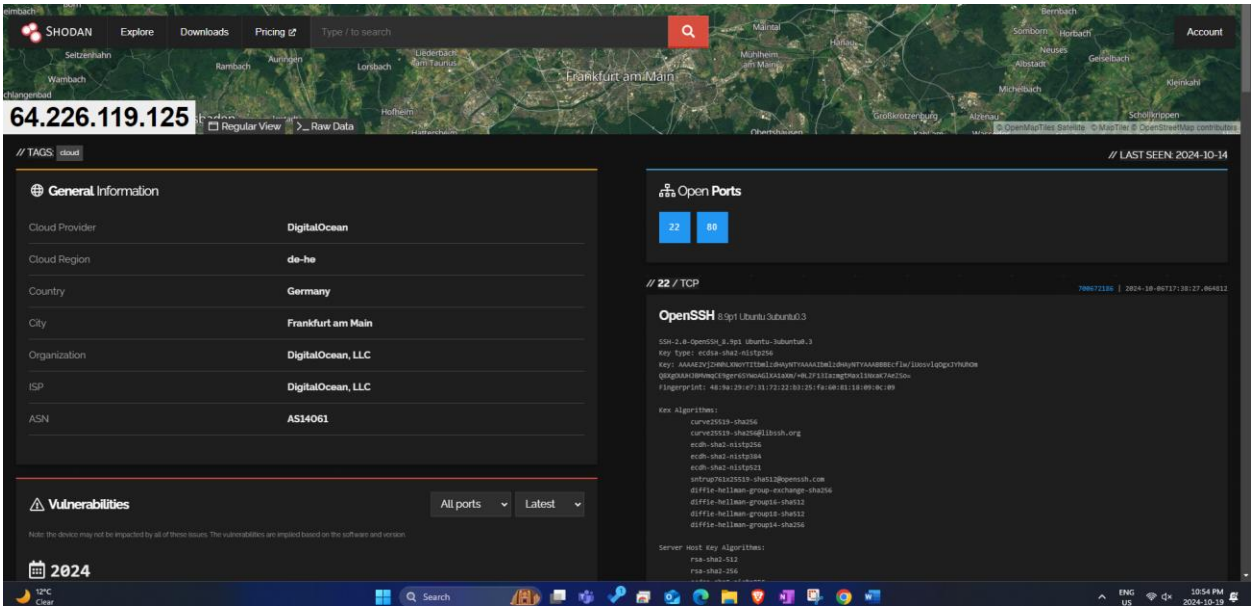


2. what are they attacking?

The destination IP in the logs is 134.209.159.70

The destination IP in the logs is 64.226.119.125

3. Why is the target being attacked?



The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

The target IP 64.226.119.125 is hosted on DigitalOcean in Germany and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

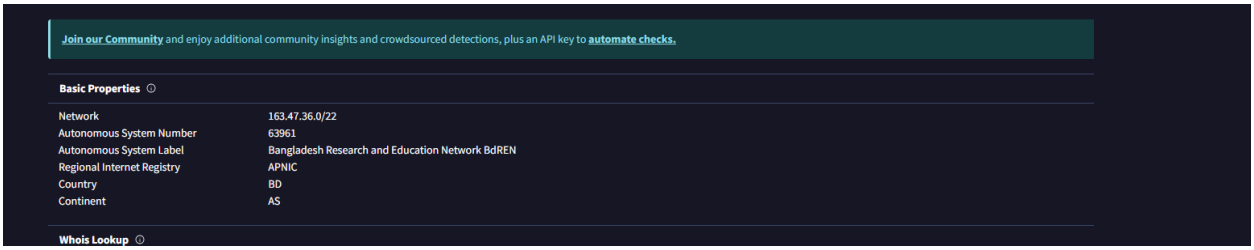
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.
2. HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.

   Attackers are likely scanning and probing these common services to gain unauthorized access or exploit weaknesses in the system.

4. What can you identify about the infrastructure used to attack, who does it belong to?

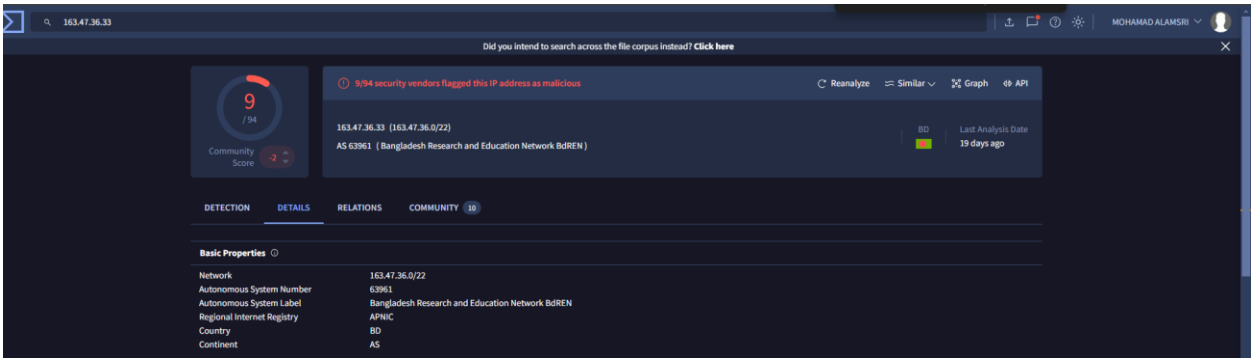
The infrastructure used is part of the Bangladesh Research and Education Network (BdREN)

The IP is flagged by 9 out of 94 security vendors as malicious, indicating that this IP has a history of malicious activity



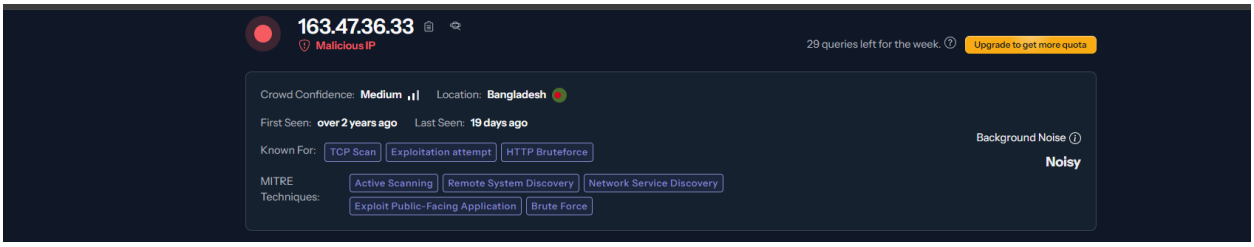
5. What is the event type?

the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses. The flow indicates continuous traffic between the attacker and the target, potentially part of a scanning or exploitation attempt.



#	src_ip	dest_ip	alert.category	event_type	_count	city	country_name	latitude	longitude
1	163.47.36.33	134.209.159.70		flow	513	Dhaka	Bangladesh	23.8103	90.4125

6. What TTPs do you observe?



Active Scan (MITER ATT&CK T1595): Source IP and open port services join to scan and detect networks. This is usually the reconnaissance phase of the attack. Public Application Exploitation (MITER ATT&CK T1190): This may be an attempt to exploit a vulnerability in a public service on the destination IP, based on the fact that the IP repeatedly attempts to connect. Connected to an abnormal port... Brute Force (MITER ATT&CK T1110): The attacker attempts to use brute force or

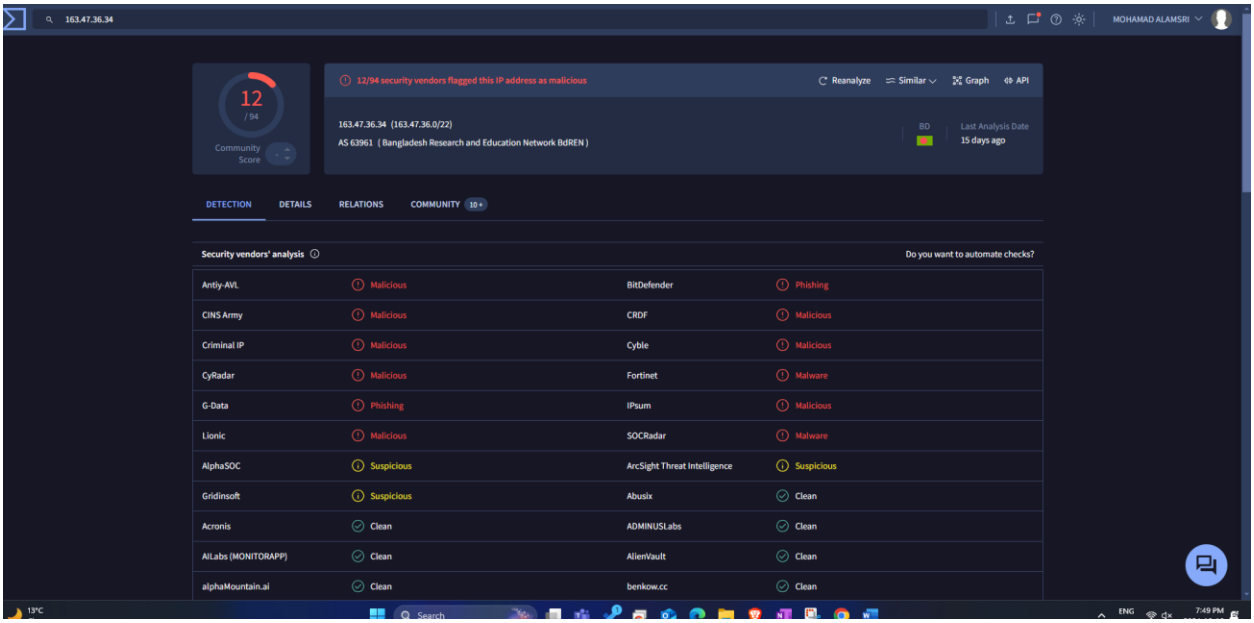
other forms of force. of authentication This depends on the nature of the malicious activity being flagged. (As seen in the analysis report)

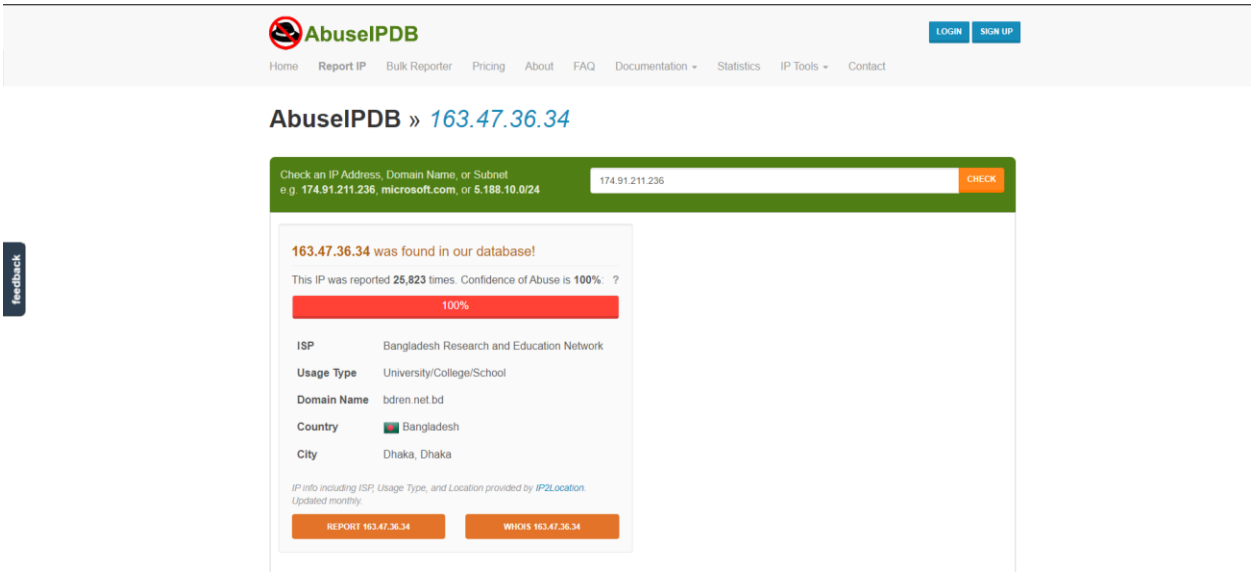
Event 3,20

1. what is the source of the attack?

20	163.47.36.34	64.226.119.125	flow	80	Dhaka	Bangladesh	23.8103	90.4125
2	163.47.36.33	64.226.119.125	flow	317	Dhaka	Bangladesh	23.8103	90.4125

163.47.36.34





2. what are they attacking?

The destination IP in the logs is 134.209.159.70

3	163.47.36.34	134.209.159.70	flow	237	Dhaka	Bangladesh	23.8103	90.4125

3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

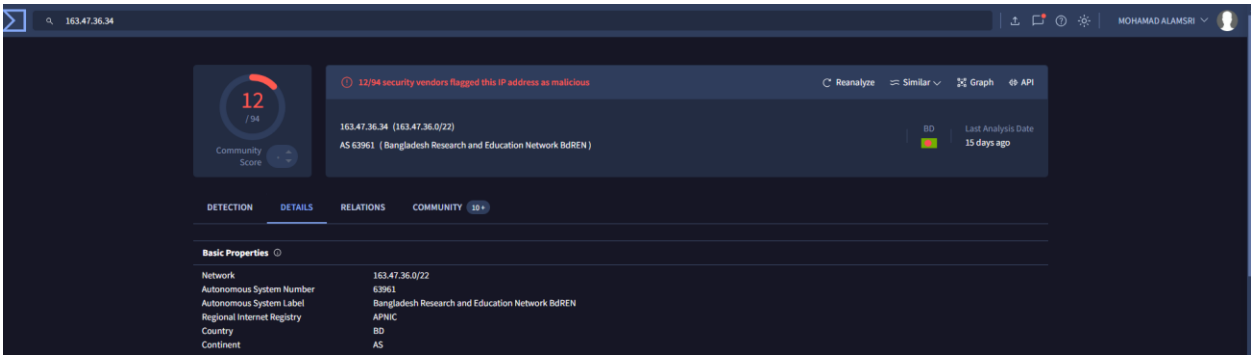
being attacked because:

1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.
2. HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.

Attackers are likely scanning and probing these common services to gain unauthorized access or exploit weaknesses in the system.

4. What can you identify about the infrastructure used to attack, who does it belong to?

- The infrastructure used is part of the Bangladesh Research and Education Network (BdREN)
- The IP is flagged by 12 out of 94 security vendors as malicious, indicating that this IP has a history of malicious activity



5. What is the event type?

The event type is flow. This means monitoring network traffic. In this case, it follows the flow of packets between the source and destination IP addresses.

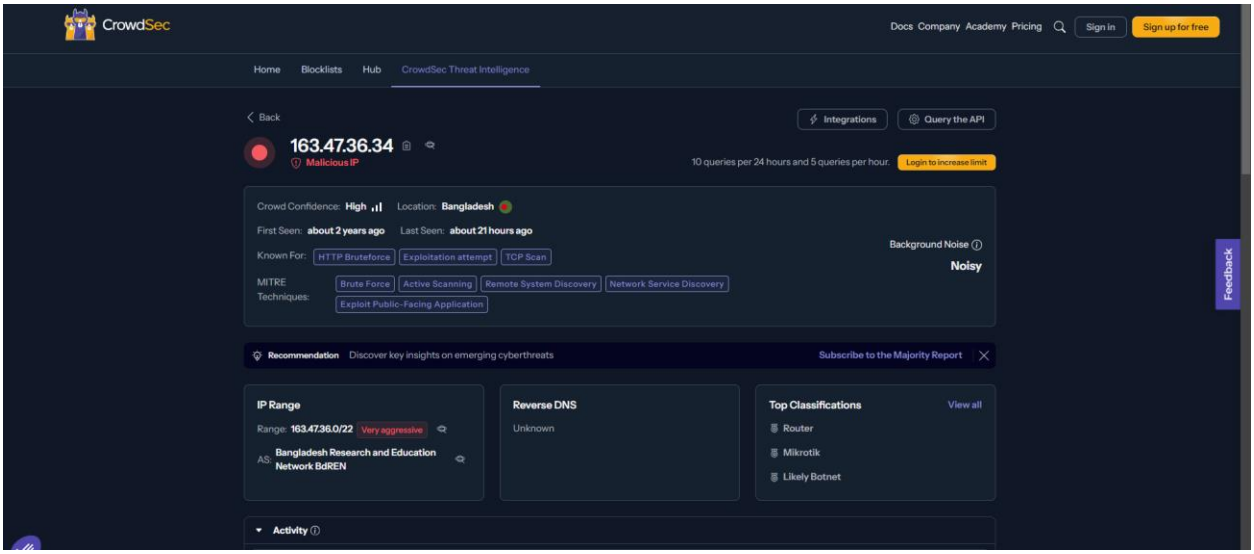
3	163.47.36.34	134.209.159.70	flow	237	Dhaka	Bangladesh	23.8103	90.4125

6. What TTPs do you observe?

The IP 163.47.36.34 is flagged as malicious and exhibits the following tactics, techniques, and procedures (TTPs):

- Brute Force (MITRE: Brute Force): Repeated attempts to guess credentials.
- Active Scanning (MITRE: Network Service Discovery): Scanning for open services or ports.
- Exploitation (MITRE: Exploit Public-Facing Application): Exploiting vulnerabilities in publicly accessible applications.

These activities indicate potential involvement in HTTP bruteforce, TCP scanning, and exploitation attempts, likely linked to botnet activity.



Event 6,8,28

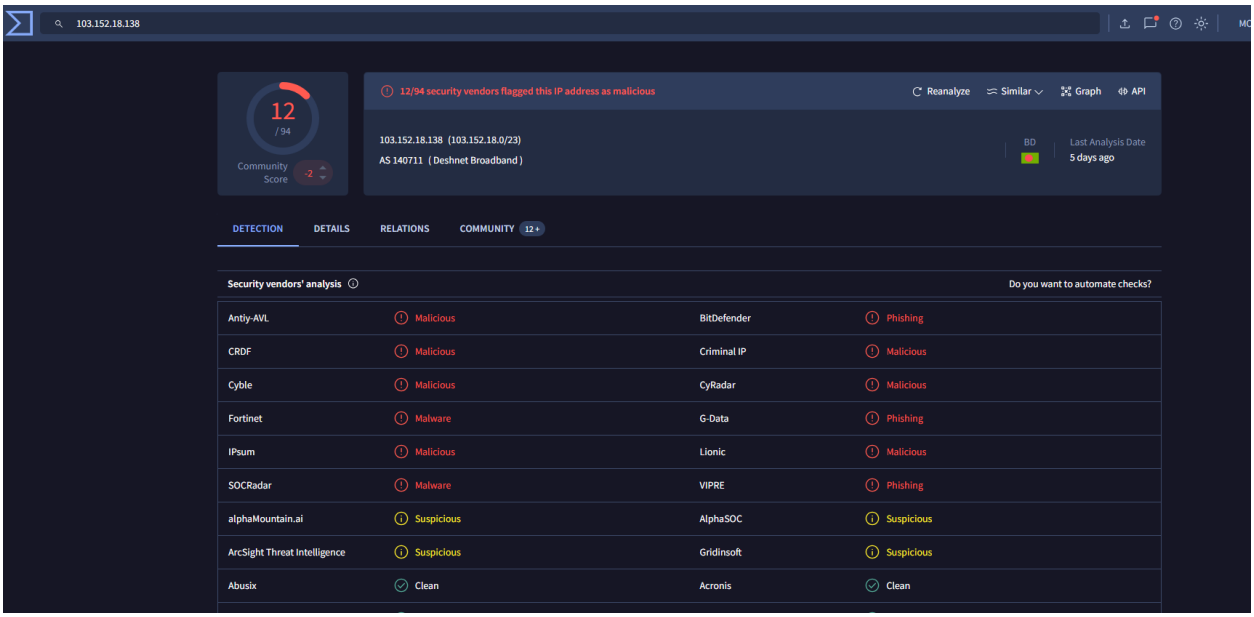
1. what is the source of the attack?

103.152.18.138

6	103.152.18.138	64.226.119.125	flow	120	Bangladesh	24	90

8	103.152.18.138	64.226.119.125	ssh	120	Bangladesh	24	90

28	103.152.18.138	134.209.159.70	flow	60	Bangladesh	24	90

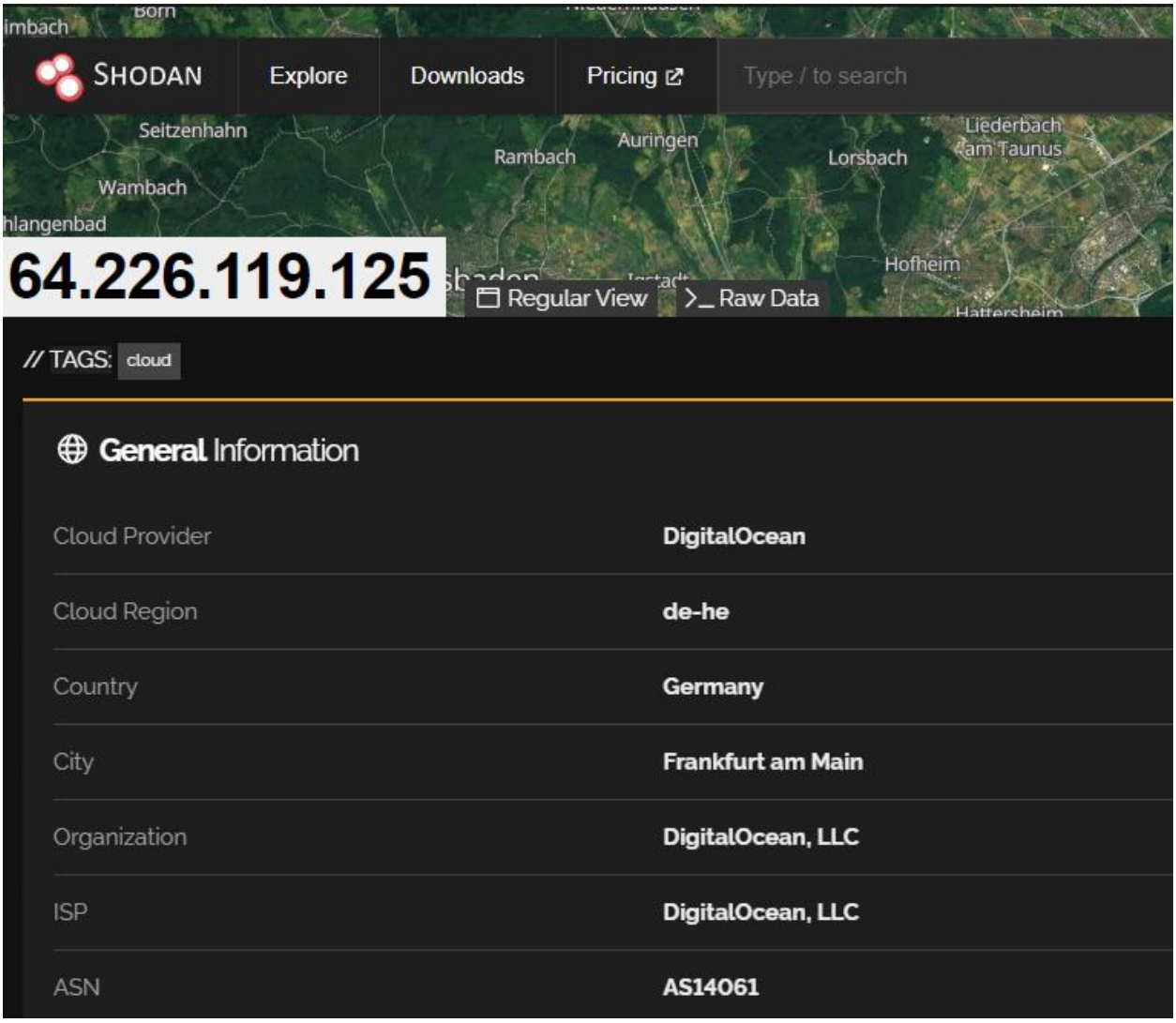


2. what are they attacking?

6	103.152.18.138	64.226.119.125	flow	120	Bangladesh	24	90

The destination IP in the logs is: 64.226.119.125

The destination IP in the logs is: 134.209.159.70



3. Why is the target being attacked?

The target IP 64.226.119.125 is hosted on DigitalOcean in Germany and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

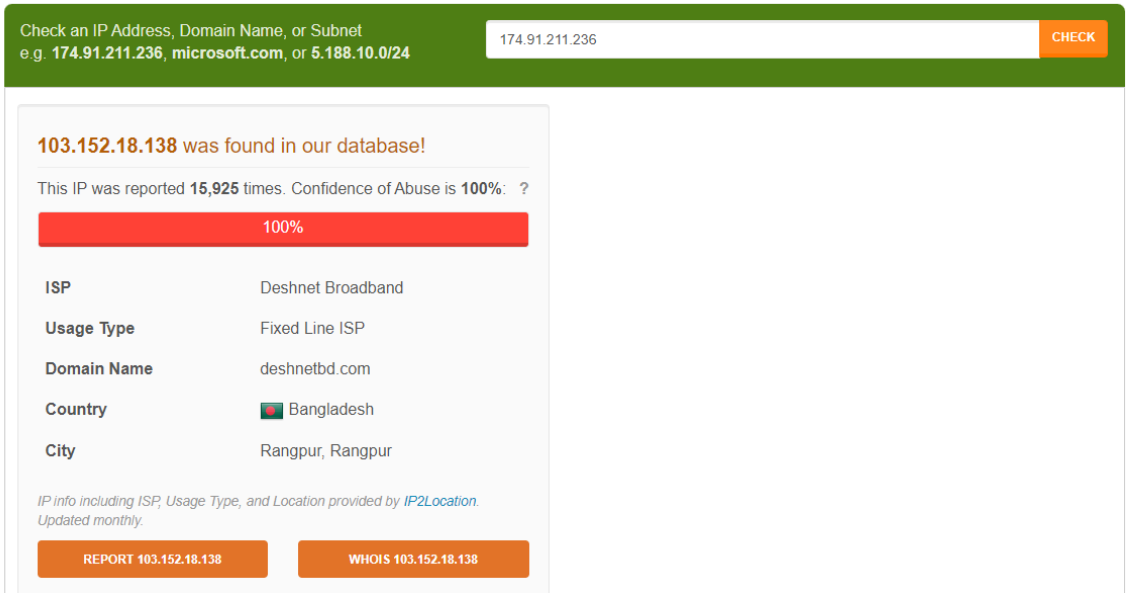
being attacked because:

1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.
2. HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.

Attackers are likely scanning and probing these common services to gain unauthorized access or exploit weaknesses in the system.

4. What can you identify about the infrastructure used to attack, who does it belong to?

AbuseIPDB » *103.152.18.138*



- The infrastructure used is part of the Deshnet Broadband
- The IP is flagged by 12 out of 94 security vendors as malicious, indicating that this IP has a history of malicious activity

5. What is the event type?

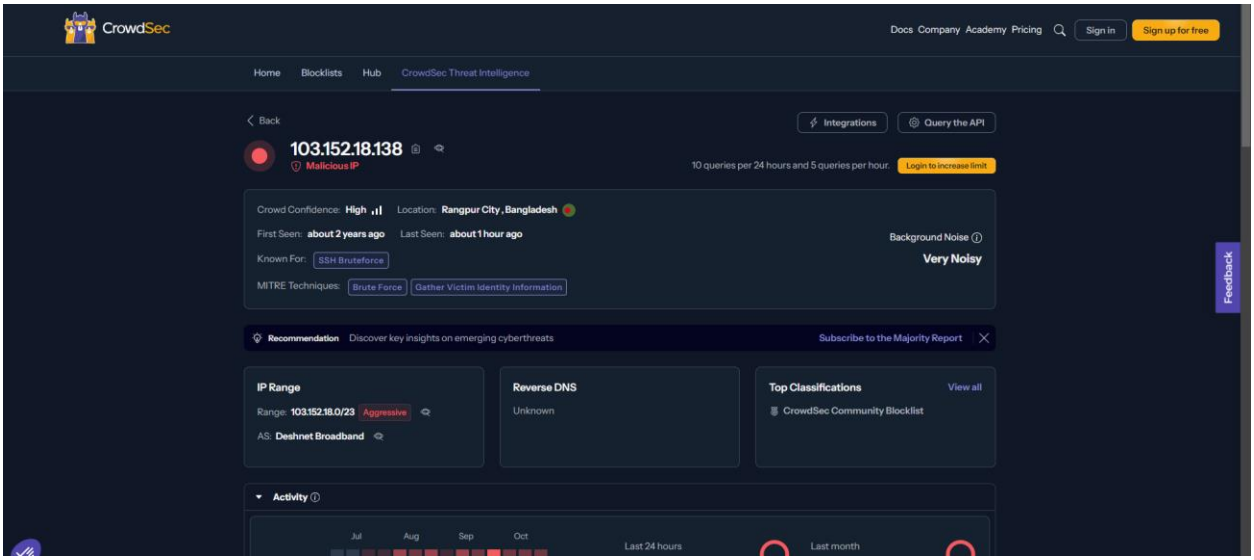
1. The event type is flow. This means monitoring network traffic. In this case, it follows the flow of packets between the source and destination IP addresses..

2. The event type is SSH for the IP 103.152.18.138, it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

6	103.152.18.138	64.226.119.125	flow	120	Bangladesh	24	90

6. What TTPs do you observe?

The IP 103.152.18.138, from Rangpur City, Bangladesh, is known for SSH brute-force attacks. This IP is likely targeting systems with open SSH ports to exploit weak passwords or vulnerabilities, aiming to gain unauthorized access to systems.



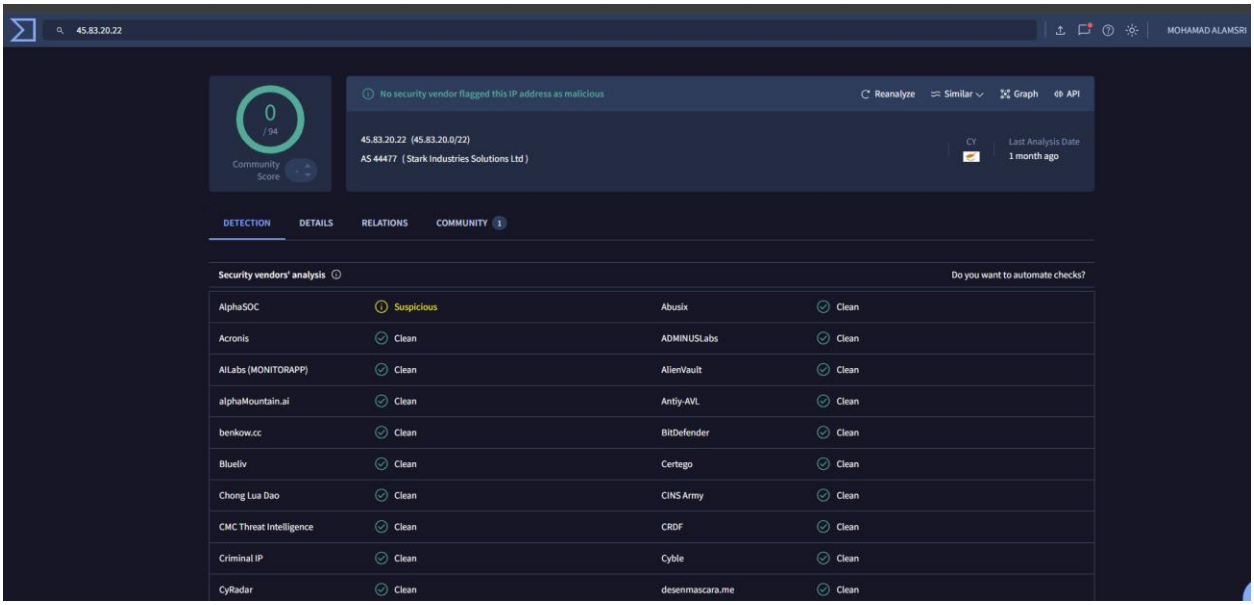
Event 4,5,21:

1. what is the source of the attack?

45.83.20.22

4	45.83.20.22	134.209.159.70	flow	225	Dhaka	Bangladesh	23.8103	90.4125
5	45.83.20.22	134.209.159.70	http	150	Dhaka	Bangladesh	23.8103	90.4125

21	45.83.20.22	134.209.159.70	fileinfo	75	Dhaka	Bangladesh	23.8103	90.4125



2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

5	45.83.20.22	134.209.159.70	http	150	Dhaka	Bangladesh	23.8103	90.4125

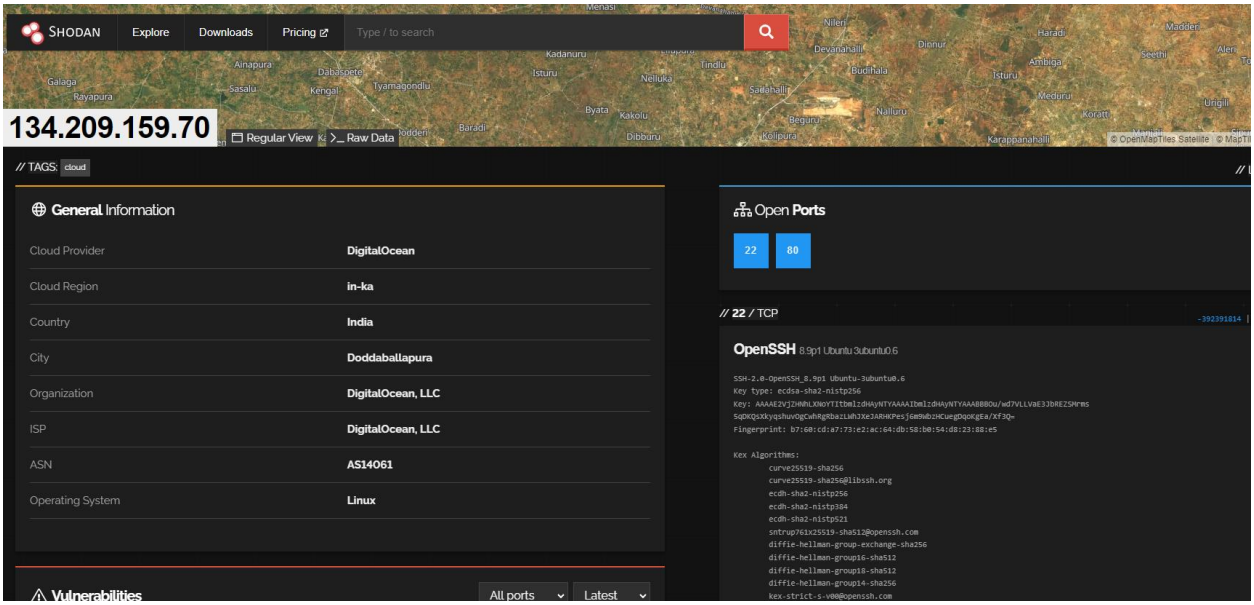
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

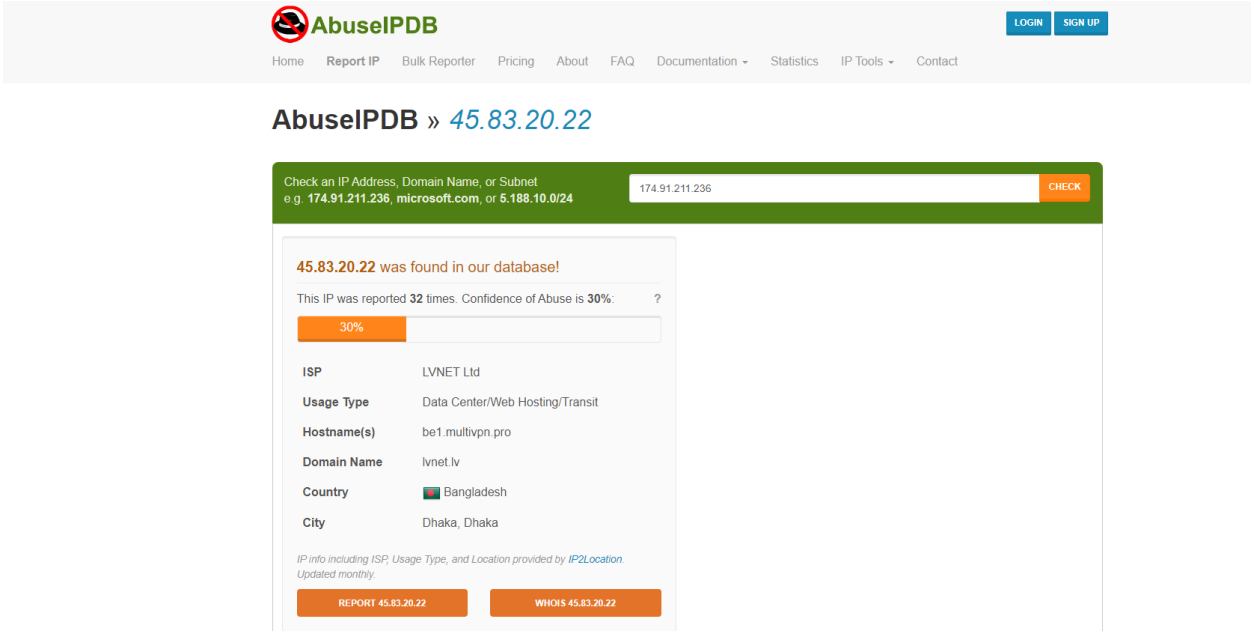
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.
2. HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.

Attackers are likely scanning and probing these common services to gain unauthorized access or exploit weaknesses in the system.



4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 45.83.20.22 belongs to LVNET Ltd, a hosting provider in Dhaka, Bangladesh. It is likely part of a data center or web hosting infrastructure, which could be used for legitimate purposes but is also reported as abusive 32 times, indicating potential misuse for attacks or malicious activities.

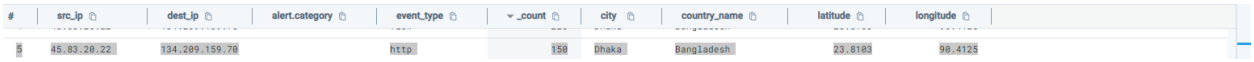


5. What is the event type?

1. The event type is HTTP, indicating that the source IP 45.83.20.22 is making HTTP requests to the target 134.209.159.70,
2. The event type is flow. This means monitoring network traffic. In this case, it follows the flow of packets between the source and destination IP addresses.The event type is fileinfo it would mean the source IP is interacting with files, such as downloading or uploading files to the target. This could indicate:

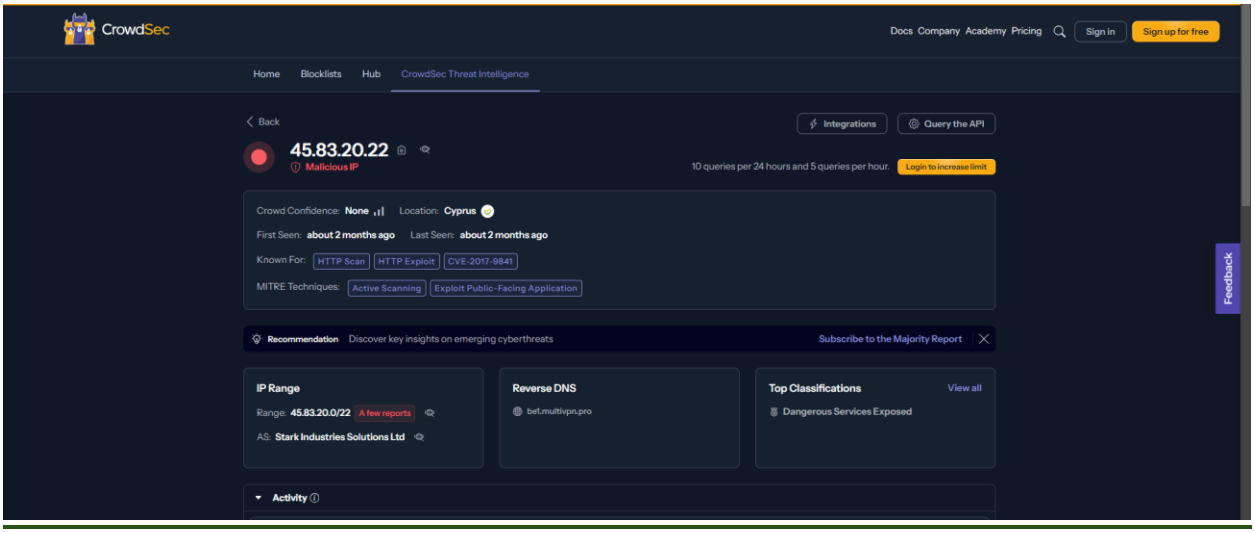
   File transfer activity.

   Potential malware delivery or data exfiltration attempts, depending on the context of the interaction.



#	src_ip	dest_ip	alert.category	event_type	_count	city	country_name	latitude	longitude
5	45.83.20.22	134.209.159.70		http	150	Dhaka	Bangladesh	23.8103	90.4125

6. What TTPs do you observe?



For IP 45.83.20.22, the following tactics, techniques, and procedures (TTPs) are observed:

Active Scanning: Searching for vulnerabilities or open services.

Exploitation (MITRE: Exploit Public-Facing Application): Attempting to exploit vulnerabilities, such as CVE-2017-9841.

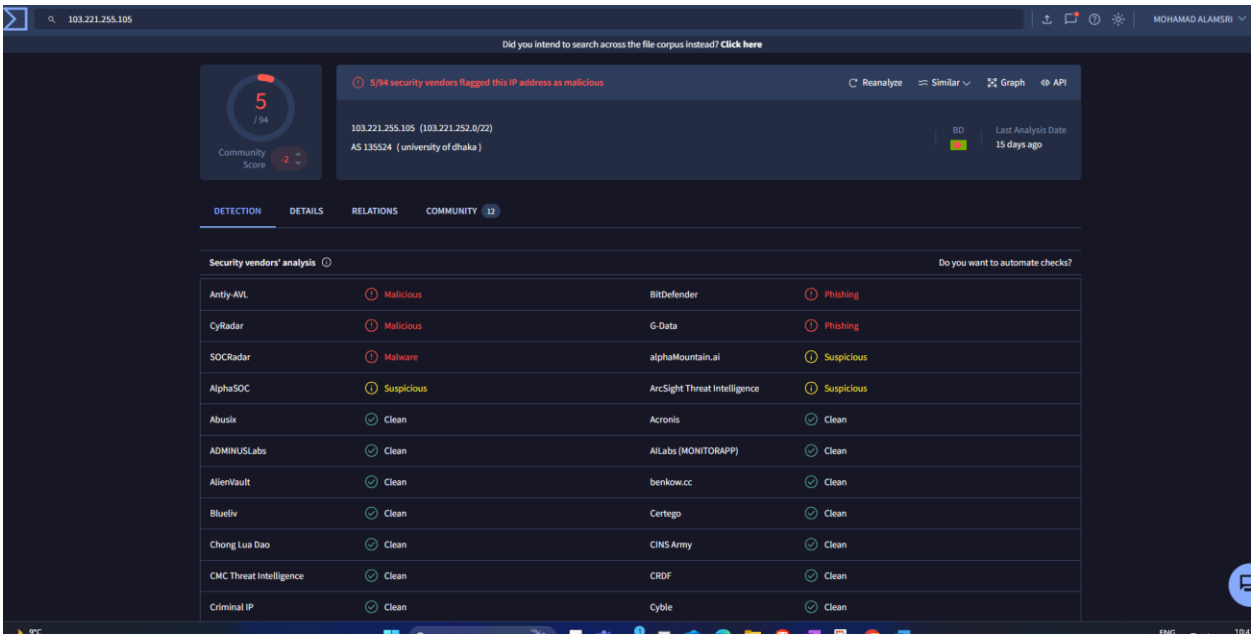
HTTP Exploit: Using HTTP vulnerabilities for attacks.

Event 10,11

1. what is the source of the attack?

103.221.255.105

10	103.221.255.105	134.209.159.70	flow	95	Dhaka	Bangladesh	23.8103	90.4125
11	103.221.255.105	134.209.159.70	ssh	95	Dhaka	Bangladesh	23.8103	90.4125



2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

10	103.221.255.105	134.209.159.70	flow	95	Dhaka	Bangladesh	23.8103	90.4125
11	103.221.255.105	134.209.159.70	ssh	95	Dhaka	Bangladesh	23.8103	90.4125

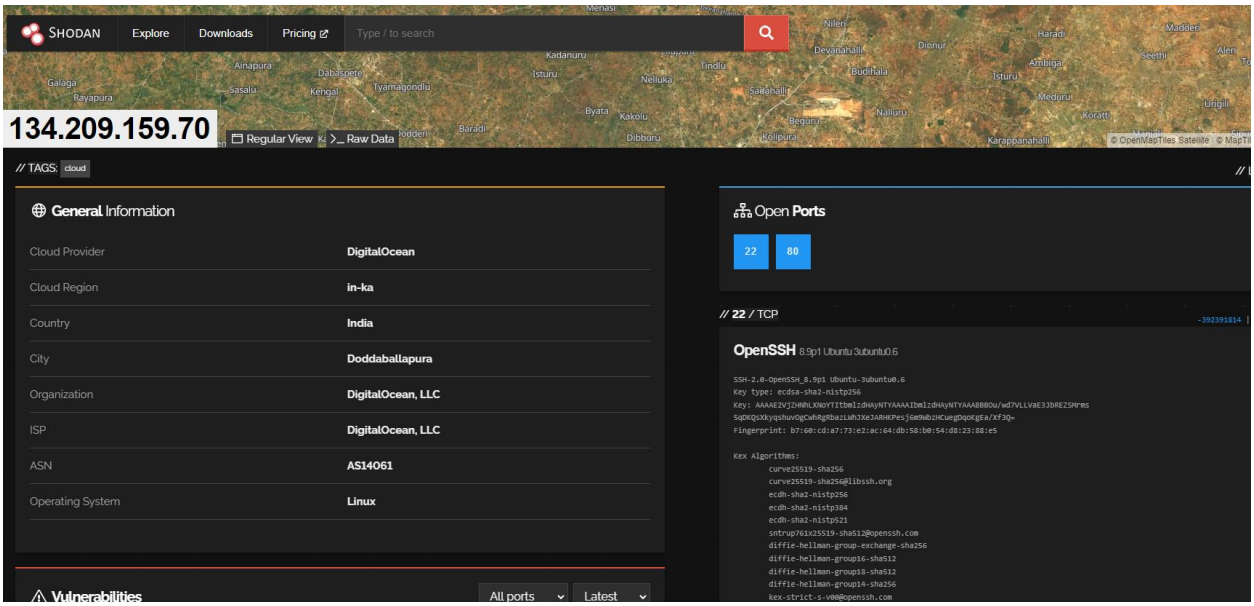
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

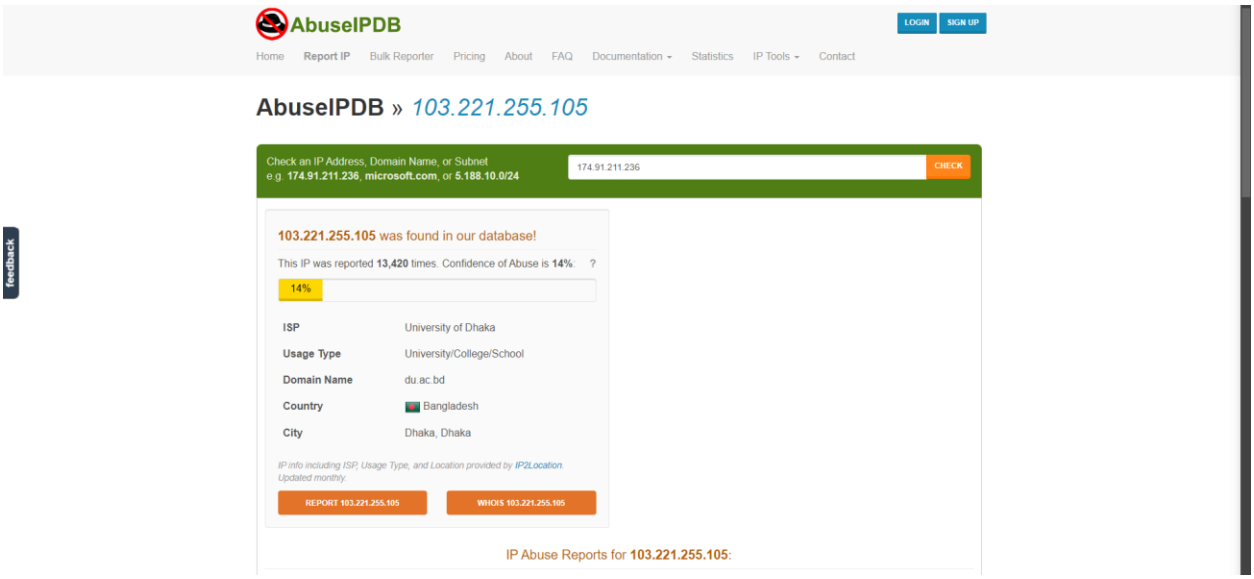
being attacked because:

1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.
2. HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.

Attackers are likely scanning and probing these common services to gain unauthorized access or exploit weaknesses in the system.



4. What can you identify about the infrastructure used to attack, who does it belong to?



The IP 103.221.255.105 belongs to the University of Dhaka in Bangladesh. It is associated with a university network, which may be exploited for malicious activities, as it has been reported over 13,420 times for abuse. The infrastructure likely includes university servers or computers that could be compromised.

5. What is the event type?

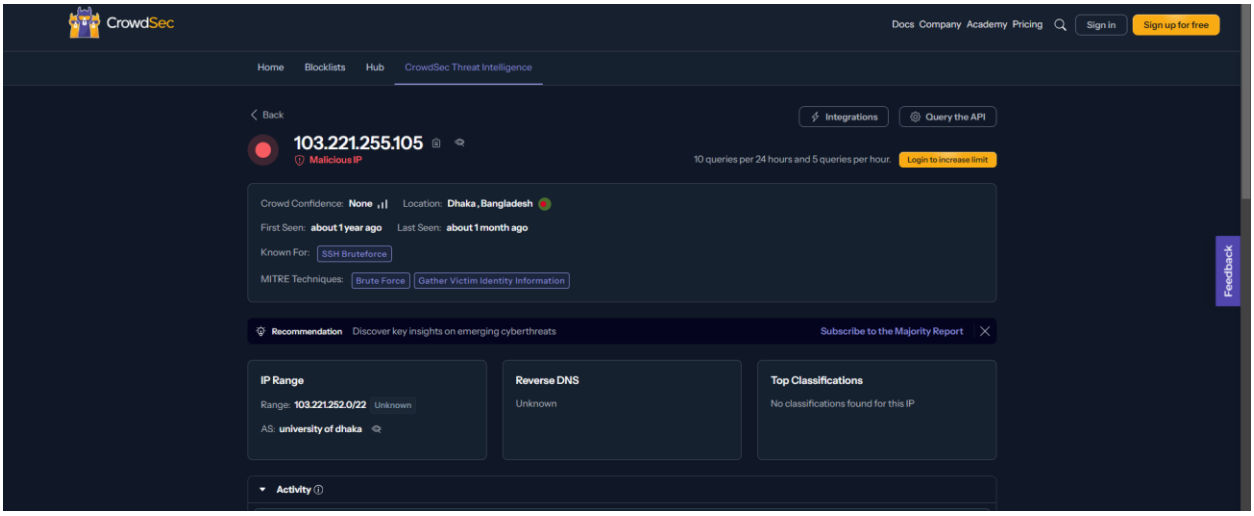
1. The event type is flow. This means monitoring network traffic. In this case, it follows the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 103.221.255.105, it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

9	103.26.136.173	134.209.159.70	ssh	120	Mirpur	Bangladesh	23.8045	90.3607
10	103.221.255.105	134.209.159.70	flow	95	Dhaka	Bangladesh	23.8103	90.4125

6. What TTPs do you observe?

For IP 103.221.255.105, the following tactics, techniques, and procedures (TTPs) are observed:

- Brute Force: SSH bruteforce attempts to gain unauthorized access.
- Gather Victim Identity Information: Likely aiming to collect sensitive data from compromised systems.



Event 7,9

1. what is the source of the attack?

103.26.136.173

7	103.26.136.173	134.209.159.70	flow	120	Mirpur	Bangladesh	23.8045	90.3607
8	103.152.18.138	64.226.119.125	ssh	120		Bangladesh	24	90
9	103.26.136.173	134.209.159.70	ssh	120	Mirpur	Bangladesh	23.8045	90.3607

2. what are they attacking?.

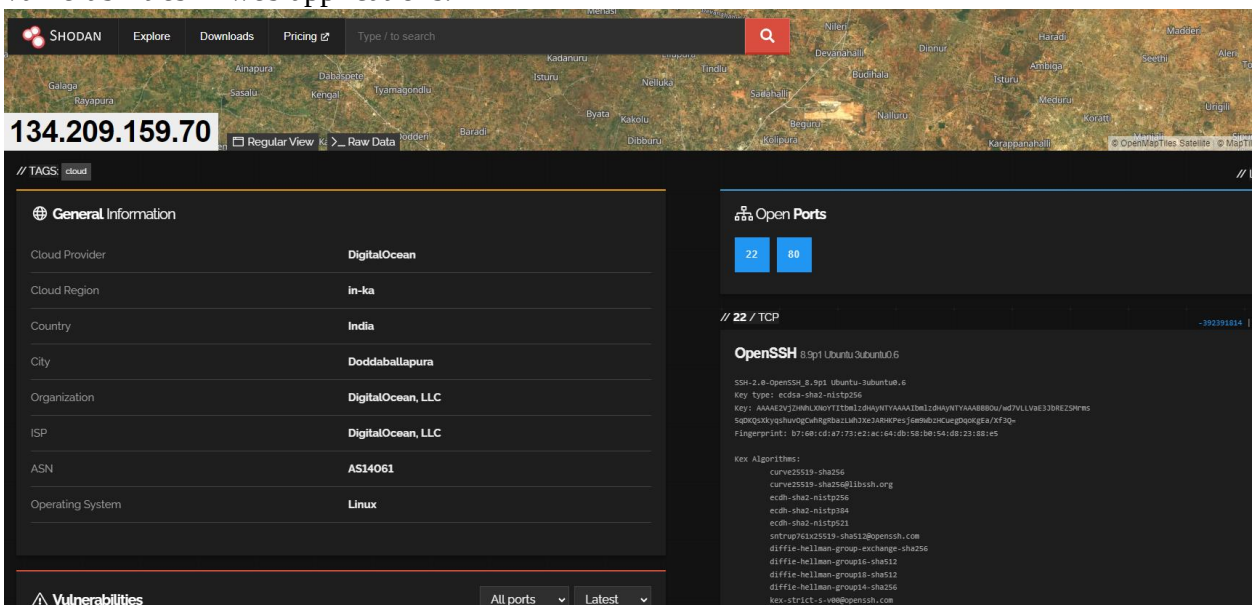
The destination IP in the logs is: 134.209.159.70

3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

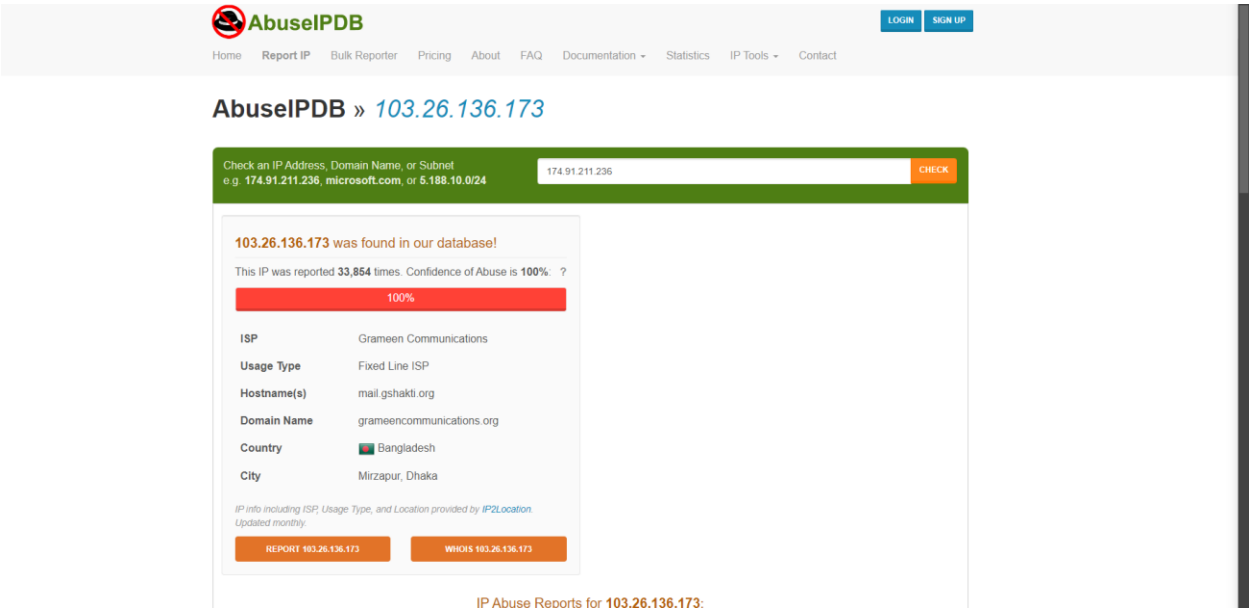
being attacked because:

1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.
2. HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.



4. What can you identify about the infrastructure used to attack, who does it belong to?

he IP 103.26.136.173 belongs to Grameen Communications, a fixed-line ISP in Mirzapur, Dhaka, Bangladesh. It is associated with over 33,854 reports of abuse, indicating that this infrastructure, likely a compromised server or a malicious actors system, is being used for attacks.



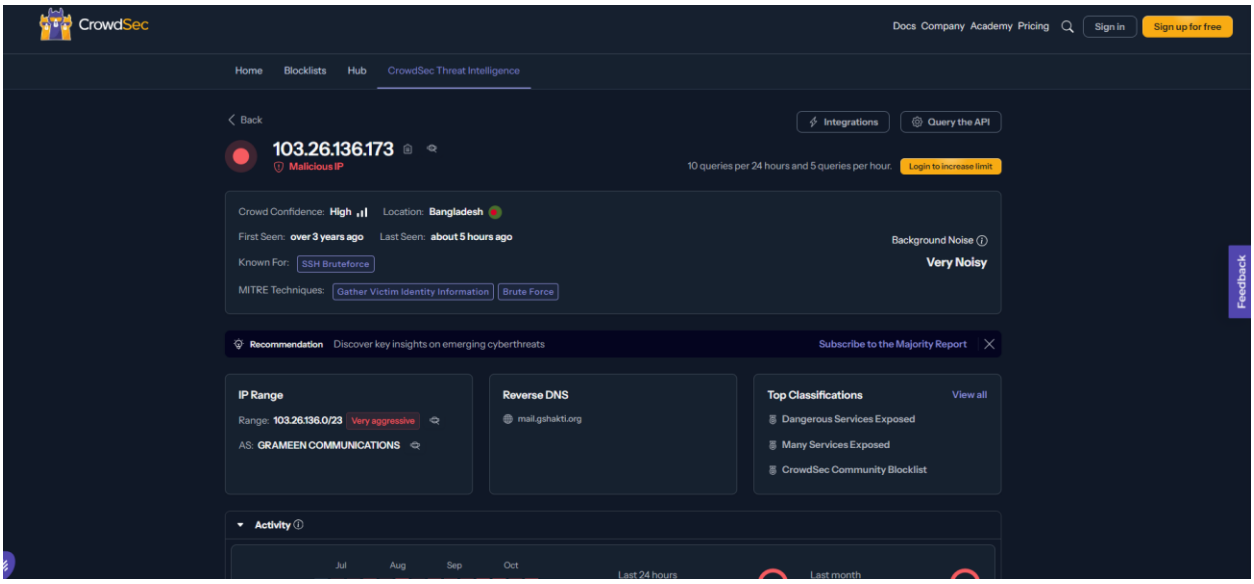
5. What is the event type?

1. The event type is flow. This means monitoring network traffic. In this case, it follows the flow of packets between the source and destination IP addresses.The event type is SSH for the IP 103.26.136.173, it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force atttacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

6. What TTPs do you observe?

For IP 103.26.136.173, the following tactics techniques, and procedures (TTPs) are observed:

- Brute Force: SSH bruteforce attempts to gain unauthorized access.



Event 12,13,30

1. what is the source of the attack?

103.147.242.68

12	103.147.242.68	134.209.159.70	ssh	91	Bangladesh	24	90
13	103.147.242.68	134.209.159.70	flow	91	Bangladesh	24	90

2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

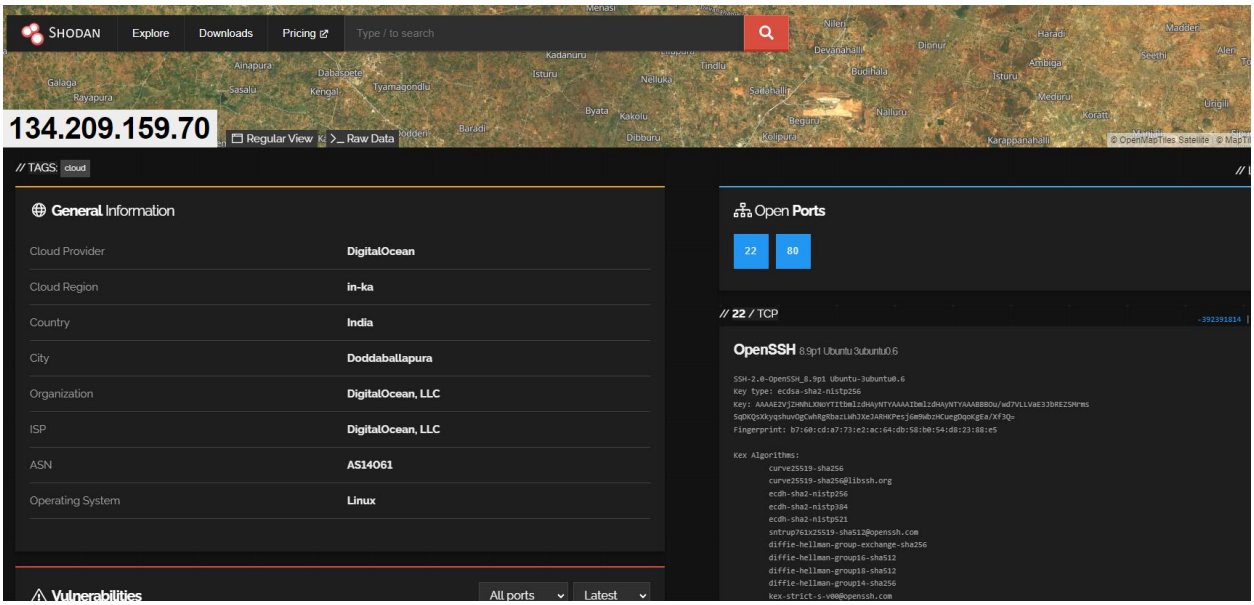
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

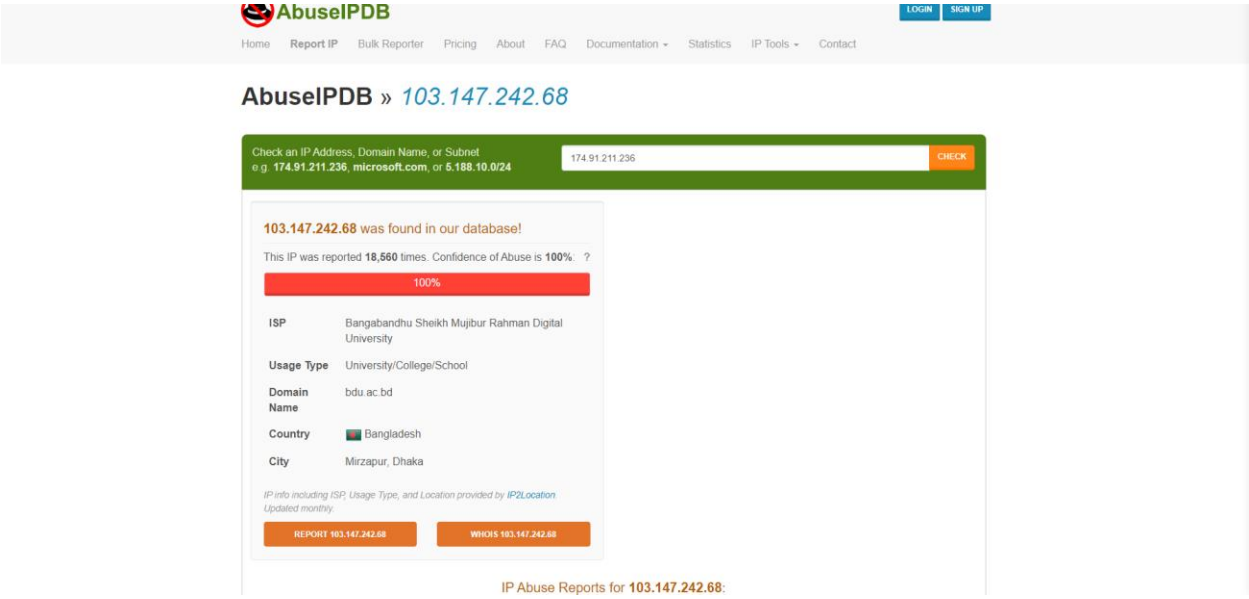
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

HTTP (port 80) can be targeted for webs-based attacks, such as exploiting vulnerabilities in web applications.



4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 103.147.242.68 belongs to Bangabandhu Sheikh Mujibur Rahman Digital University in Mirzapur, Dhaka, Bangladesh. It has been reported 18,560 times for abuse, indicating that the university's network may have been compromised and used for malicious activities.



5. What is the event type?

1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 103.147.242.68 it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

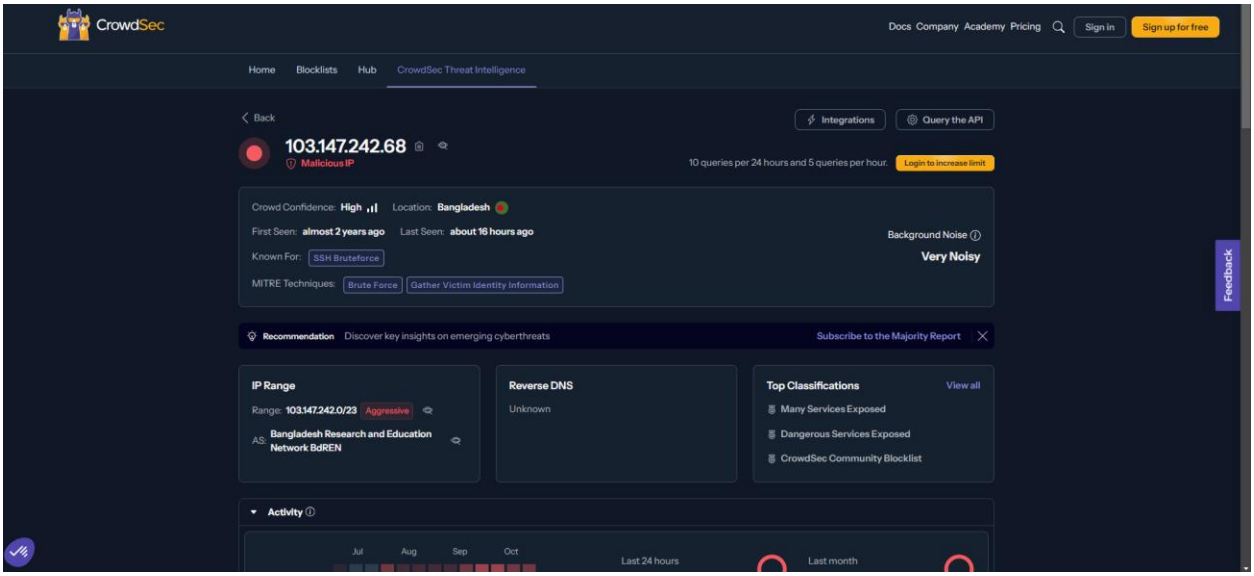
12	103.147.242.68	134.209.159.70	ssh	91	Bangladesh	24	90
13	103.147.242.68	134.209.159.70	flow	91	Bangladesh	24	90

6. What TTPs do you observe?

For IP 103.147.242.68, the following TTPs are observed:

- Brute Force: Involvement in SSH bruteforce attacks.
- Gather Victim Identity Information: Likely collecting sensitive information from compromised systems.

The IP has a high crowd confidence level and is associated with aggressive and noisy malicious activity, exposing many dangerous services.



Event 14,16

1. what is the source of the attack?

202.72.235.223

14	202.72.235.223	134.209.159.70	ssh	90	Dhaka	Bangladesh	23.8103	90.4125
16	202.72.235.223	134.209.159.70	flow	90	Dhaka	Bangladesh	23.8103	90.4125

2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

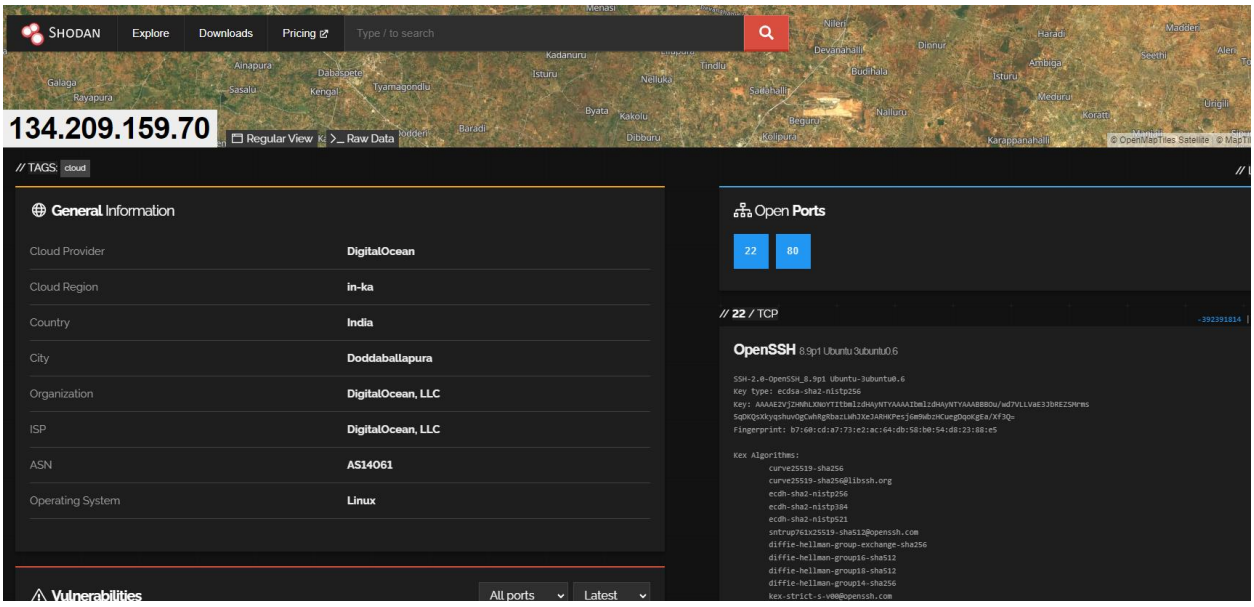
3. Why is the target being attacked?

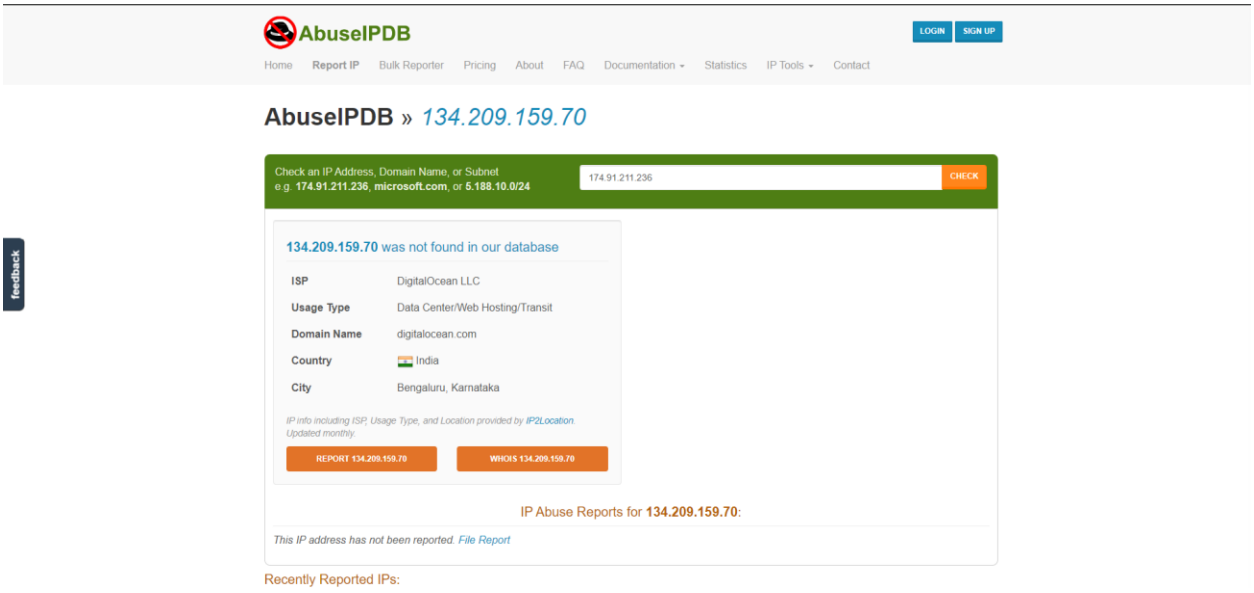
The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

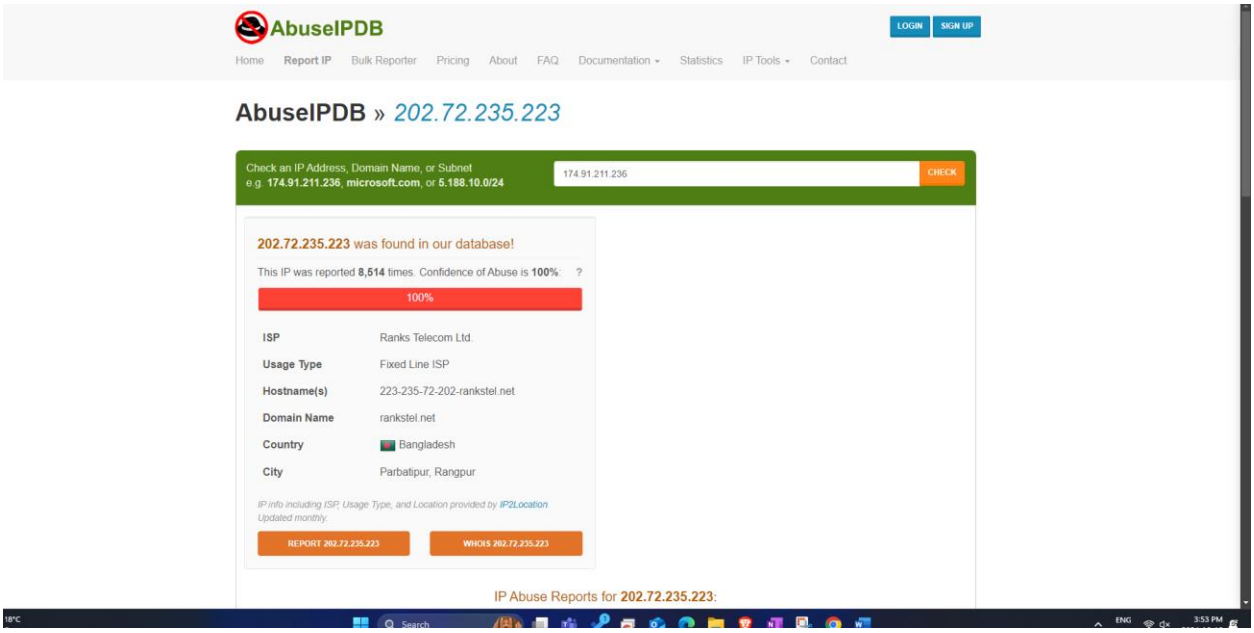
HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.





4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 202.72.235.223 belongs to Ranks Telecom Ltd, a fixed-line ISP in Parbatipur, Rangpur, Bangladesh. It has been reported 8,514 times for abuse, indicating that the infrastructure is either being used for malicious purposes or has been compromised.



5. What is the event type?

1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 202.72.235.223 it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

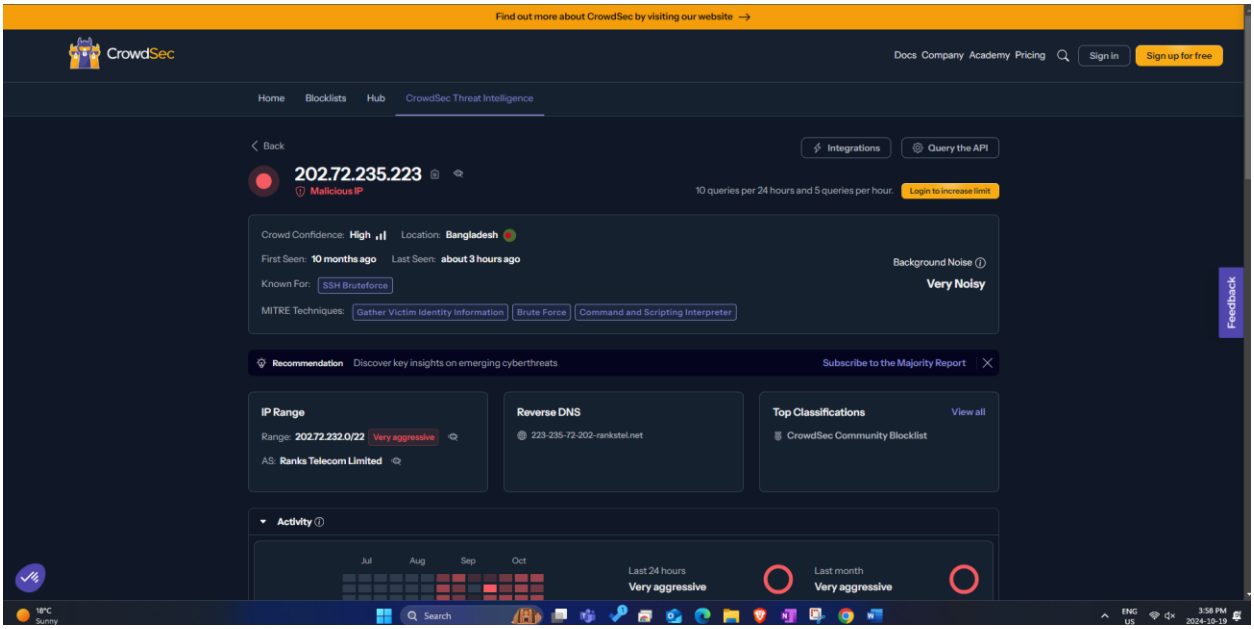
6. What TTPs do you observe?

For IP 202.72.235.223, the following TTPs are observed:

- SSH Bruteforce: Attempts to brute-force SSH credentials.
- Gather Victim Identity Information: Likely collecting sensitive data from compromised systems.

- Command and Scripting Interpreter: Possibly executing scripts or commands on compromised systems.

  This IP is marked as highly aggressive and noisy, frequently involved in malicious activities.

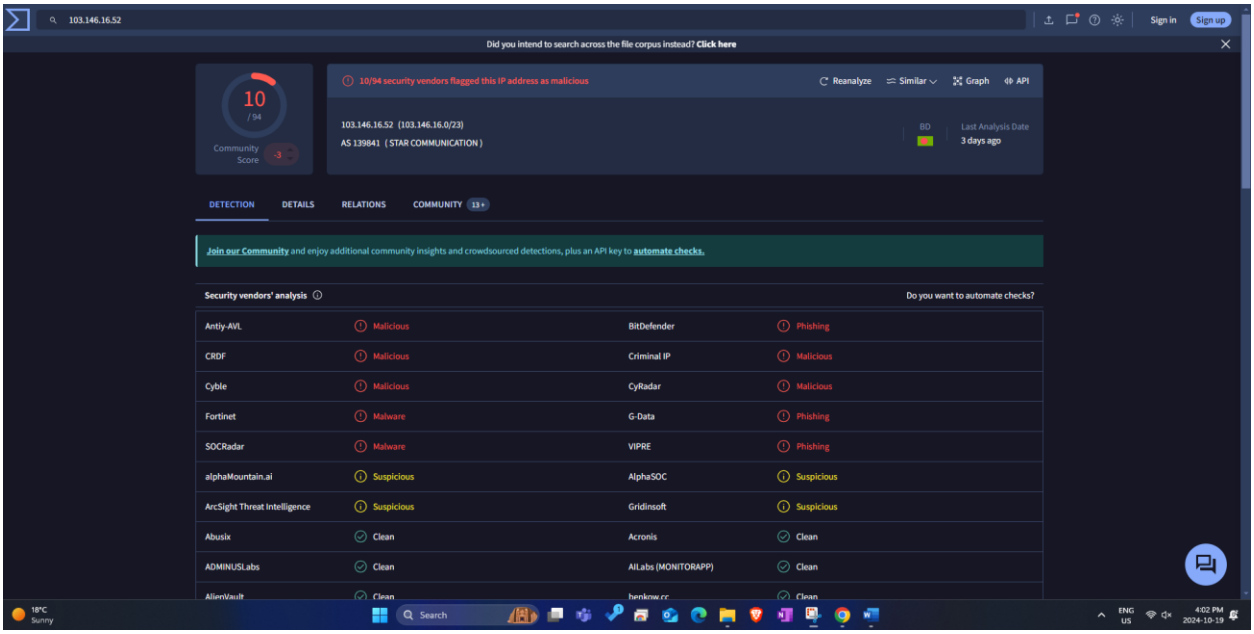


Event 15,19

1. what is the source of the attack?

103.146.16.52

15	103.146.16.52	134.209.159.70	ssh	90	Bangladesh	24	90
19	103.146.16.52	134.209.159.70	flow	90	Bangladesh	24	90



2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

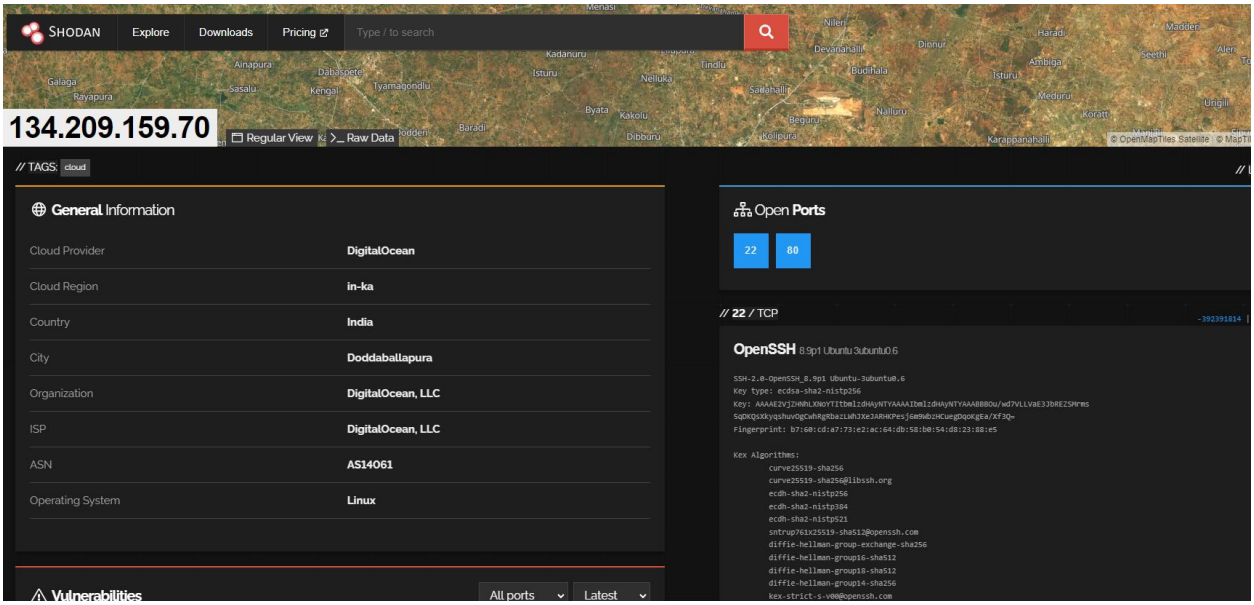
3. Why is the target being attacked?

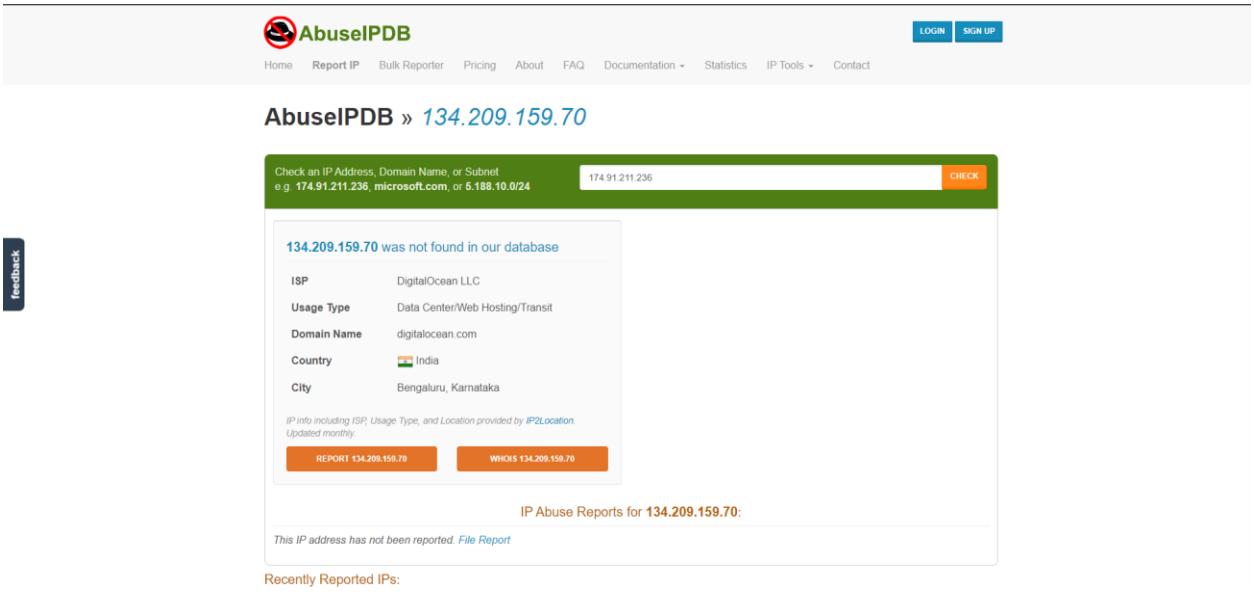
The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

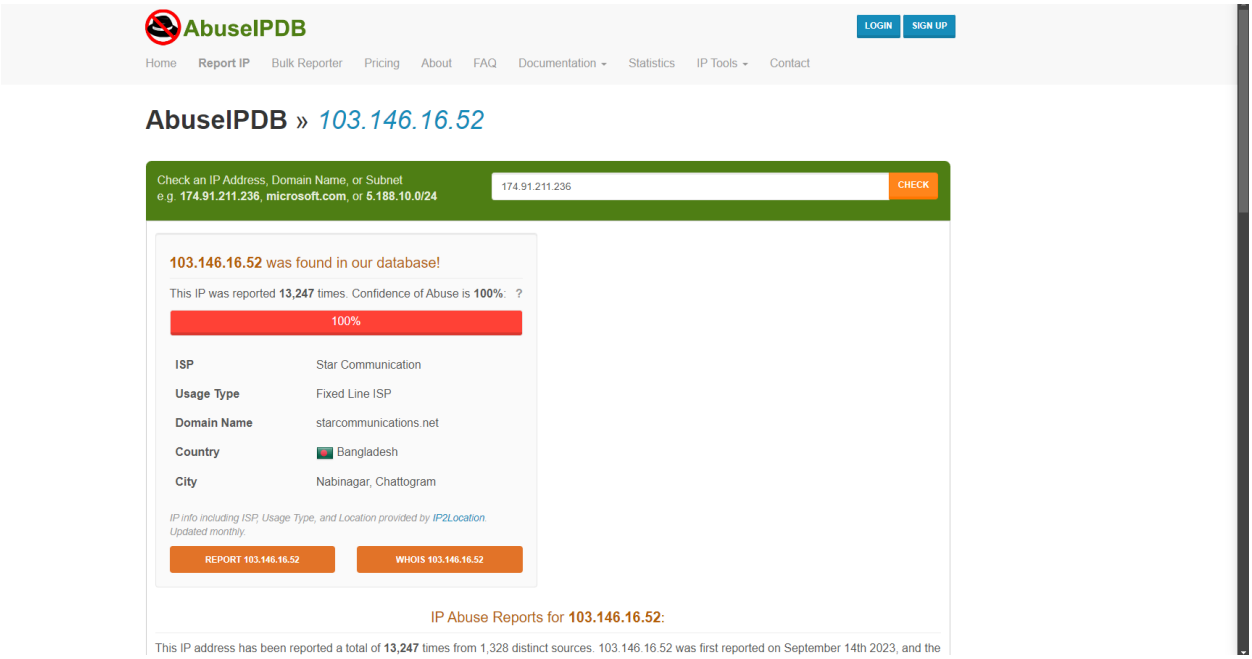
HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.





4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 103.146.16.52 belongs to Star Communication, a fixed-line ISP in Nabinagar, Chattogram, Bangladesh. It has been reported 13,247 times for abuse, indicating that the infrastructure may be compromised or being used for malicious activities.



5. What is the event type?

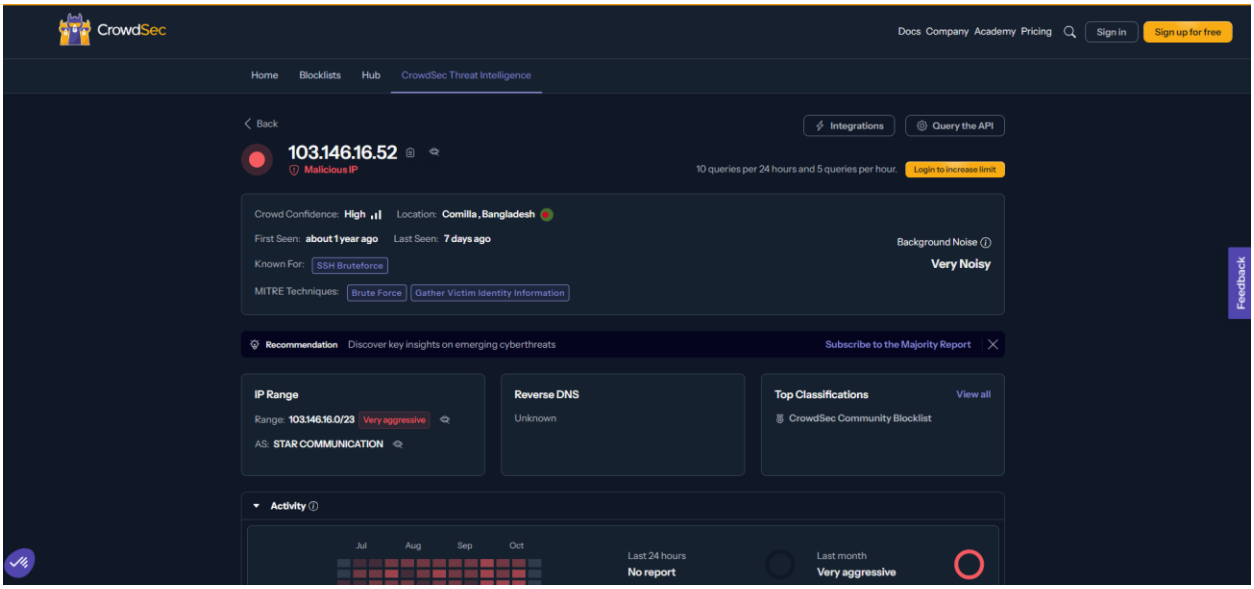
1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 103.146.16.52 it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

6. What TTPs do you observe?

For IP 103.146.16.52, the following TTPs are observed:

- Brute Force: Involvement in SSH bruteforce attacks.
- Gather Victim Identity Information: Likely collecting sensitive data from compromised systems.

This IP is marked as highly aggressive, noisy, and involved in repeated malicious activities, particularly focused on brute-forcing SSH credentials.

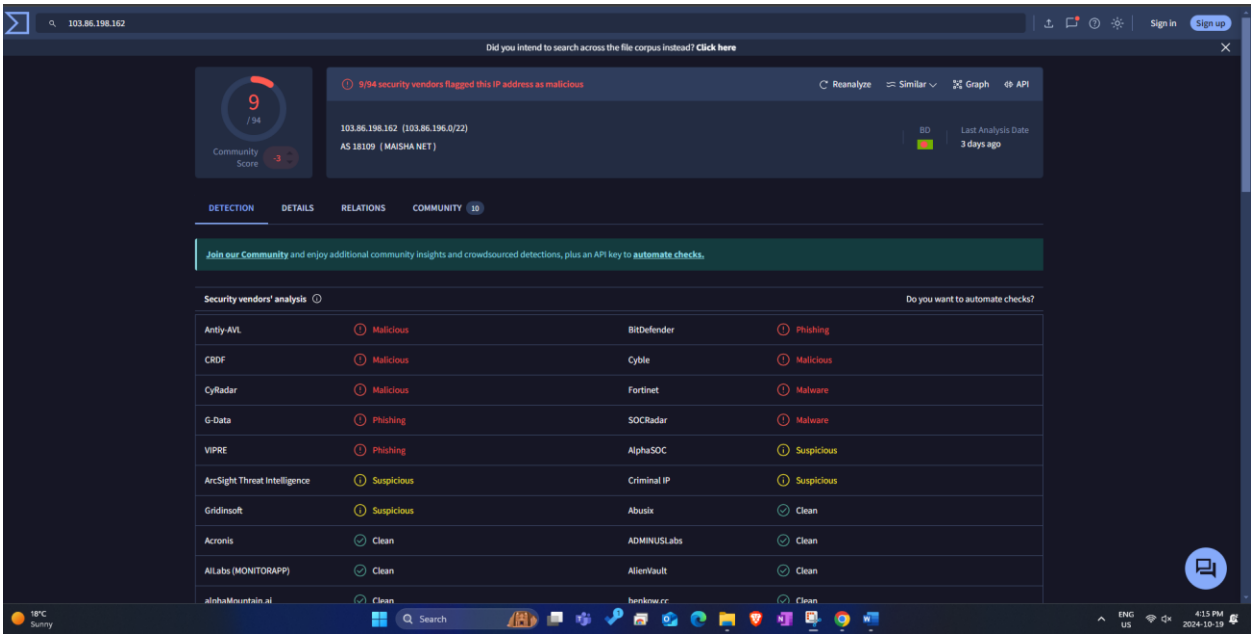


Event 17,18

1. **what is the source of the attack?**

   103.86.198.162

17	103.86.198.162	134.209.159.70	flow	90	Dhaka	Bangladesh	23.8103	90.4125
18	103.86.198.162	134.209.159.70	ssh	90	Dhaka	Bangladesh	23.8103	90.4125



2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

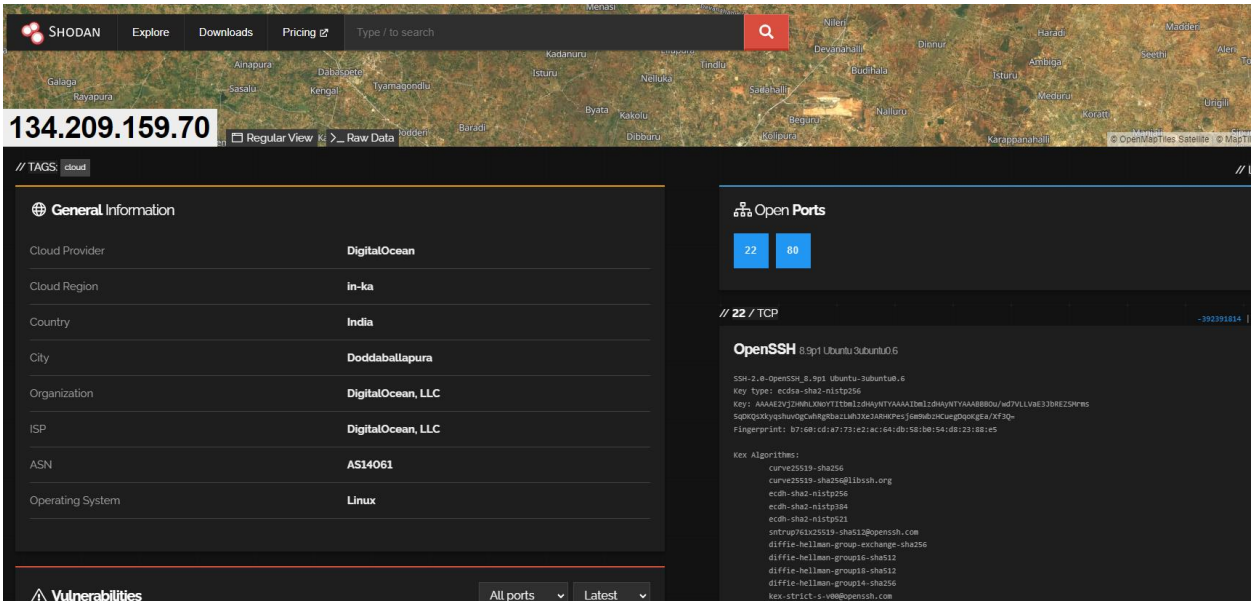
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

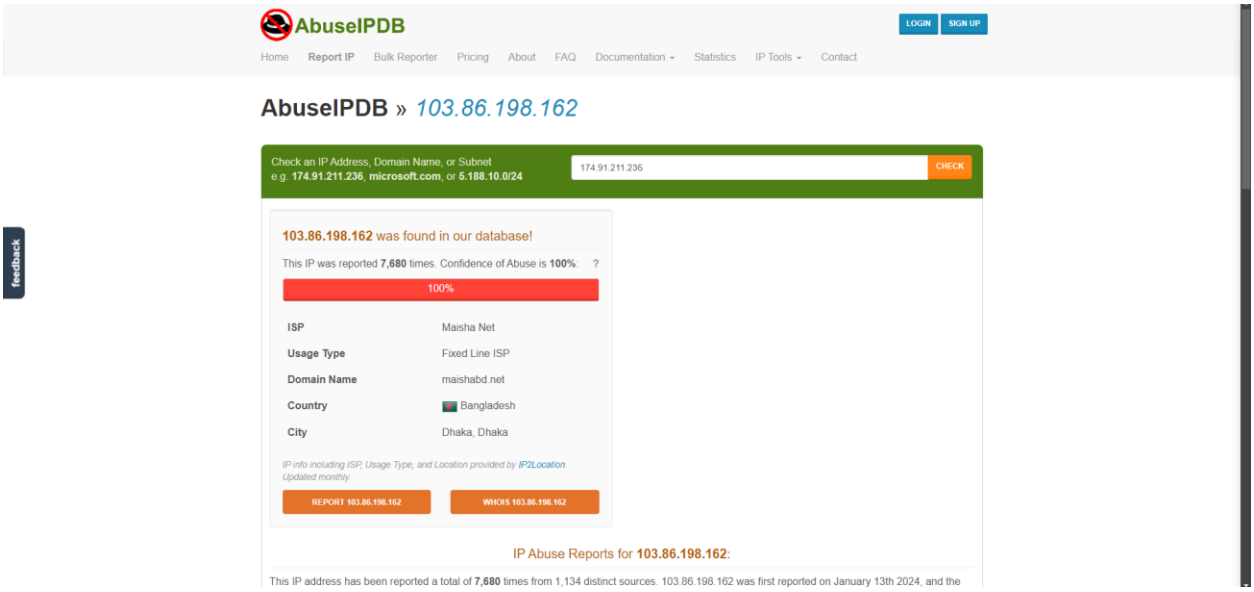
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.



4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 103.86.198.162 belongs to Maisha Net, a fixed-line ISP in Dhaka, Bangladesh. It has been reported 7,680 times for abuse, indicating that the infrastructure may be compromised or being used for malicious activities.



5. What is the event type?

1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 103.86.198.162 it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

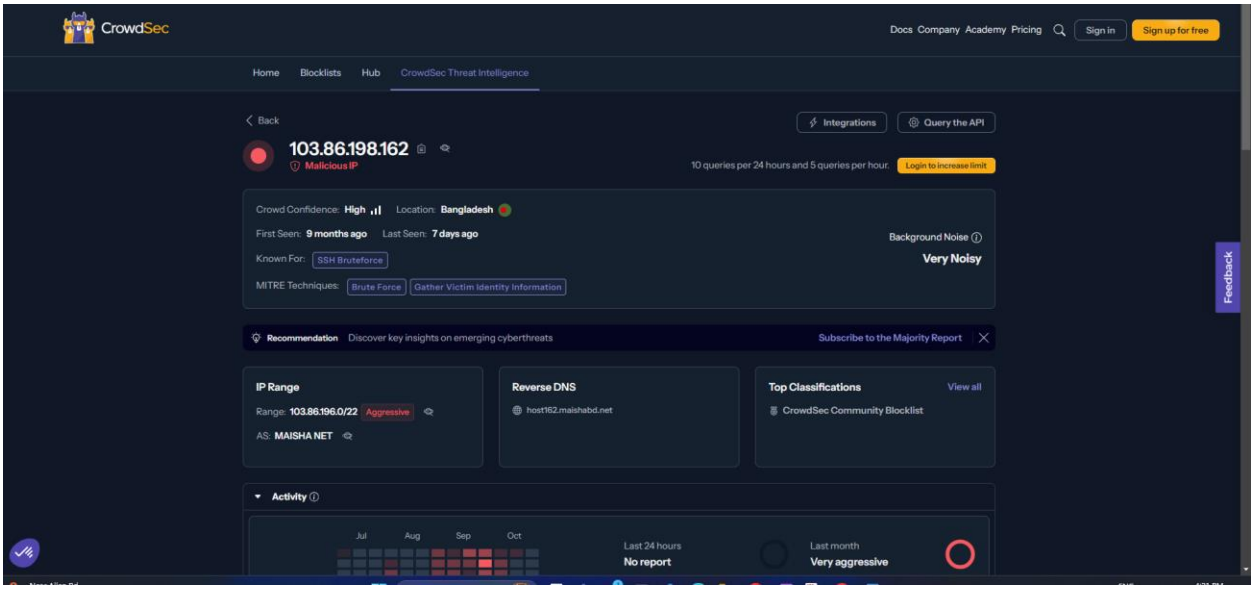
17	103.86.198.162	134.209.159.70	flow	90	Dhaka	Bangladesh	23.8103	90.4125
18	103.86.198.162	134.209.159.70	ssh	90	Dhaka	Bangladesh	23.8103	90.4125

6. What TTPs do you observe?

For IP 103.86.198.162, the following TTPs are observed:

- Brute Force: SSH bruteforce attacks aimed at gaining unauthorized access.
- Gather Victim Identity Information: Likely attempting to collect sensitive data from targeted systems.

This IP is labeled as very noisy and aggressive, consistently involved in SSH bruteforce activity.



Event 22,23

1. what is the source of the attack?

103.137.75.74

2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

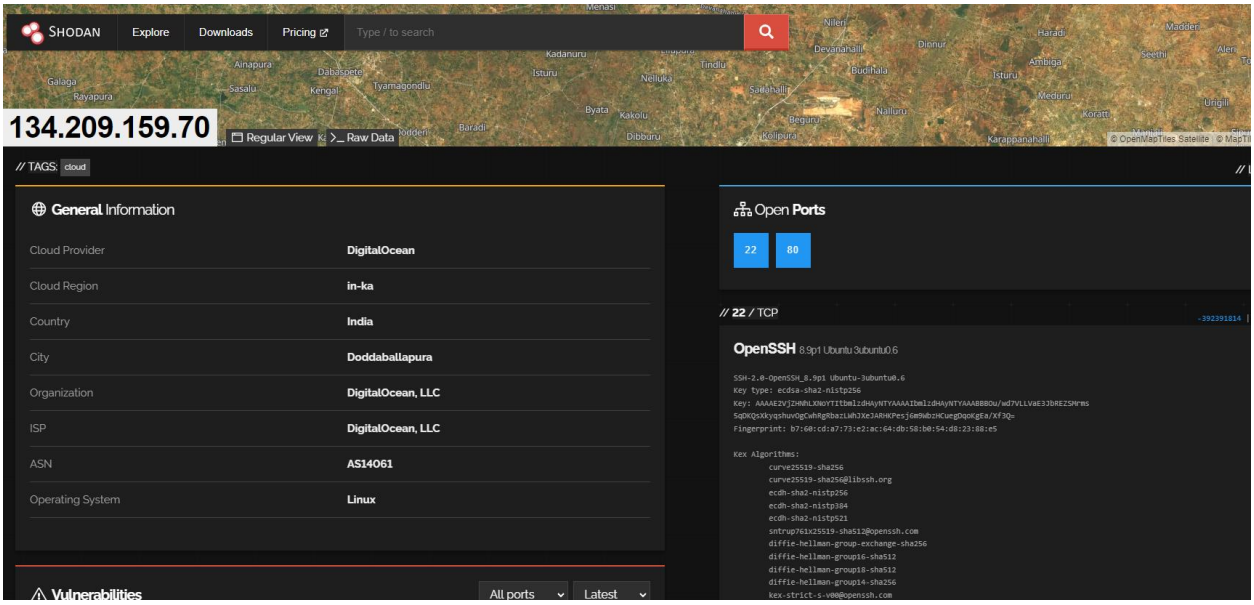
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

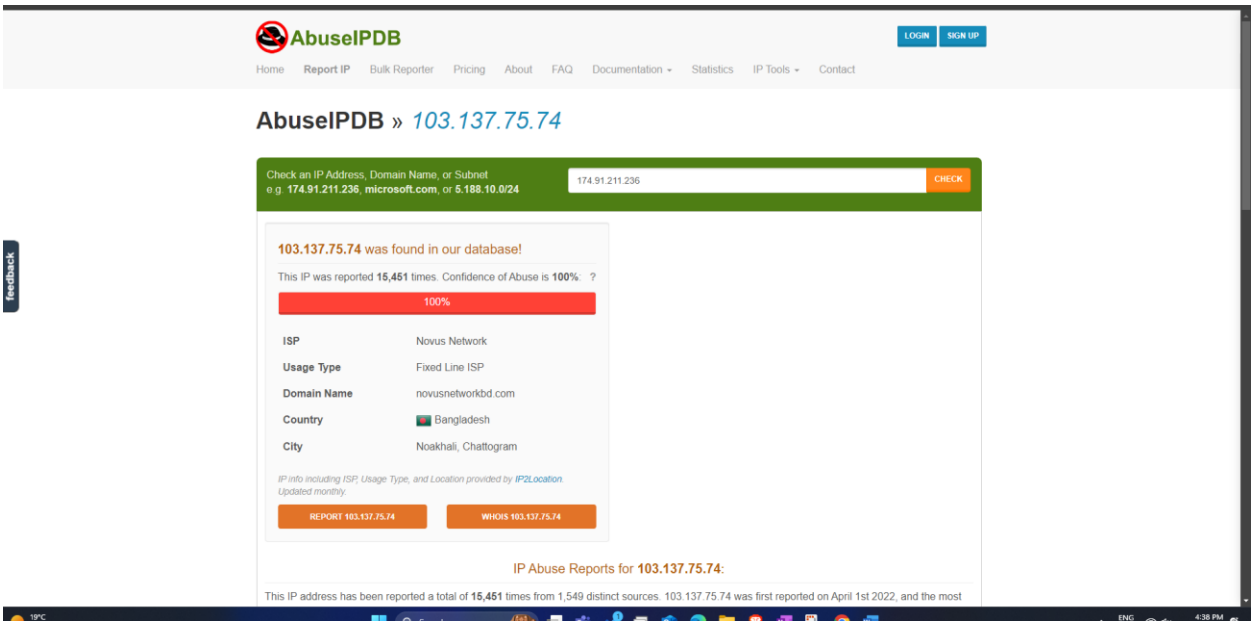
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.



4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 103.137.75.74 belongs to Novus Network, a fixed-line ISP in Noakhali, Chattogram, Bangladesh. It has been reported 15,451 times for abuse, indicating that the infrastructure may be compromised or is being used for malicious purposes.



5. What is the event type?

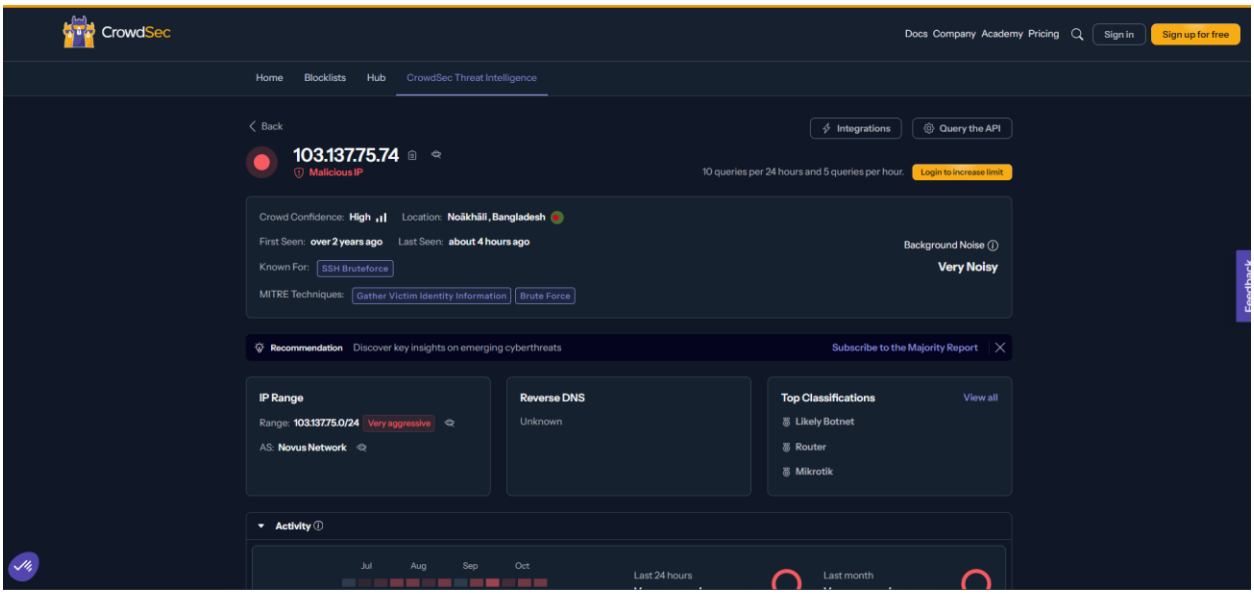
1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 103.137.75.74 it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

6. What TTPs do you observe?

Brute Force: SSH bruteforce attacks aimed at gaining unauthorized access.

vccccccGather Victim Identity Information: Likely attempting to collect sensitive data from targeted systems.

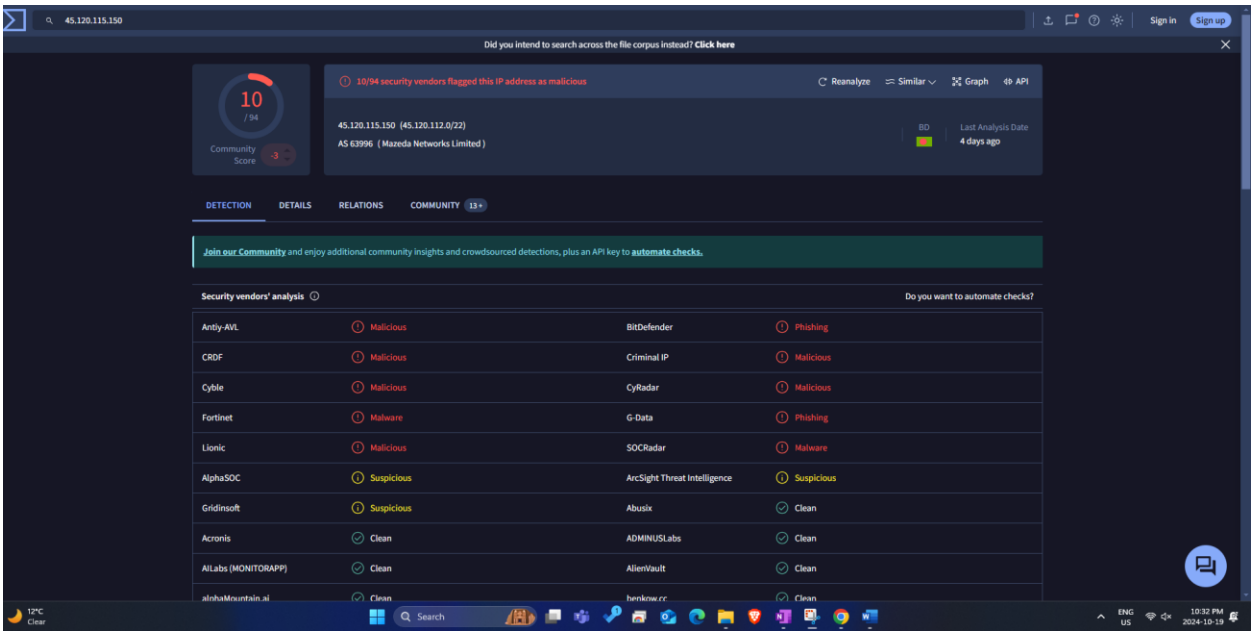
This IP is labeled as very noisy and aggressive, consistently involved in SSH bruteforce activity.



Event 24,25

1. what is the source of the attack?

45.120.115.150



2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

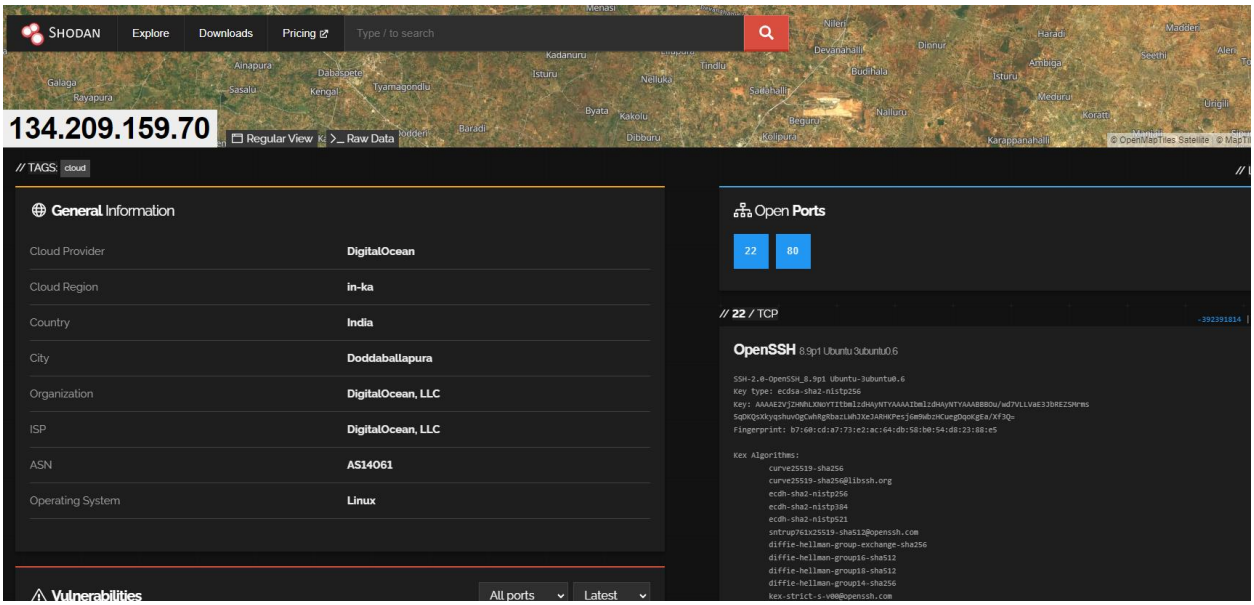
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

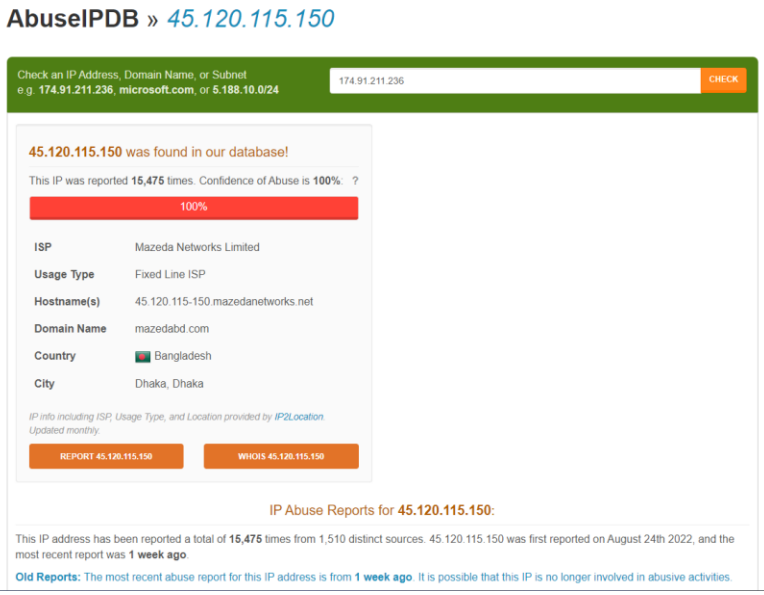
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.



4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 45.120.115.150 belongs to Mazeda Networks Limited, a fixed-line ISP in Dhaka, Bangladesh**.** It has been reported 15,475 times for abuse, suggesting that the infrastructure may be compromised or is being used for malicious activities.



5. What is the event type?

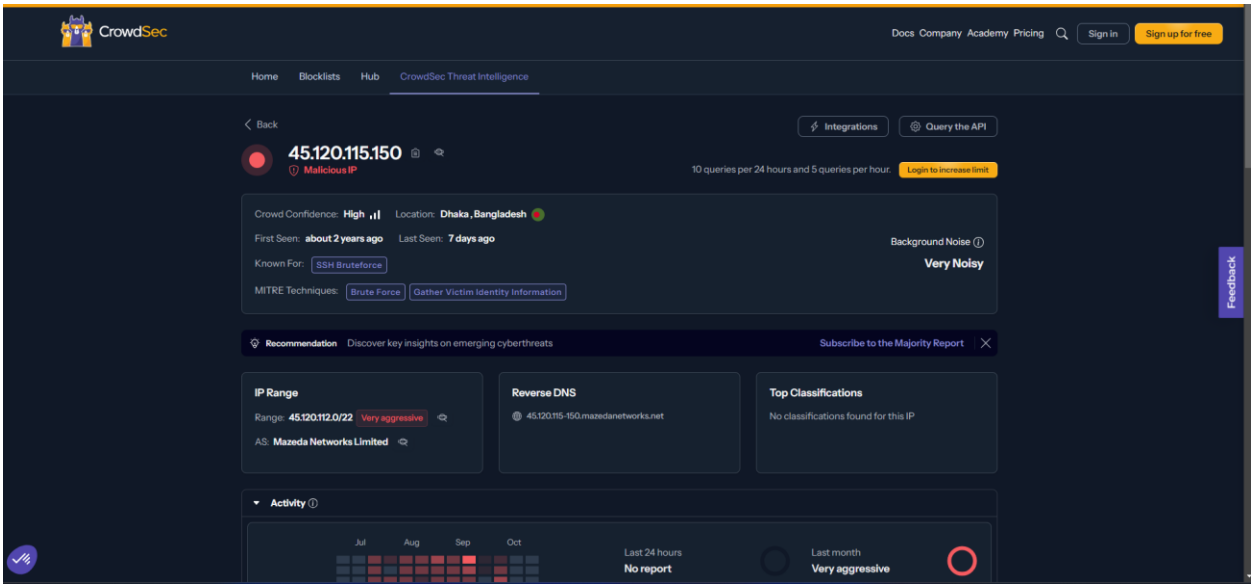
1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is SSH for the IP 45.120.115.150 it means that this IP is attempting to connect to the target system using the SSH protocol. This is typically an indication of brute-force attacks or attempts to exploit vulnerabilities in SSH to gain unauthorized access to the system.

6. What TTPs do you observe?

For IP 45.120.115.150, the following TTPs are observed:

- Brute Force: SSH bruteforce attacks to gain unauthorized access.
- Gather Victim Identity Information: Likely attempting to steal sensitive data from compromised systems.

This IP is highly aggressive and noisy, frequently involved in SSH bruteforce activity.

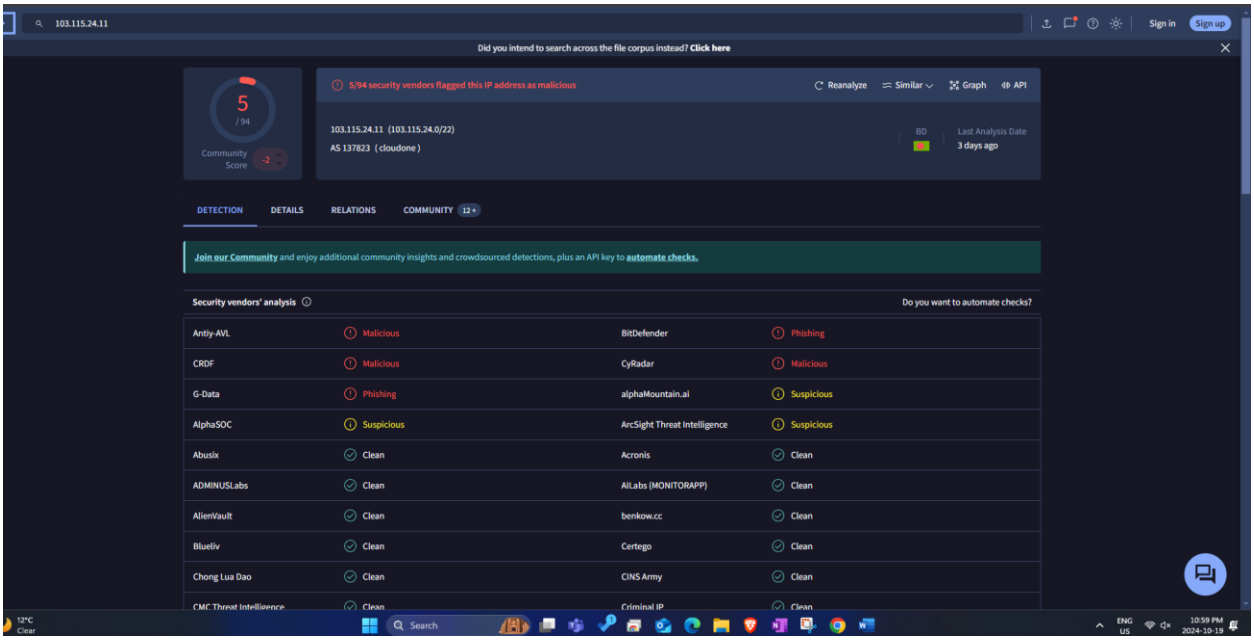


Event 26,27

1. what is the source of the attack?

103.115.24.11

26	103.115.24.11	134.209.159.70	flow	61	Bangladesh	24	90
27	103.115.24.11	134.209.159.70	ssh	61	Bangladesh	24	90



2. what are they attacking?

The destination IP in the logs is: 134.209.159.70

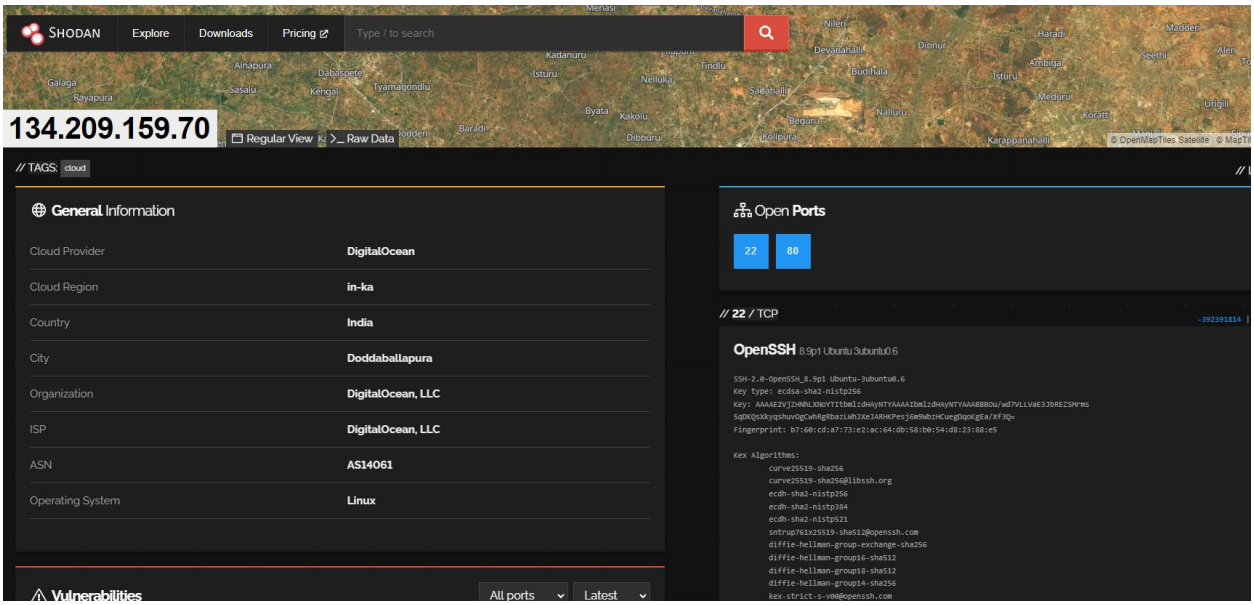
3. Why is the target being attacked?

The target IP 134.209.159.70 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server.

being attacked because:

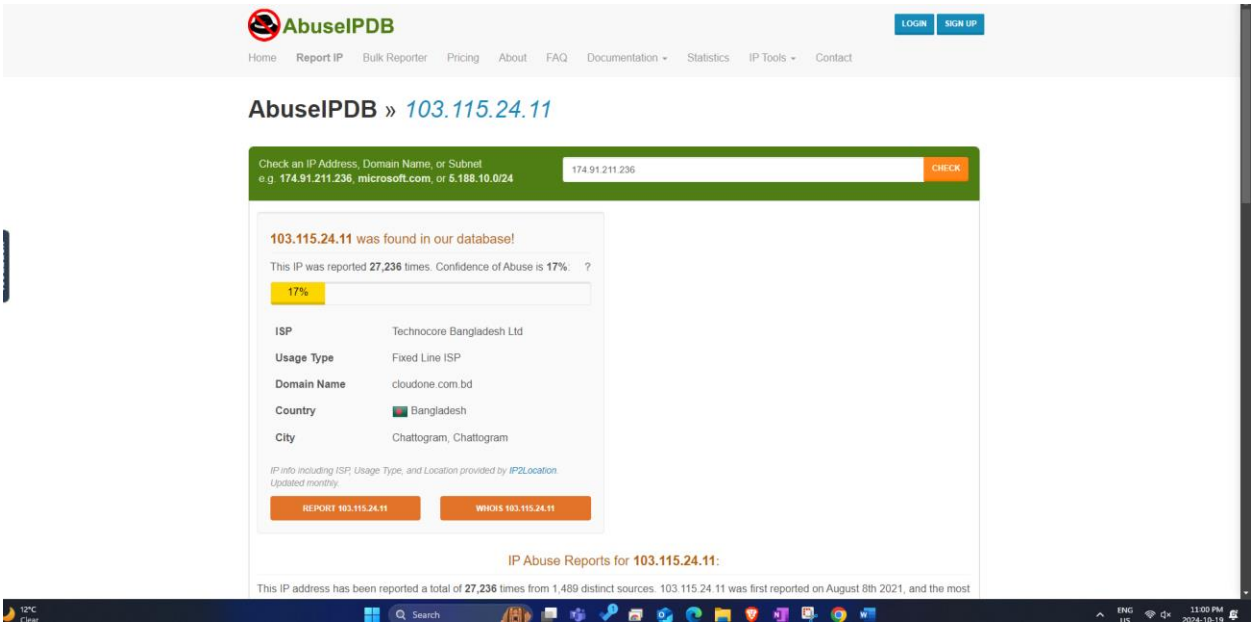
1. SSH (port 22) is a common target for brute-force attacks or attempts to exploit misconfigured authentication.

HTTP (port 80) can be targeted for web-based attacks, such as exploiting vulnerabilities in web applications.



4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 103.115.24.11 belongs to Technocore Bangladesh Ltd, a fixed-line ISP in Chattogram, Bangladesh. It has been reported 27,236 times for abuse, indicating that the infrastructure may be compromised or is being used for malicious activities.



5. What is the event type?

1. the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.

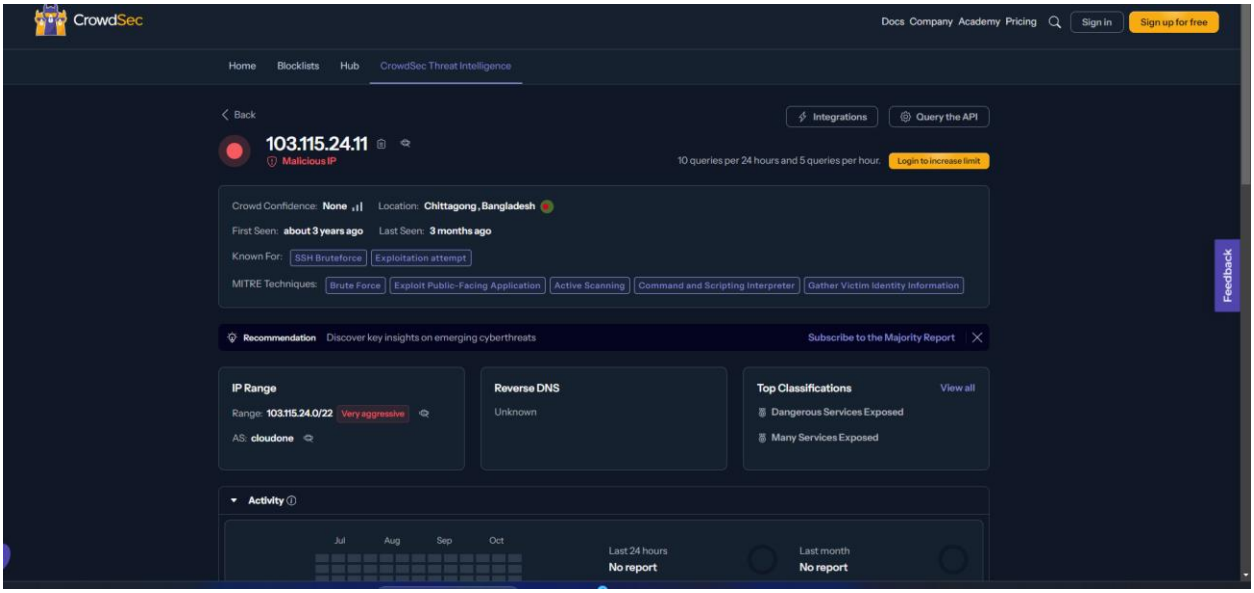
2. The event type is SSH for the IP 103.115.24.11 it means that this IP is attempting to connect to the target system using the SSH protocol.

26	103.115.24.11	134.209.159.70	flow	61	Bangladesh	24	90
27	103.115.24.11	134.209.159.70	ssh	61	Bangladesh	24	90

6. What TTPs do you observe?

For IP 103.115.24.11, the following TTPs are observed:

- Brute Force: SSH bruteforce attacks.
- Exploit Public-Facing Application: Attempts to exploit vulnerable public services.
- Active Scanning: Scanning for exposed services.
- Command and Scripting Interpreter: Likely executing scripts on compromised systems.
- Gather Victim Identity Information: Trying to collect sensitive data.

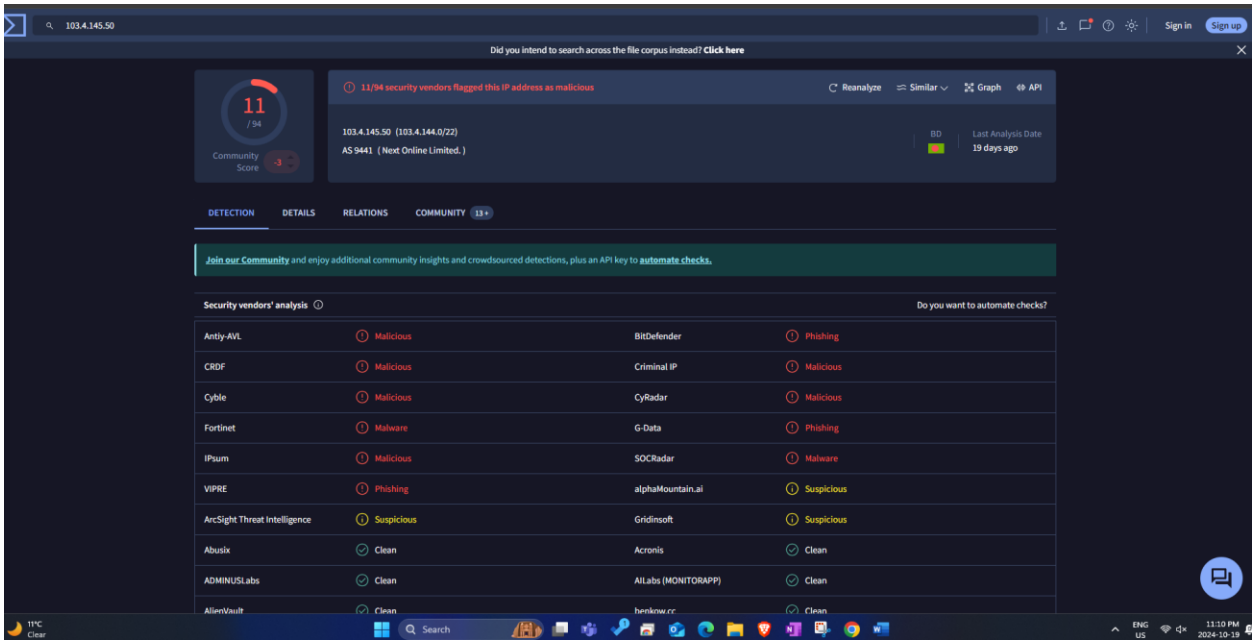


Event 29

1. what is the source of the attack?

103.152.18.138

29	103.4.145.50	64.226.119.125		flow	60	Dhaka	Bangladesh	23.8103	90.4125



2. what are they attacking?

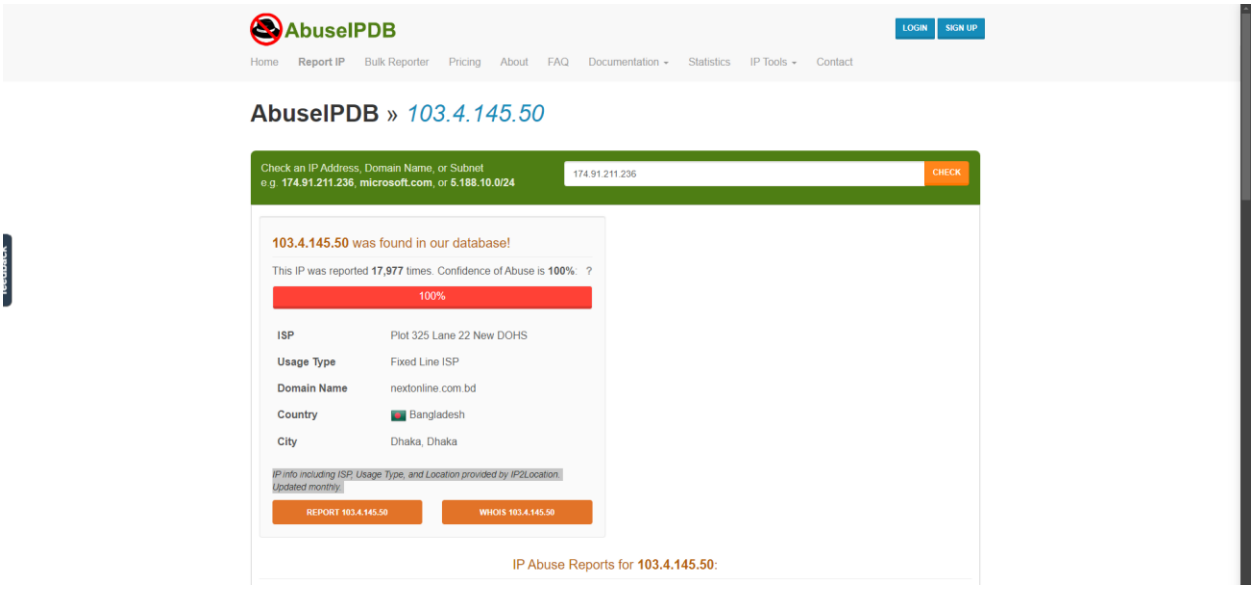
64.226.119.125

3. Why is the target being attacked?

The target IP 64.226.119.125 is hosted on DigitalOcean in India and runs services like SSH (port 22) and HTTP (port 80) on a Linux server

4. What can you identify about the infrastructure used to attack, who does it belong to?

The IP 103.4.145.50 belongs to Nexton Communications, a fixed-line ISP in Dhaka, Bangladesh. It has been reported 17,977 times for abuse, indicating that this infrastructure may be compromised or is being used for malicious activities.



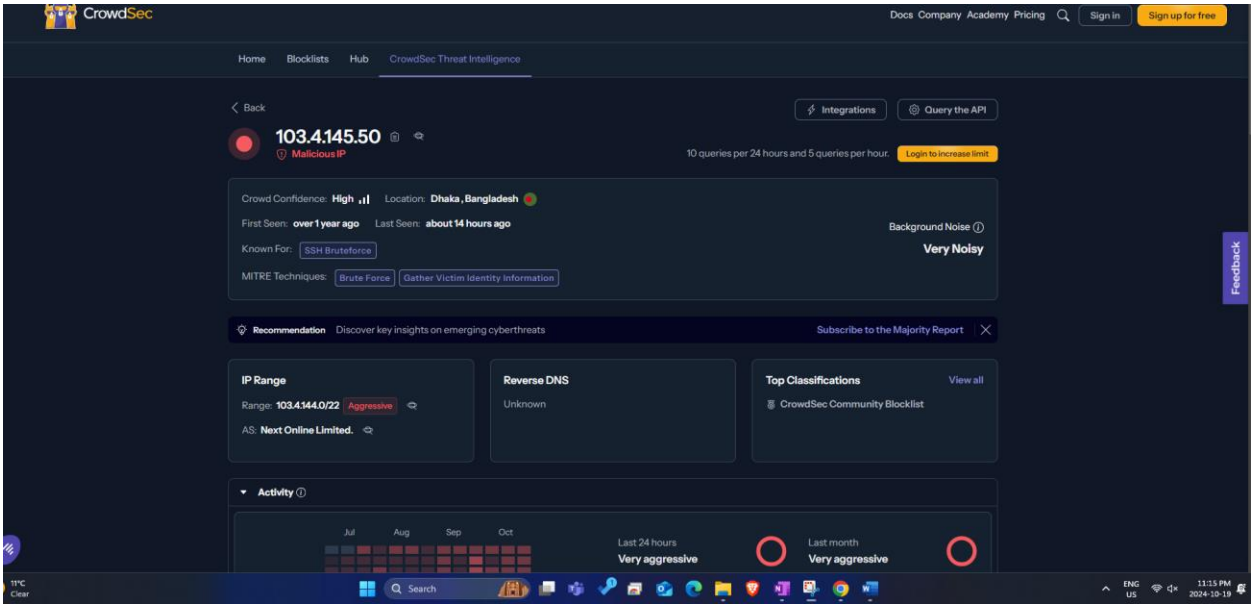
5. What is the event type?

the event type is flow, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses

6. What TTPs do you observe?

Brute Force: SSH bruteforce attacks.

Gather Victim Identity Information: Trying to collect sensitive data


CrowdSec
Docs Company Academy Pricing
Sign in
Sign up for free
Home
Blocklists
Hub
CrowdSec Threat Intelligence
Back
Integrations
Query the API
103.4.145.50
Malicious IP
10 queries per 24 hours and 5 queries per hour.
Login to increase limit
Crowd Confidence: High
Location: Dhaka, Bangladesh
First Seen: over 1 year ago
Last Seen: about 14 hours ago
Known For: SSH Bruteforce
MITRE Techniques: Brute Force
Gather Victim Identity Information
Background Noise
Very Noisy
Recommendation
Discover key insights on emerging cyberthreats
Subscribe to the Majority Report
IP Range
Range: 103.4.144.0/22
Aggressive
AS: Next Online Limited.
Reverse DNS
Unknown
Top Classifications
View all
CrowdSec Community Blocklist
Activity
Jul
Aug
Sep
Oct
Last 24 hours
Very aggressive
Last month
Very aggressive
Feedback
Search