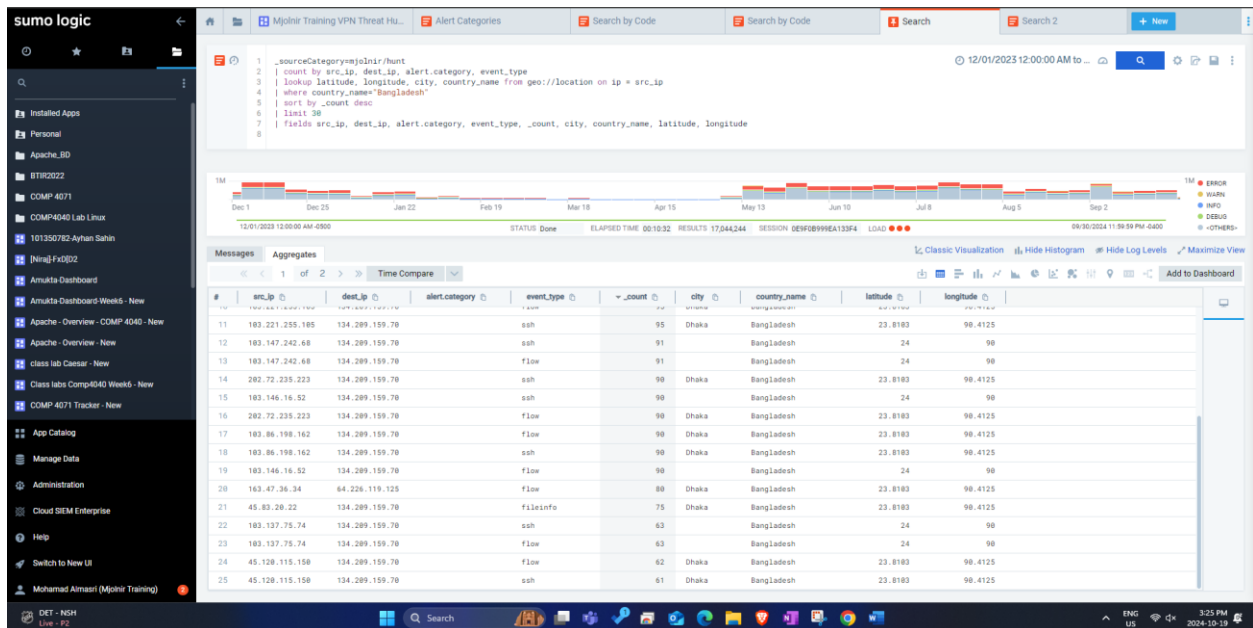
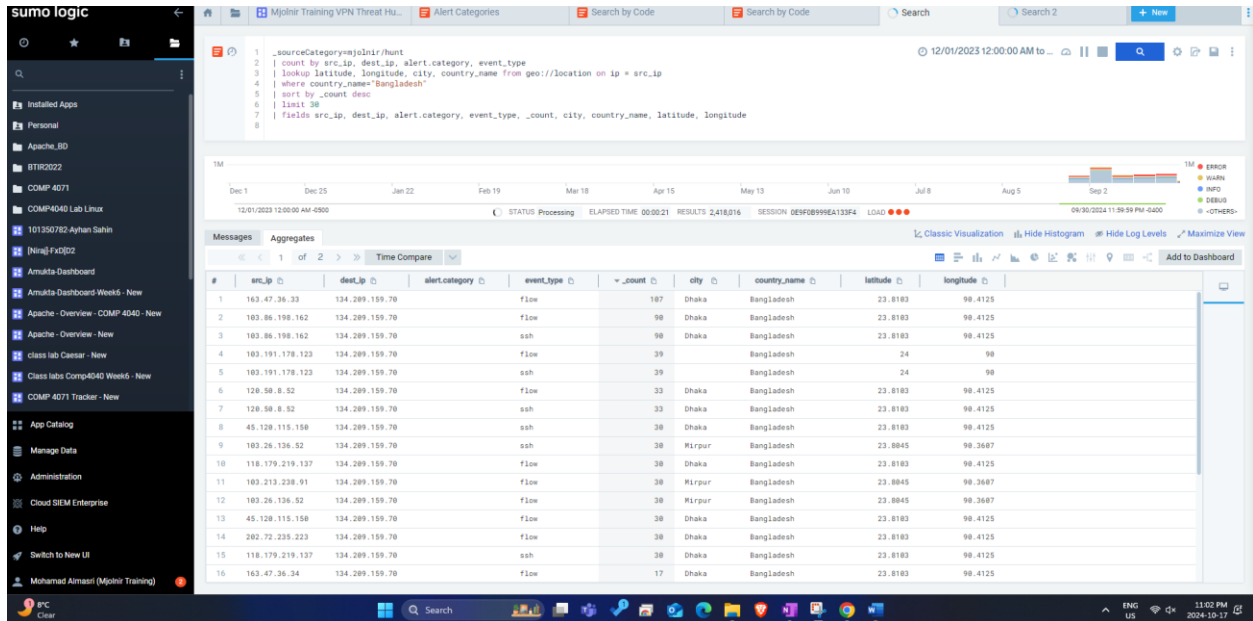
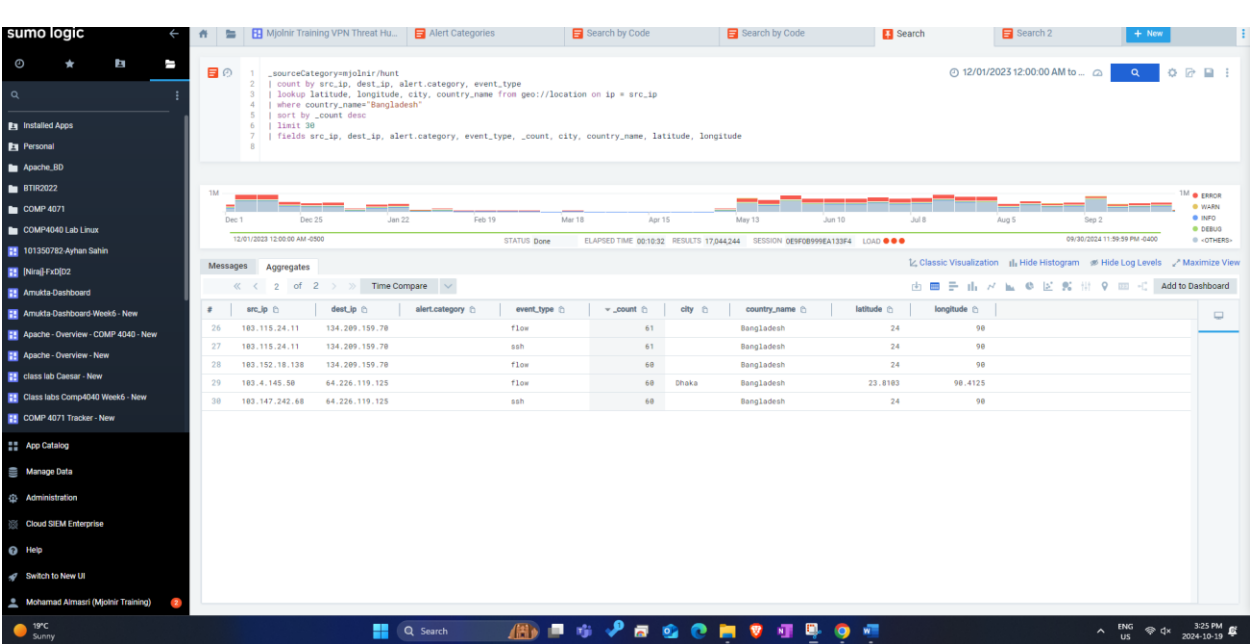


DIGITAL FORENSICS&INCID. RESP - COMP 4071

Assignment 1





Event 1,2

1. what is the source of the attack?

1	163.47.36.33	134.209.159.78	flow	513	Dhaka	Bangladesh	23.8183	98.4125
1	163.47.36.33	134.209.159.78	flow	513	Dhaka	Bangladesh	23.8183	98.4125
2	163.47.36.33	64.226.119.125	flow	317	Dhaka	Bangladesh	23.8183	98.4125

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

AbuseIPDB LOGIN SIGN UP

Home Report IP Bulk Reporter Pricing About FAQ Documentation - Statistics IP Tools - Contact

AbuseIPDB » 163.47.36.33

Check an IP Address, Domain Name, or Subnet
e.g. 174.91.211.236, microsoft.com, or 5.188.10.0/24

174.91.211.236 CHECK

163.47.36.33 was found in our database!

This IP was reported 14,632 times. Confidence of Abuse is 100% ?

100%

ISP Bangladesh Research and Education Network

Usage Type University/College/School

Domain Name bdren.net.bd

Country Bangladesh

City Dhaka, Dhaka

IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 163.47.36.33 WHOIS 163.47.36.33

IP Abuse Reports for 163.47.36.33

163.47.36.33

Did you intend to search across the file corpus instead? [Click here](#)

9/94 security vendors flagged this IP address as malicious

163.47.36.33 (163.47.36.0/22)
AS 63961 (Bangladesh Research and Education Network BdREN)

BD Last Analysis Date 19 days ago

Community Score 9 / 94

DETECTION DETAILS RELATIONS COMMUNITY 18

Security vendors' analysis

Vendor	Verdict	Vendor	Verdict
Antiy-AVL	Malicious	Cluster25	Malicious
CRDF	Malicious	Criminal IP	Malicious
Cyble	Malicious	CyRadar	Malicious
Fortinet	Malware	Lionic	Malicious
SOCRadar	Malicious	alphaMountain.ai	Suspicious
AlphaSOC	Suspicious	ArcSight Threat Intelligence	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	benkow.cc	Clean
BitDefender	Clean	Blueliv	Clean

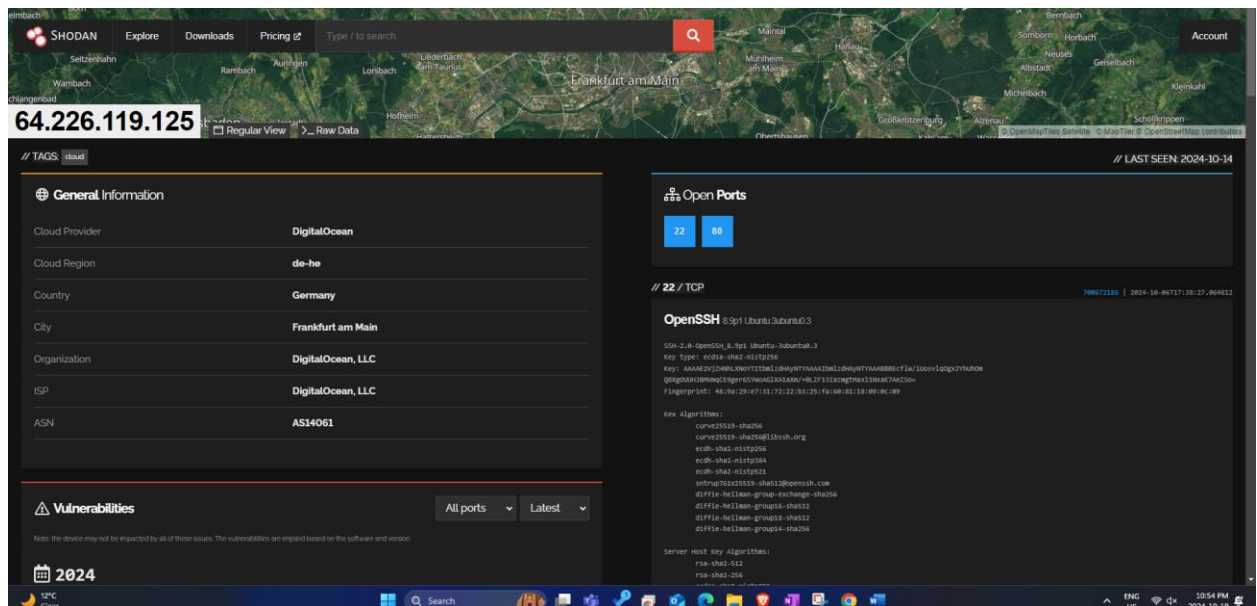
Do you want to automate checks?

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

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

Basic Properties

Network

Autonomous System Number

Autonomous System Label

Regional Internet Registry

Country

Continent

163.47.36.0/22

63961

Bangladesh Research and Education Network BdREN

APNIC

BD

AS

Whois Lookup

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.

163.47.36.33

Did you intend to search across the file corpus instead? Click here

9 / 94

Community Score

9/94 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

163.47.36.33 (163.47.36.0/22)

BD

AS 63961 (Bangladesh Research and Education Network BdREN)

Last Analysis Date

19 days ago

DETECTION

DETAILS

RELATIONS

COMMUNITY 16

Basic Properties

Network

Autonomous System Number

Autonomous System Label

Regional Internet Registry

Country

Continent

163.47.36.0/22

63961

Bangladesh Research and Education Network BdREN

APNIC

BD

AS

#	src_ip	dest_ip	alert.category	event_type	_count	city	country_name	latitude	longitude
1	163.47.36.33	134.209.159.78		flow	513	Dhaka	Bangladesh	23.8183	90.4125

6. What TTPs do you observe?

163.47.36.33

Malicious IP

29 queries left for the week. Upgrade to get more quota

Crowd Confidence: Medium

Location: Bangladesh

First Seen: over 2 years ago

Last Seen: 19 days ago

Known For: TCP Scan Exploitation attempt HTTP Bruteforce

Background Noise Noisy

Mitre Techniques: Active Scanning Remote System Discovery Network Service Discovery Exploit Public-Facing Application Bruteforce

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

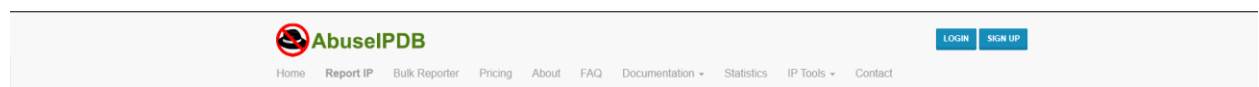
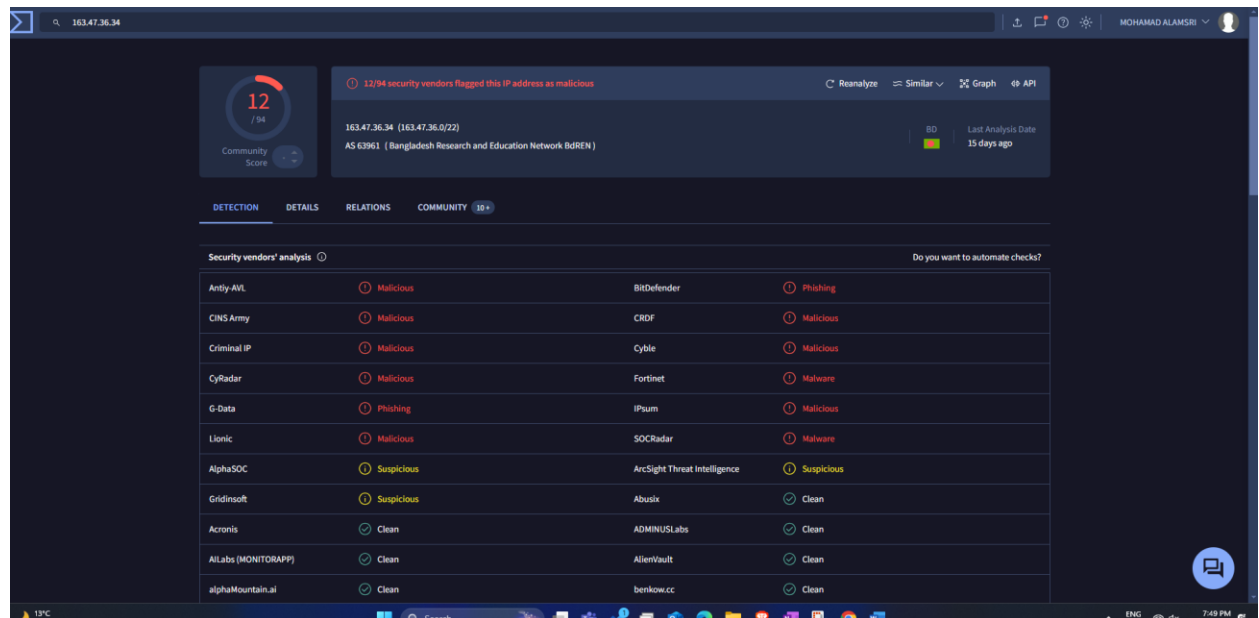
other forms of force. of authentication This depends on the nature of the malicious activity being flagged. (As seen in the analysis report)

Event 3,20

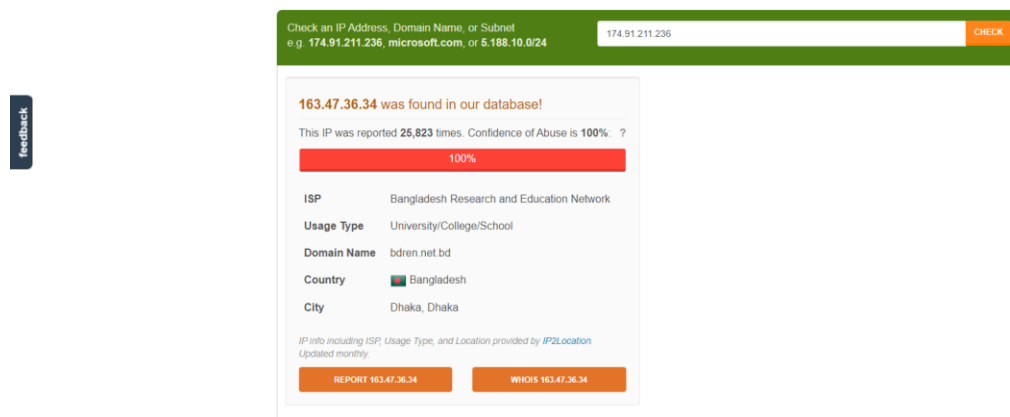
1. what is the source of the attack?

20	163.47.36.34	64.226.119.125	flow	88	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



AbuseIPDB » 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 98.4125

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.

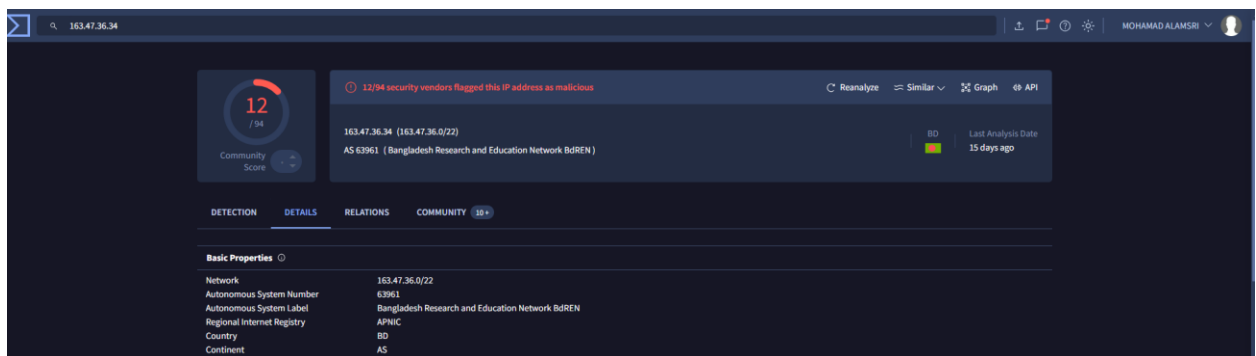
being attacked because:

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.

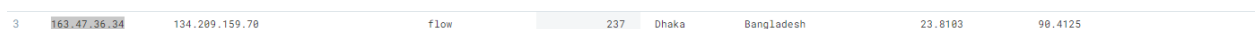
4. What can you identify about the infrastructure used to attack, who does it belong to?

- 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.

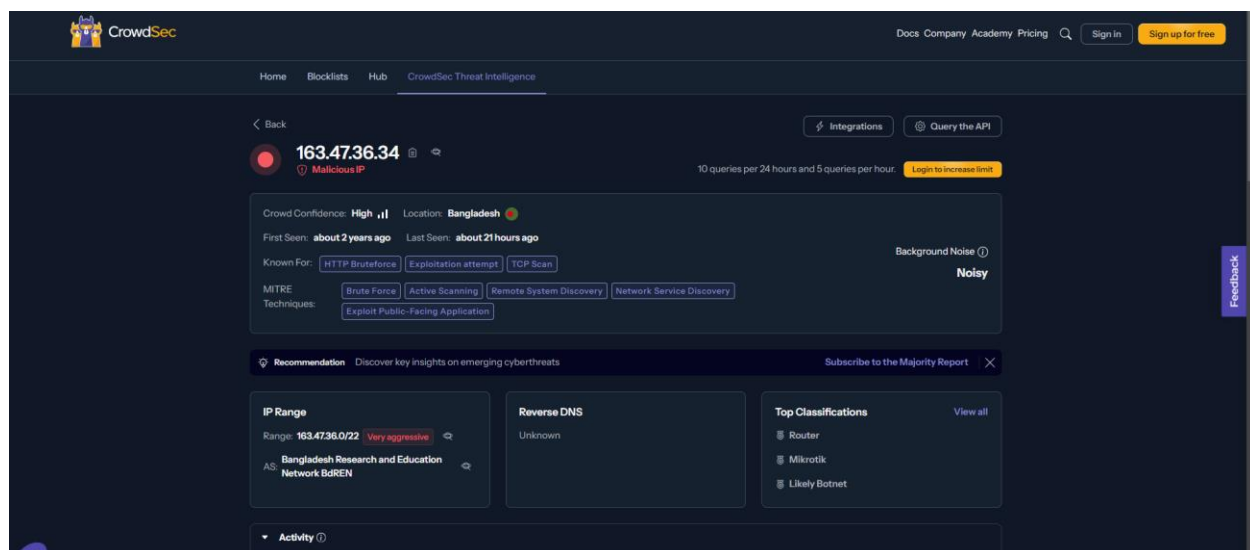


6. What TTPs do you observe?

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 brute force, TCP scanning, and exploitation attempts, likely linked to botnet activity.

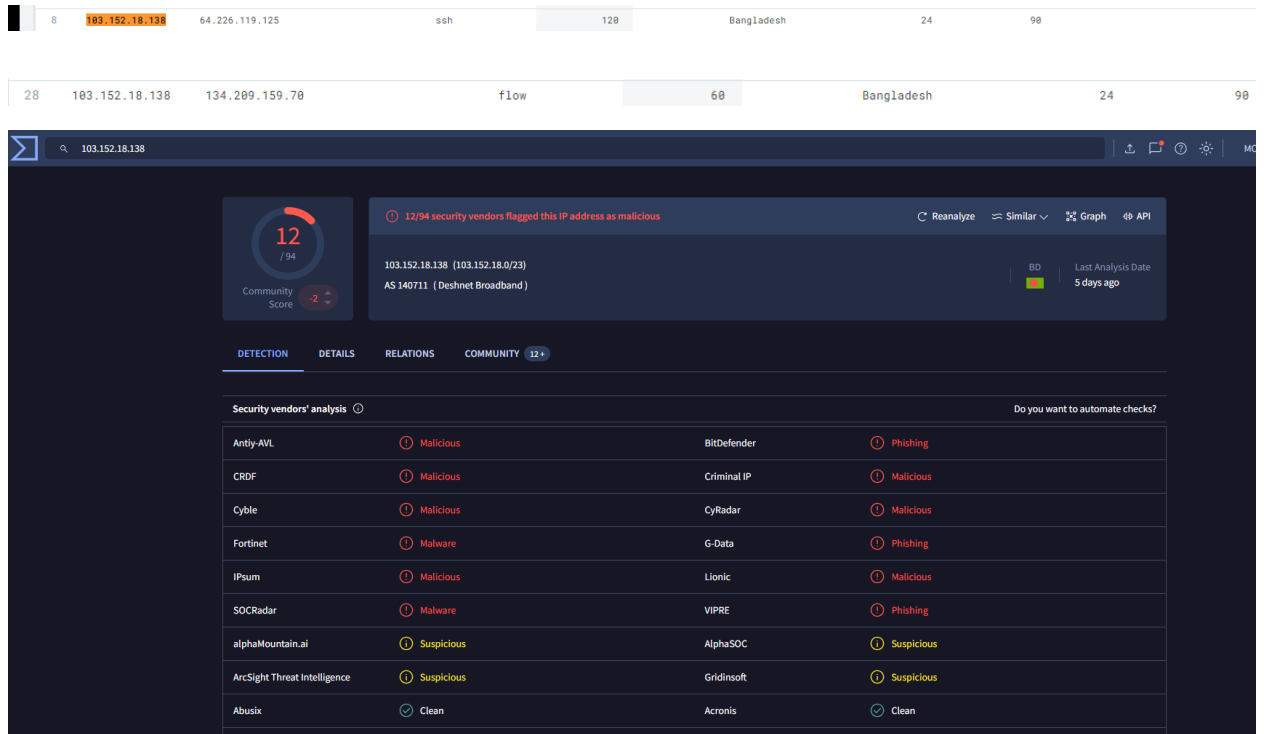


Event 6,8,28

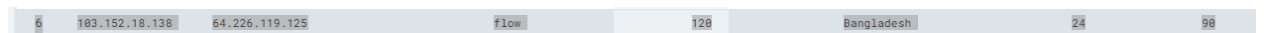
1. what is the source of the attack?

103.152.18.138

8	103.152.18.138	84.226.119.125	flow	120	Bangladesh	24	98
---	----------------	----------------	------	-----	------------	----	----

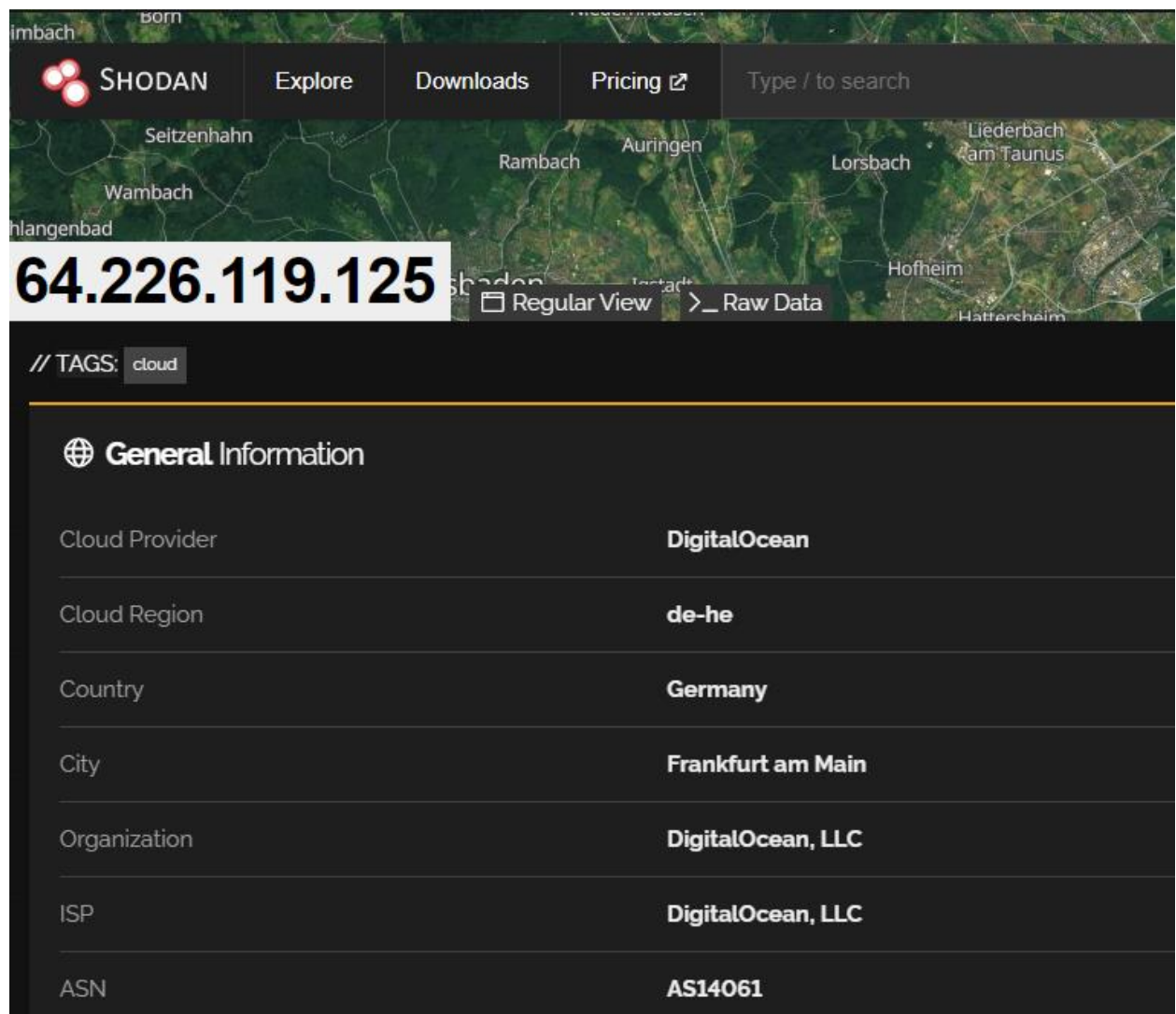


2. what are they attacking?



The destination IP in the logs is: 64.226.119.125

The destination IP in the logs is: 134.209.159.70



SHODAN Explore Downloads Pricing Type / to search

64.226.119.125 Regular View Raw Data

// TAGS: cloud

General Information

Cloud Provider	DigitalOcean
Cloud Region	de-he
Country	Germany
City	Frankfurt am Main
Organization	DigitalOcean, LLC
ISP	DigitalOcean, LLC
ASN	AS14061

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](#)

Check an IP Address, Domain Name, or Subnet
e.g. 174.91.211.236, microsoft.com, or 5.188.10.0/24

174.91.211.236

CHECK

103.152.18.138 was found in our database!

This IP was reported **15,925** times. Confidence of Abuse is **100%**: ?

100%

ISP	Deshnet Broadband
Usage Type	Fixed Line ISP
Domain Name	deshnetbd.com
Country	 Bangladesh
City	Rangpur, Rangpur

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

REPORT 103.152.18.138

WHOIS 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.

Docs Company Academy Pricing [Sign in](#) [Sign up for free](#)

[Home](#) [Blocklists](#) [Hub](#) [CrowdSec Threat Intelligence](#)

[Back](#) [Integrations](#) [Query the API](#)

103.152.18.138

Malicious IP

10 queries per 24 hours and 5 queries per hour. [Login to increase limit](#)

Crowd Confidence: **High**

Location: **Rangpur City, Bangladesh**

First Seen: **about 2 years ago**

Last Seen: **about 1 hour ago**

Known For: **SSH Bruteforce**

Background Noise: **Very Noisy**

MITRE Techniques: **Brute Force**

Gather Victim Identity Information

[Recommendation](#) Discover key insights on emerging cyberthreats [Subscribe to the Majority Report](#)

IP Range

Range: **103.152.18.0/23** **Aggressive**

AS: **Deshnet Broadband**

Reverse DNS

Unknown

Top Classifications

[View all](#)

CrowdSec Community Blocklist

Activity

Jul Aug Sep Oct

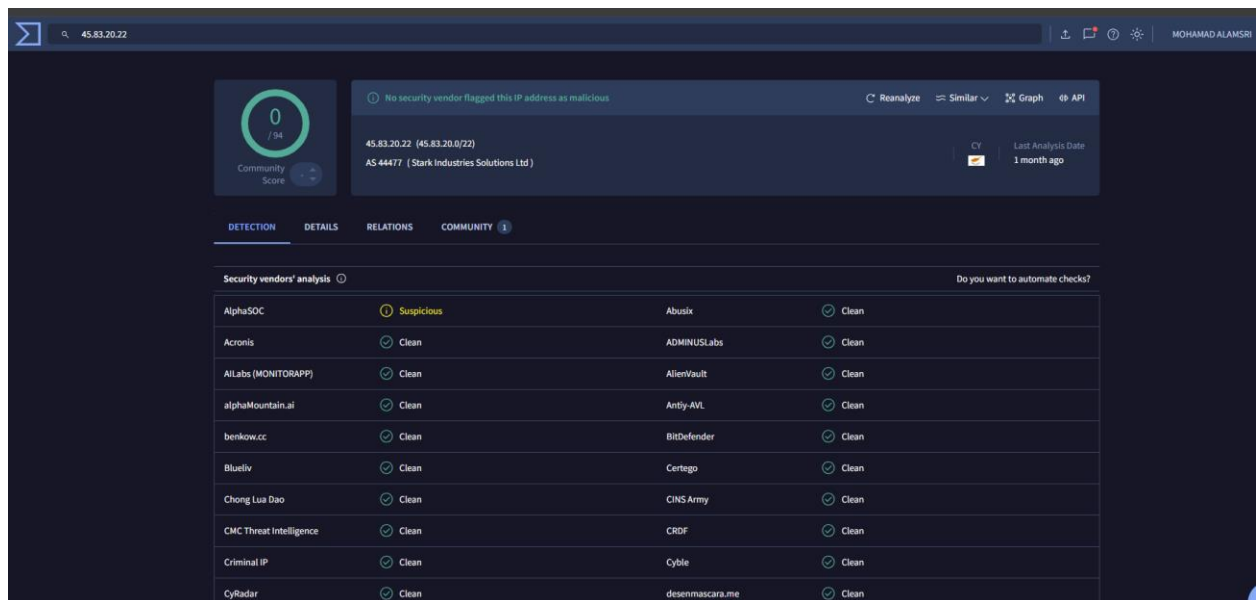
Last 24 hours Last month

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?


[Report IP](#)
[Bulk Reporter](#)
[Pricing](#)
[About](#)
[FAQ](#)
[Documentation](#)
[Statistics](#)
[IP Tools](#)
[Contact](#)

Check an IP Address, Domain Name, or Subnet
e.g. 174.91.211.236, microsoft.com, or 5.188.10.0/24

174.91.211.236

CHECK

45.83.20.22 was found in our database!

This IP was reported 32 times. Confidence of Abuse is 30%: ?

30%

ISP

LVNET Ltd

Usage Type

Data Center/Web Hosting/Transit

Hostname(s)

be1.multipn.pro

Domain Name

lvnet.lv

Country

 Bangladesh

City

Dhaka, Dhaka

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

REPORT 45.83.20.22

WHOIS 45.83.20.22

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	158	Dhaka	Bangladesh	23.8183	90.4125

6. What TTPs do you observe?

The screenshot shows the CrowdSec Threat Intelligence interface for the IP address 45.83.20.22. The interface is dark-themed and includes a navigation bar at the top with links to Home, Blocklists, Hub, and CrowdSec Threat Intelligence. The main content area displays the IP address 45.83.20.22 with a red circle icon and the label 'Malicious IP'. Below this, there is a section for 'Crowd Confidence' (None) and 'Location' (Cyprus). It also shows 'First Seen: about 2 months ago' and 'Last Seen: about 2 months ago'. The 'Known For' section lists 'HTTP Scan', 'HTTP Exploit', and 'CVE-2017-9841'. The 'MITRE Techniques' section lists 'Active Scanning' and 'Exploit Public-Facing Application'. There is a 'Recommendation' section with a link to 'Discover key insights on emerging cyberthreats'. The 'IP Range' section shows the range '45.83.20.0/22' with a link to 'A few reports'. The 'Reverse DNS' section shows 'belmultivpn.pro'. The 'Top Classifications' section shows 'Dangerous Services Exposed'. The interface also includes a 'Feedback' button on the right and a 'Subscribe to the Majority Report' link.

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

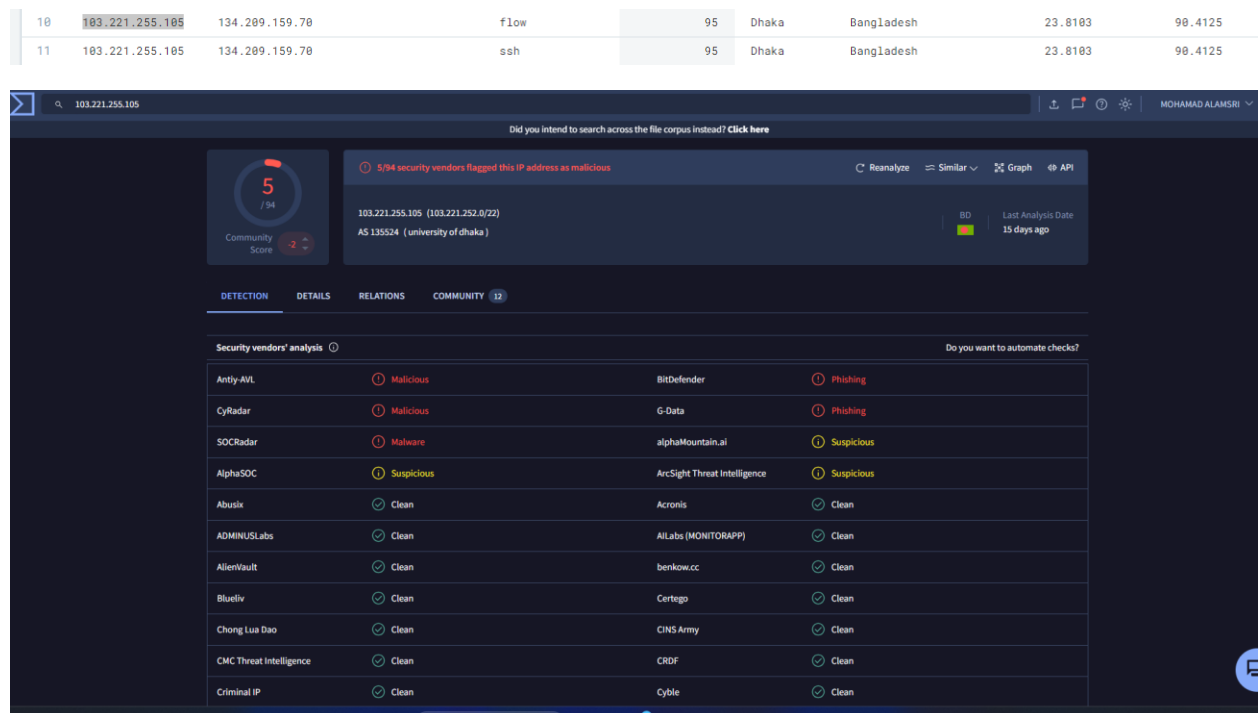
Active Scanning: Searching for vulnerabilities or open services.

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

**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.

SHODAN

Explore

Downloads

Pricing

Type / to search

134.209.159.70

Regular View Raw Data

Tags: cloud

General Information

Cloud Provider	DigitalOcean
Cloud Region	in-ka
Country	India
City	Doddaballapura
Organization	DigitalOcean, LLC
ISP	DigitalOcean, LLC
ASN	AS14061
Operating System	Linux

Open Ports

22 80

// 22 / TCP

OpenSSH 8.3p1 Ubuntu-3ubuntu0.6

```

SSH-2.0-OpenSSH_8.3p1_Ubuntu-3ubuntu0.6
Key type: ecdsa-sha2-nistp256
Key: AAAAE2VjZDh0LXN0YVY1I1b012dW9NTYAAAT0b12dW9NTYAAAB8B0u/wPvLLV3633R8ZSPW8
5qpcX5xyshv0gCwHfGba11wH323d8KPe5Jd6m60Cueg0Q0gta/Xf9q-
Fingerpr int: 0716b:cd:a7:731e2:ac184:db:581b:541d8:23183:es

Kex Algorithms:
curve25519-sha256
curve25519-sha256@libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
sh256pV1412519-sha256@openssh.com
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha256
diffie-hellman-group18-sha256
diffie-hellman-group14-sha256
new-trust

```

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

 AbuseIPDB

[Home](#) [Report IP](#) [Bulk Reporter](#) [Pricing](#) [About](#) [FAQ](#) [Documentation](#) [Statistics](#) [IP Tools](#) [Contact](#)

174.91.211.236

CHECK

103.221.255.105 was found in our database!

This IP was reported 13,420 times. Confidence of Abuse is 14% ?

14%

ISP

University of Dhaka

Usage Type

University/College/School

Domain Name

du.ac.bd

Country

 Bangladesh

City

Dhaka, Dhaka

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

Updated monthly.

REPORT 103.221.255.105

WHICH 103.221.255.105

IP Abuse Reports for 103.221.255.105:

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	23.8845	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.

The screenshot shows the CrowdSec Threat Intelligence interface for the IP address 103.221.255.105. The interface is dark-themed and includes a navigation bar at the top with links to Home, Blocklists, Hub, and CrowdSec Threat Intelligence. The main content area displays the IP address 103.221.255.105, marked as a 'Malicious IP'. Below this, there is a section for 'Crowd Confidence' (None) and 'Location' (Dhaka, Bangladesh). It also shows 'First Seen' (about 1 year ago) and 'Last Seen' (about 1 month ago). A 'Known For' section lists 'SSH Bruteforce' as a technique. The 'MITRE Techniques' section includes 'Brute Force' and 'Gather Victim Identity Information'. A 'Recommendation' section suggests discovering key insights on emerging cyberthreats. The 'IP Range' section shows the range 103.221.252.0/22, with the AS identified as 'university of dhaka'. The 'Reverse DNS' section is unknown. The 'Top Classifications' section shows no classifications found for this IP. The interface also includes a 'Feedback' button on the right and a 'Subscribe to the Majority Report' link.

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.

SHODAN Explore Downloads Pricing Type / to search

134.209.159.70 Regular View Raw Data

// TAGS: cloud

General Information

Cloud Provider	DigitalOcean
Cloud Region	in-ka
Country	India
City	Doddaballapura
Organization	DigitalOcean, LLC
ISP	DigitalOcean, LLC
ASN	AS14061
Operating System	Linux

Open Ports

// 22 / TCP

OpenSSH 8.9p1 Ubuntu:Ubuntu.6

SSH-2.0-openssh_8.9p1 Ubuntu:Ubuntu.6

Key types: ecdsa-sha2-nistp256

Key: AAAAC3Q3dHhUJ0vY1tbt1dHhYNTAAATbtl2dHhYNTAAAB880U/w7V/LVaE330REZ5Hms

Spqc5k5q5h0v0GcW8g8aZLh3x23ARHkP5j6eMb0CuegDq0G5A/Xf3Q+

Fingerprint: 67168:cd:a7173:e2:ac:64:db:58:bb:54:ds:23:88:e5

Key Algorithms:

- curve25519-sha256
- curve25519-sha256@libssh.org
- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- sntrup761x25519-sha512@openssh.com
- diffie-hellman-group-exchange-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512
- diffie-hellman-group14-sha256
- key-strict-s-van@openssh.com

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.

The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with links: Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. The main header displays 'AbuseIPDB » 103.26.136.173'. Below this, a search bar contains the IP address '174.91.211.236' and a 'CHECK' button. The results section indicates that '103.26.136.173 was found in our database!' and shows a 'Confidence of Abuse' of 100%. A table lists the following details:

ISP	Grameen Communications
Usage Type	Fixed Line ISP
Hostname(s)	mail.gshakti.org
Domain Name	grameencommunications.org
Country	Bangladesh
City	Mirzapur, Dhaka

Below the table, it states 'IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.' At the bottom, there are two buttons: 'REPORT 103.26.136.173' and 'WHICH 103.26.136.173'. A footer note reads 'IP Abuse Reports for 103.26.136.173:'.

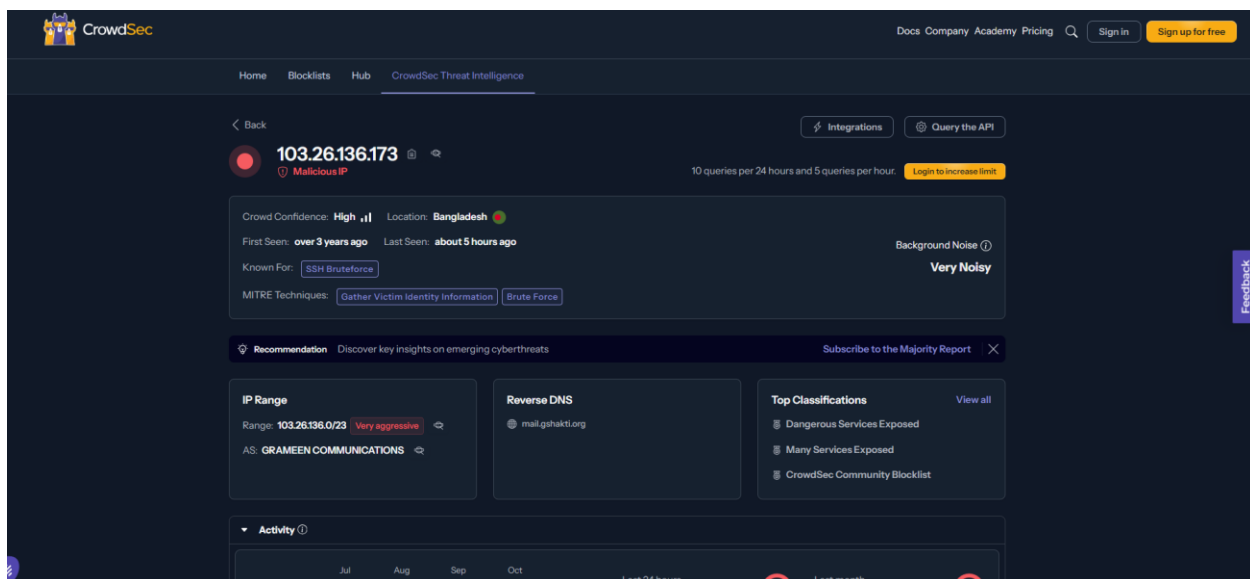
5. What is the event type?

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 attacks 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:

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

SHODAN

Explore

Downloads

Pricing &

Type / to search

134.209.159.70

Regular View

< Raw Data

// TAGS

cloud

General Information

Cloud Provider

DigitalOcean

Cloud Region

in-ka

Country

India

City

Doddabailapura

Organization

DigitalOcean, LLC

ISP

DigitalOcean, LLC

ASN

AS14061

Operating System

Linux

Vulnerabilities

All ports

Latest

Open Ports

22

80

// 22 / TCP

OpenSSH 8.3p1 Ubuntu-3ubuntu0.6

SSH-2.0-OpenSSH_8.3p1_Ubuntu-3ubuntu0.6

key type: ecdsa-sha2-nistp256

Key: AAAAEVjZmhlLnwvT1tblzdwYNTYAAADbdlzdwYNTYAAABSSUw/dTULVLE3B3REZPNfMS5qpcx5y5h9wGdWd9gob3k3WATA3d88w5j5j6wducUepQoZg8r/KFqg

Fingerprints: 87f68cd8773e22ac184db56198594682338es

KEX Algorithms:

curve25519-sha256

curve25519-sha256@libssh.org

ecdh-sha2-nistp256

ecdh-sha2-nistp384

ecdh-sha2-nistp2561

sntrup761x25519-sha512@openssh.com

diffie-hellman-group-exchange-sha256

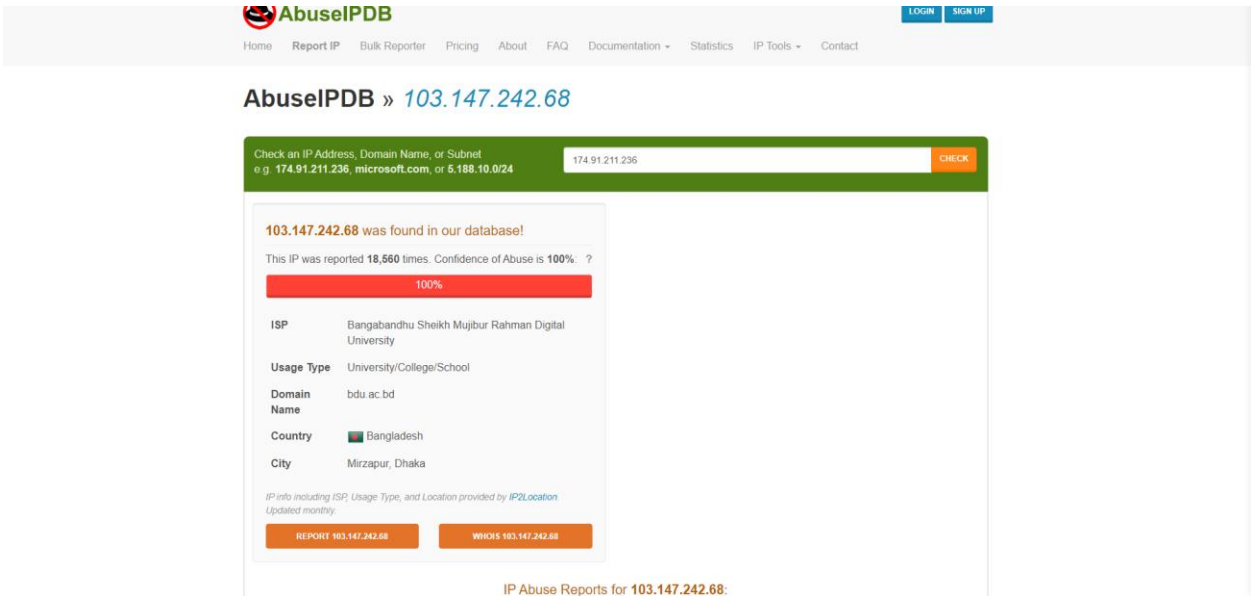
diffie-hellman-group1-sha512

diffie-hellman-group1-sha256

diffie-hellman-group1-sha256

hmac-sha1@openssh.com

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.

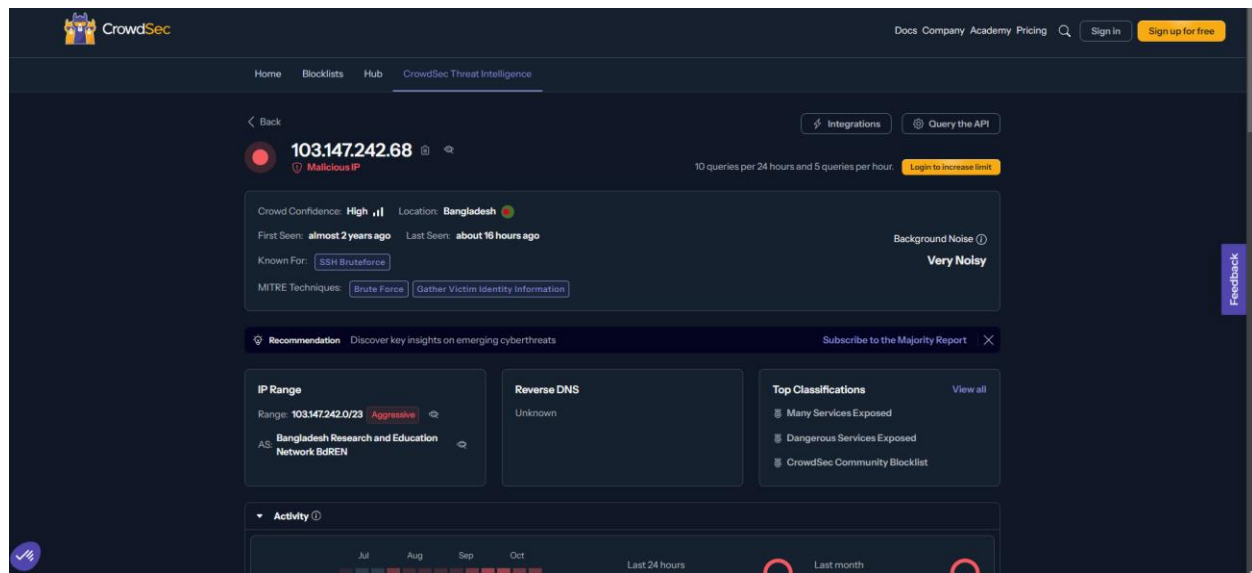
12	103.147.242.68	134.209.159.70	ssh	91	Bangladesh	24	90
13	103.147.242.68	134.209.159.70	flow	91	Bangladesh	24	90

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

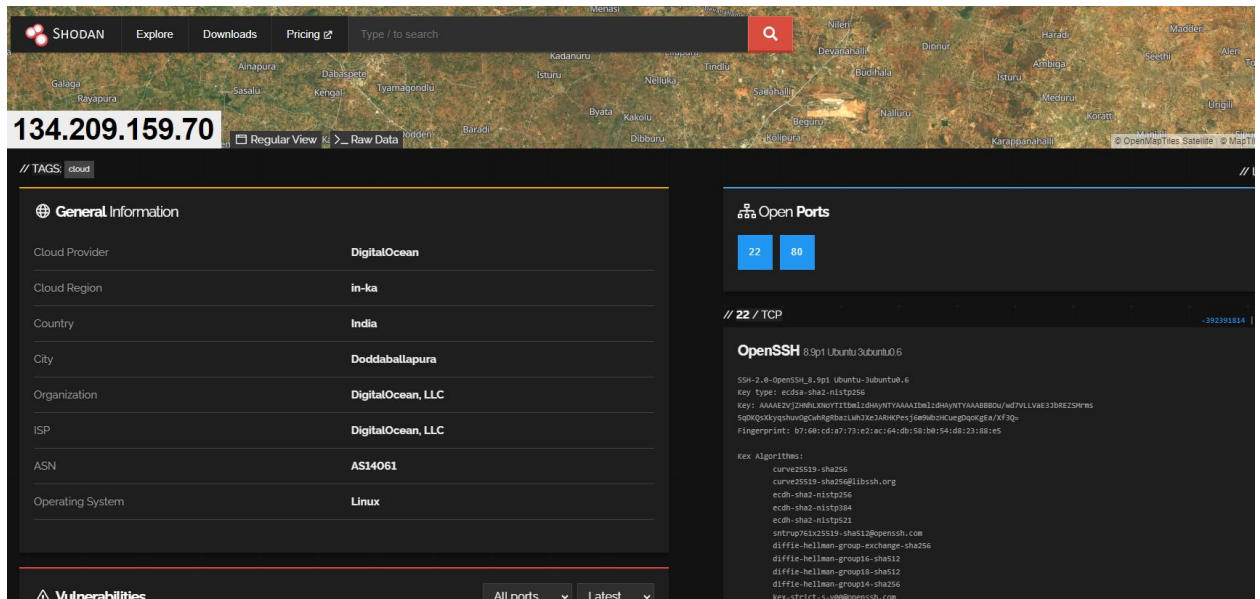
3. Why is the target being attacked?

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.

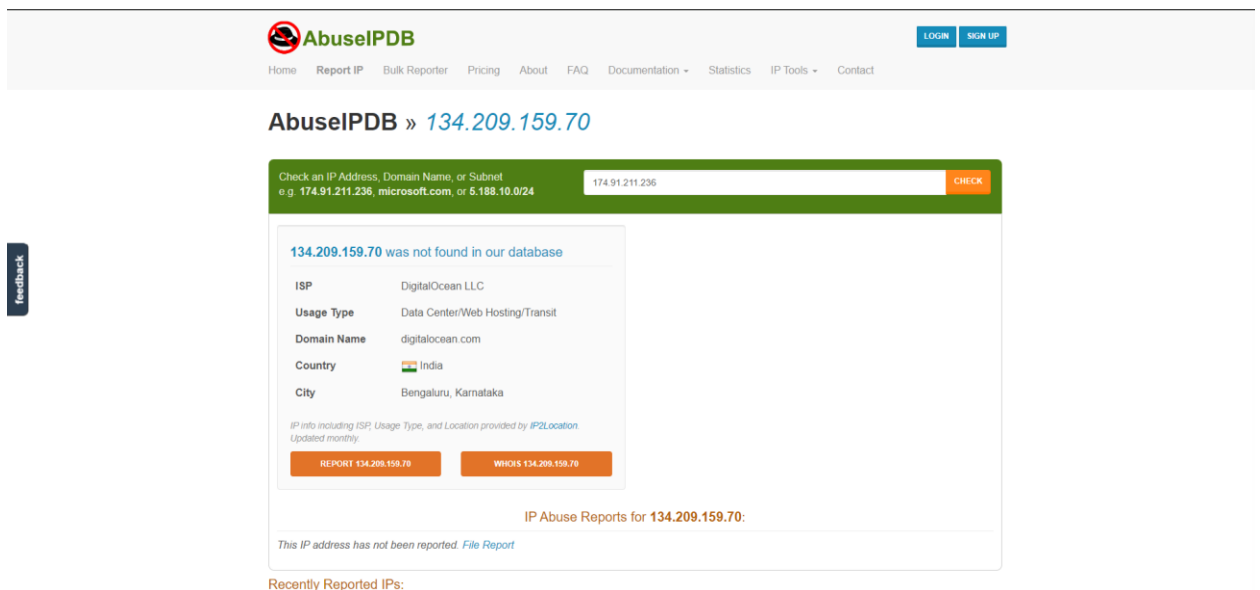
being attacked because:

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.



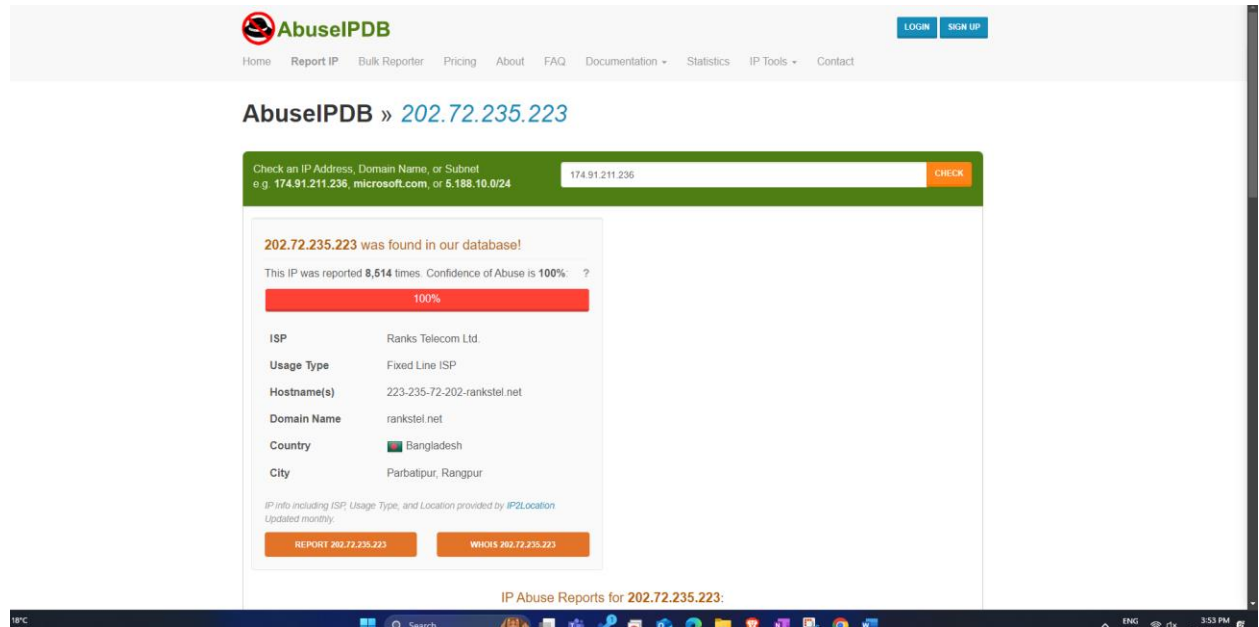
The screenshot shows the SHODAN search results for the IP address 134.209.159.70. The interface includes a search bar at the top with the IP entered. Below the search bar, there is a map showing the location of the IP. The main section displays general information about the IP, including the cloud provider (DigitalOcean), region (in-ka), country (India), city (Doddaballapura), organization (DigitalOcean, LLC), ISP (DigitalOcean, LLC), ASN (AS14061), and operating system (Linux). On the right side, there is a section for open ports, showing ports 22 and 80. Below the ports, there is a section for TCP connections, showing an OpenSSH connection to a Ubuntu 16.04 server. The OpenSSH section includes details such as the SSH version (2.8), key type (ecdsa-sha2-nistp256), key, fingerprint, and Kex Algorithms.



The screenshot shows the AbuseIPDB search results for the IP address 134.209.159.70. The interface includes a search bar at the top with the IP entered. Below the search bar, there is a section for IP information, including the ISP (DigitalOcean LLC), usage type (Data Center/Web Hosting/Transit), domain name (digitalocean.com), country (India), and city (Bengaluru, Karnataka). Below the IP information, there is a section for IP abuse reports, showing that the IP has not been reported. At the bottom, there is a section for recently reported IPs.

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.

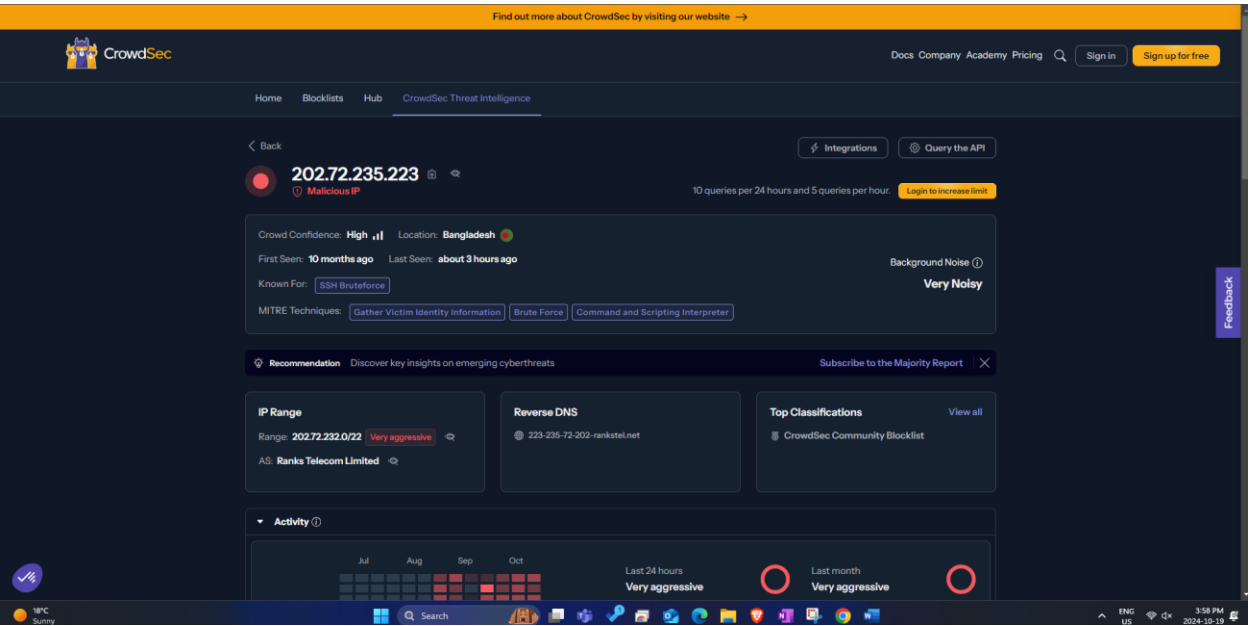
6. What TTPs do you observe?

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.

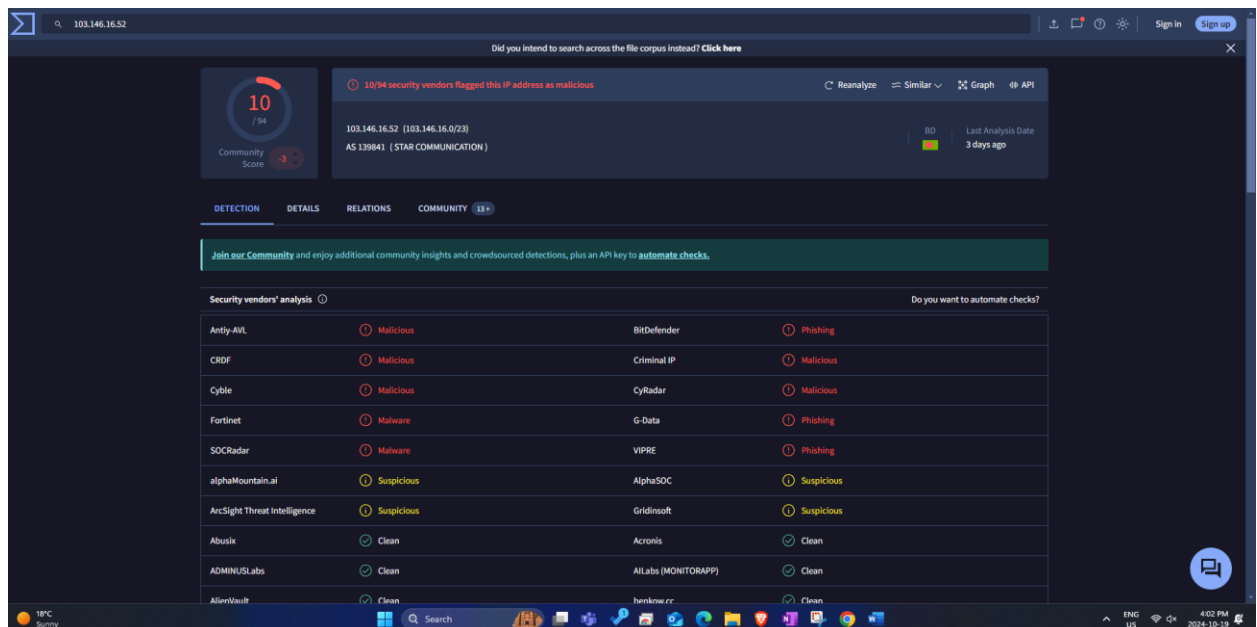


Event 15,19

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.

 **AbuselPDB**

[Home](#) [Report IP](#) [Bulk Reporter](#) [Pricing](#) [About](#) [FAQ](#) [Documentation](#) [Statistics](#) [IP Tools](#) [Contact](#)

[LOGIN](#) [SIGN UP](#)

Check an IP Address, Domain Name, or Subnet
e.g. 174.91.211.236, microsoft.com, or 5.188.10.0/24

174.91.211.236

134.209.159.70 was not found in our database

ISP	DigitalOcean LLC
Usage Type	Data Center/Web Hosting/Transit
Domain Name	digitalocean.com
Country	India
City	Bengaluru, Karnataka

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

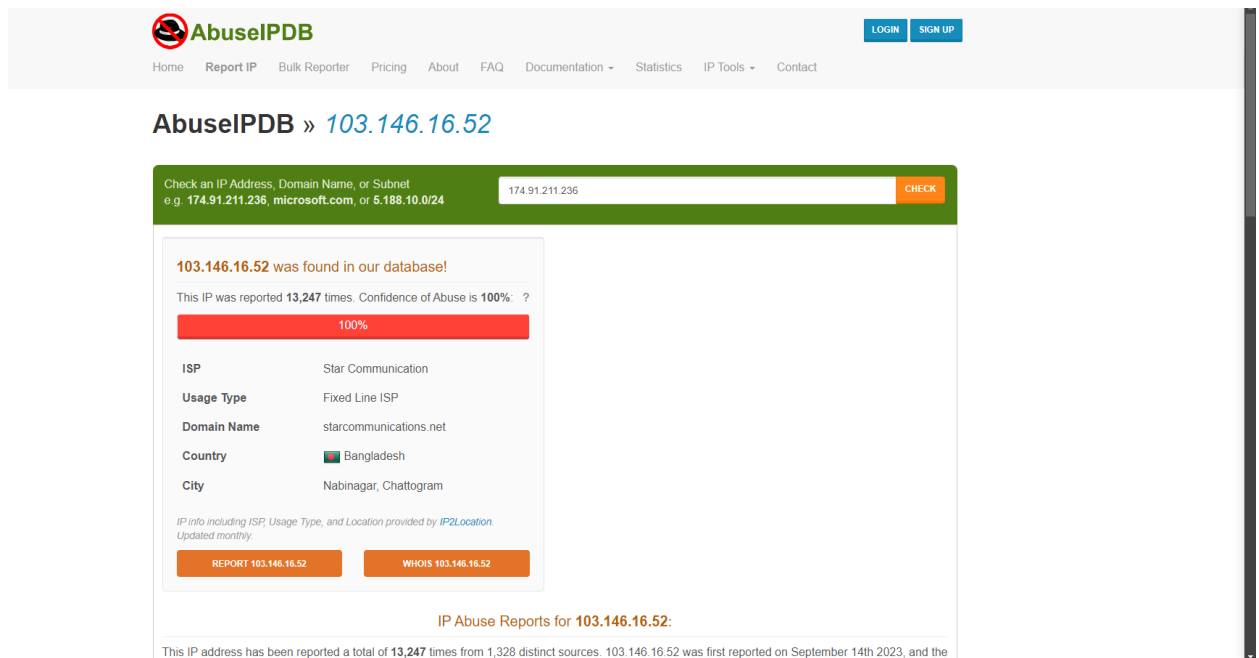
[REPORT 134.209.159.70](#) [WHOSIS 134.209.159.70](#)

IP Abuse Reports for 134.209.159.70:

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

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.



The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with links: Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. The main header displays the AbuseIPDB logo and a search bar. Below the search bar, the results for IP 103.146.16.52 are shown. A green banner at the top of the results section states "103.146.16.52 was found in our database!". Below this, a red bar indicates "100%" confidence of abuse. The results are organized into a table with the following information:

Field	Value
ISP	Star Communication
Usage Type	Fixed Line ISP
Domain Name	starcommunications.net
Country	Bangladesh
City	Nabinagar, Chattogram

Below the table, there is a note: "IP info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly." At the bottom of the results section, there are two buttons: "REPORT 103.146.16.52" and "WHOIS 103.146.16.52".

5. What is the event type?

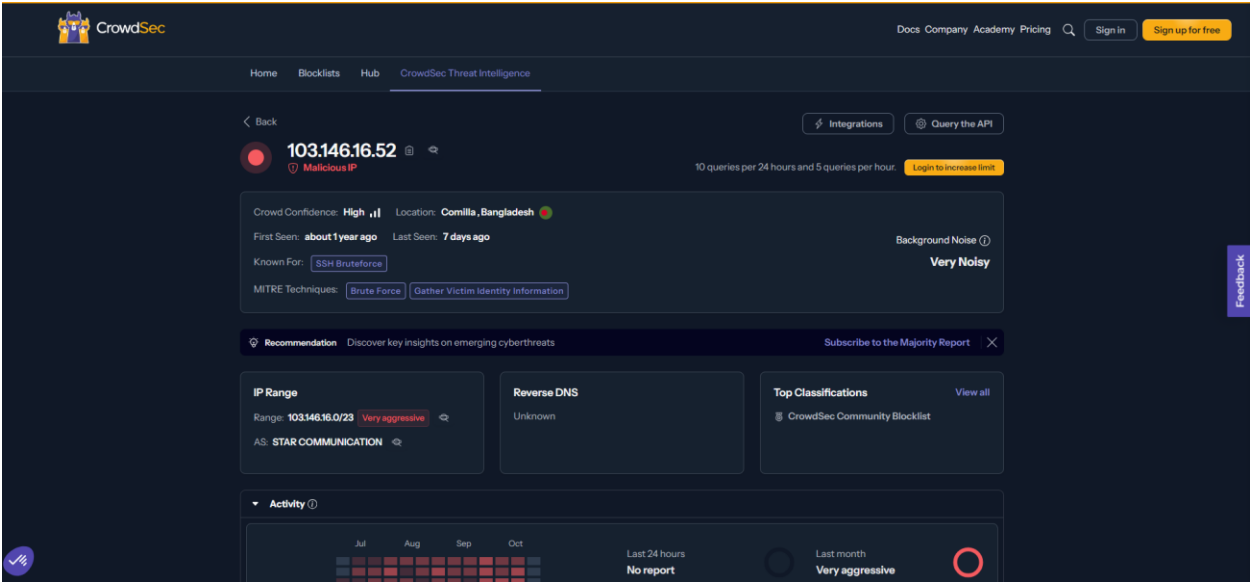
1. the event type is **flow**, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is **SSH** for the IP 103.146.16.52 it means that this IP is attempting to connect to the target system using 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.

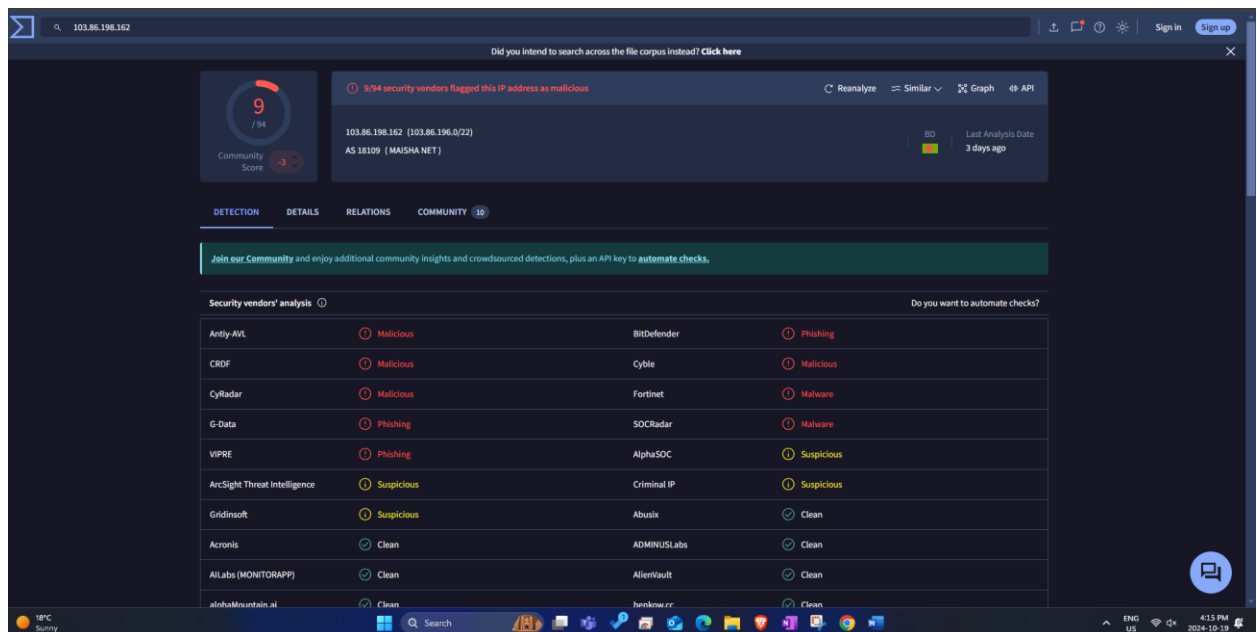


Event 17,18

1. what is the source of the attack?

103.86.198.162

17	103.86.198.162	134.289.159.78	flow	98	Dhaka	Bangladesh	23.8183	98.4125
18	103.86.198.162	134.289.159.78	ssh	98	Dhaka	Bangladesh	23.8183	98.4125



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?

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.

The screenshot shows the CrowdSec Threat Intelligence interface for the IP address 103.86.198.162. The interface is dark-themed and includes the following information:

- IP Address:** 103.86.198.162 (labeled as Malicious IP)
- Location:** Bangladesh
- Crowd Confidence:** High
- First Seen:** 9 months ago
- Last Seen:** 7 days ago
- Known For:** SSH Bruteforce
- MITRE Techniques:** Brute Force, Gather Victim Identity Information
- Background Noise:** Very Noisy
- Recommendation:** Discover key insights on emerging cyberthreats
- IP Range:** Range: 103.86.196.0/22 (Aggressive), AS: MAISHA.NET
- Reverse DNS:** host162.maishabd.net
- Top Classifications:** CrowdSec Community Blocklist
- Activity:** A calendar view showing activity from July to October. The last 24 hours show "No report", and the last month shows "Very aggressive".

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.

SHODAN

Explore

Downloads

Pricing

Type / to search

134.209.159.70

☐ Regular View
 ☒ Raw Data

// TAGS: cloud

General Information

Cloud Provider	DigitalOcean
Cloud Region	in-ka
Country	India
City	Doddaballapura
Organization	DigitalOcean, LLC
ISP	DigitalOcean, LLC
ASN	AS14061
Operating System	Linux

Open Ports

22

80

// 22 / TCP

OpenSSH 8.9p1 Ubuntu:Ubuntu0.6

```

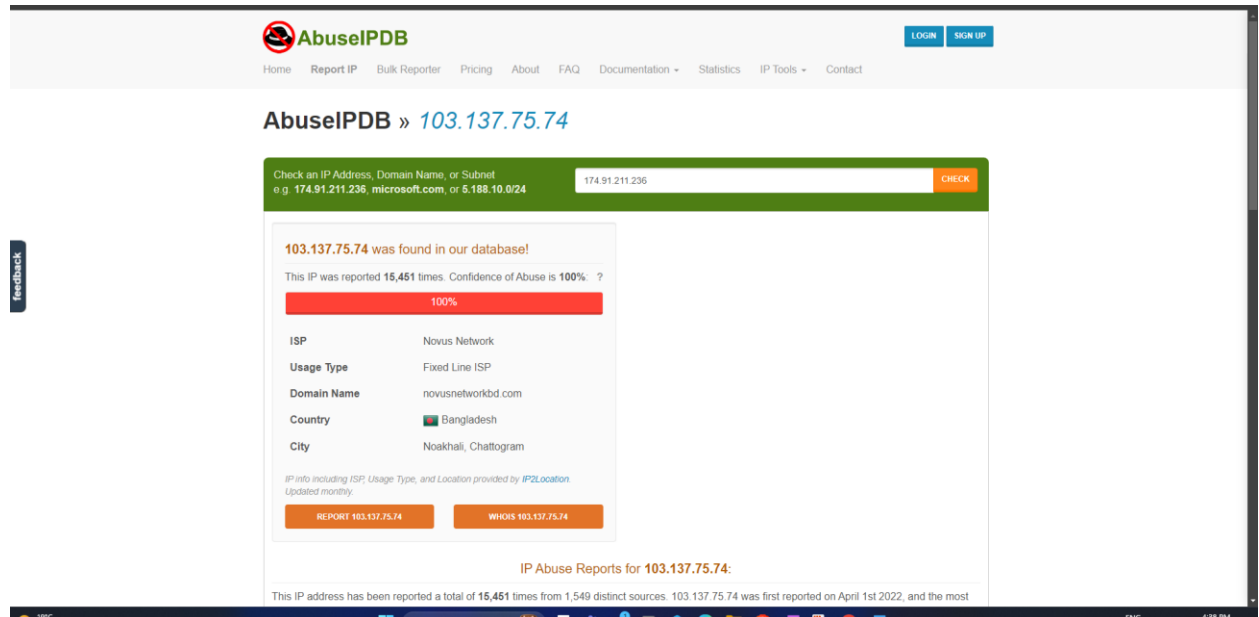
SSH-2.0-OpenSSH_8.9p1_Ubuntu-0ubuntu0.6
Key Type: ecdsa-sha2-nistp256
Key: AAAAE2VjZDh0LmR0b3VIT1B1dWYNTYAAAB1dWYNTYAAABBBBw/wFvLLVME3DREZSPfms
5p9xkxyshovQCaHgftBz1sh3x2A8KPe5Jem6zhCuegqogfA/XfQ=
Fingerprint: 87f68:cd:a7f73:e2:ac:64:db:58:08:54:d8:23:88:e5

Key Algorithms:
curve25519-sha256
curve25519-sha256libssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
sntrup761x25519-sha512@openssh.com
diffie-hellman-group-exchange-sha256
diffie-hellman-group1-sha512
diffie-hellman-group18-sha512
diffie-hellman-group14-sha256

```

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?

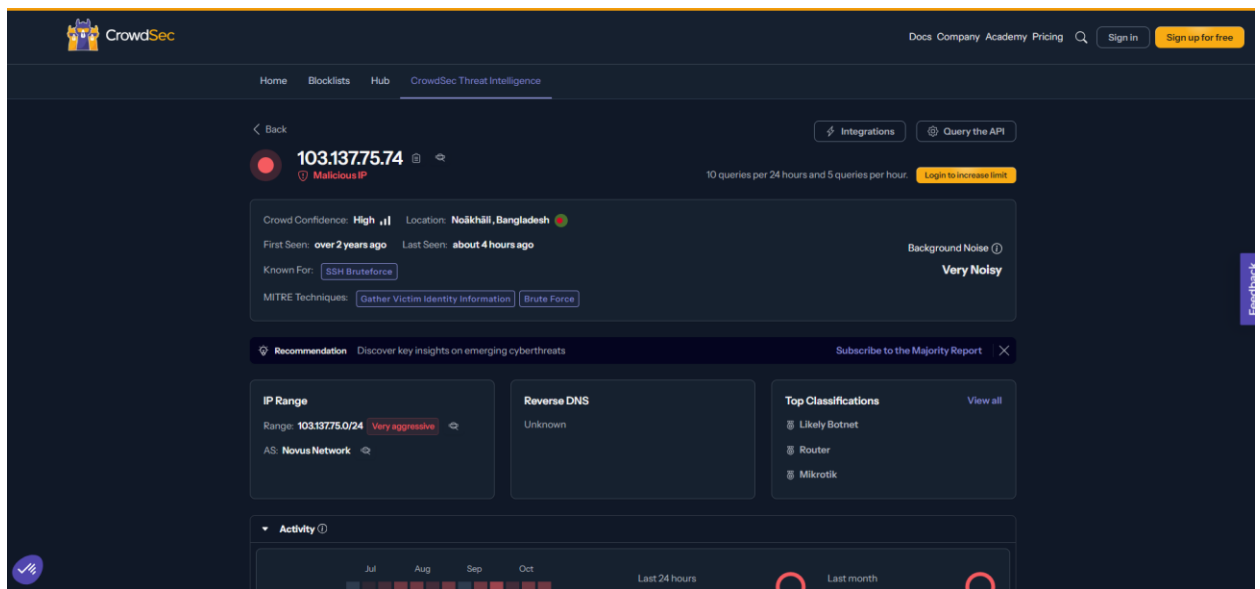
1. the event type is **flow**, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is **SSH** for the IP 103.137.75.74 it means that this IP is attempting to connect to the target system using 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.

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

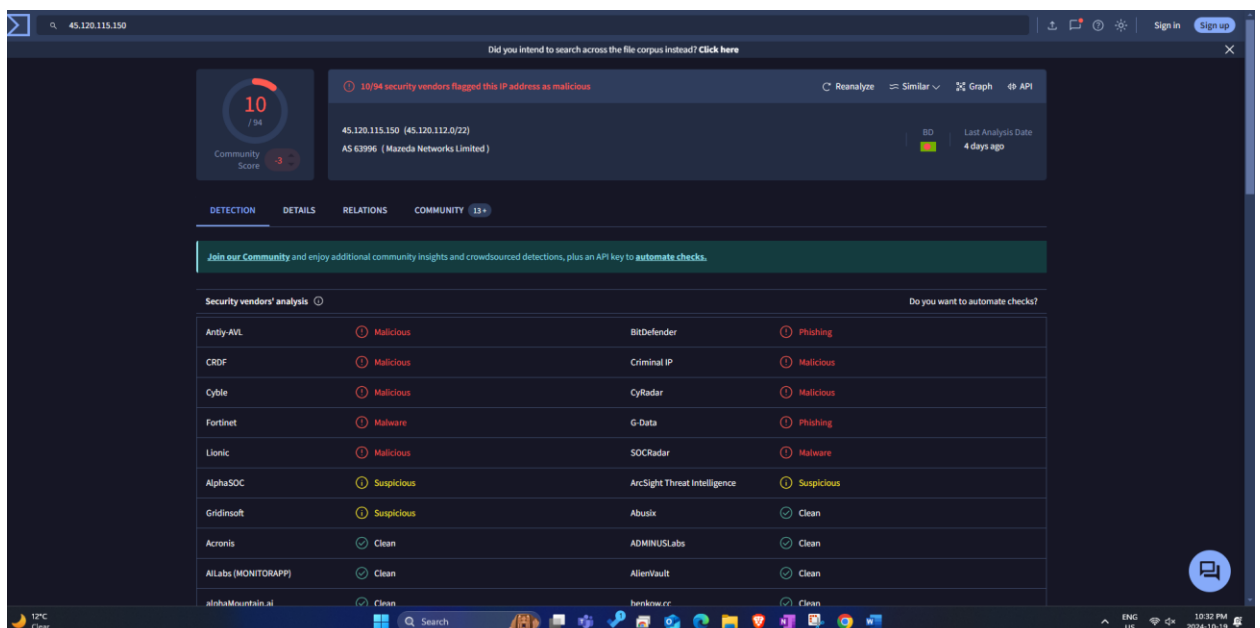
This IP is labeled as very noisy and aggressive, consistently involved in SSH bruteforce activity.



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.

The screenshot shows the SHODAN search results for the IP address 134.209.159.70. The interface includes a map at the top showing the location of the IP in India. Below the map, the IP address is displayed in a large font. To the right of the IP, there are buttons for 'Regular View' and 'Raw Data'. Below this, there is a section titled 'General Information' with a table of details:

General Information	
Cloud Provider	DigitalOcean
Cloud Region	in-ka
Country	India
City	Doddaballapura
Organization	DigitalOcean, LLC
ISP	DigitalOcean, LLC
ASN	AS14061
Operating System	Linux

To the right of the 'General Information' table, there is a section titled 'Open Ports' showing the ports 22 and 80. Below this, there is a section titled 'OpenSSH' showing the SSH configuration details:

```
SSH-2.0-OpenSSH_8.3p1 Ubuntu-3ubuntu0.6
key type: ecdsa-sha2-nistp256
key: AAAAEZvJ2wHLKwV7T1bL1dHvNTYAAAIbL1dHvNTYAAABBBwId7VLLVE33BEEZ3Pms
5pXqSKyqshuvGqCnHgBacLwH323d8KPe5j6w6bzCuegDqg6A/MF3q=
Fingerprint: 87:68:cd:47:73:e2:ac:64:db:58:1b:54:db:23:88:e5

Kex Algorithms:
curve25519-sha256
curve25519-sha256glibssh.org
ecdh-sha2-nistp256
ecdh-sha2-nistp384
ecdh-sha2-nistp521
untrap761x25519-sha512@openssh.com
diffie-hellman-group-exchange-sha256
diffie-hellman-group16-sha512
diffie-hellman-group14-sha256
kex-strict-s-van@openssh.com
```

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

The IP 45.120.115.150 belongs to Mazed 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.

AbuseIPDB » 45.120.115.150

Check an IP Address, Domain Name, or Subnet
e.g. 174.91.211.236, microsoft.com, or 5.188.10.0/24

174.91.211.236

CHECK

45.120.115.150 was found in our database!

This IP was reported 15,475 times. Confidence of Abuse is 100% ?

100%

ISP

Mazeda Networks Limited

Usage Type

Fixed Line ISP

Hostname(s)

45.120.115-150.mazedanetworks.net

Domain Name

mazedabd.com

Country

 Bangladesh

City

Dhaka, Dhaka

IP info including ISP, Usage Type, and Location provided by IP2Location
Updated monthly.

REPORT 45.120.115.150

WHOIS 45.120.115.150

IP Abuse Reports for 45.120.115.150:

This IP address has been reported a total of 15,475 times from 1,510 distinct sources. 45.120.115.150 was first reported on August 24th 2022, and the most recent report was 1 week ago.

Old Reports: The most recent abuse report for this IP address is from 1 week ago. It is possible that this IP is no longer involved in abusive activities.

5. What is the event type?

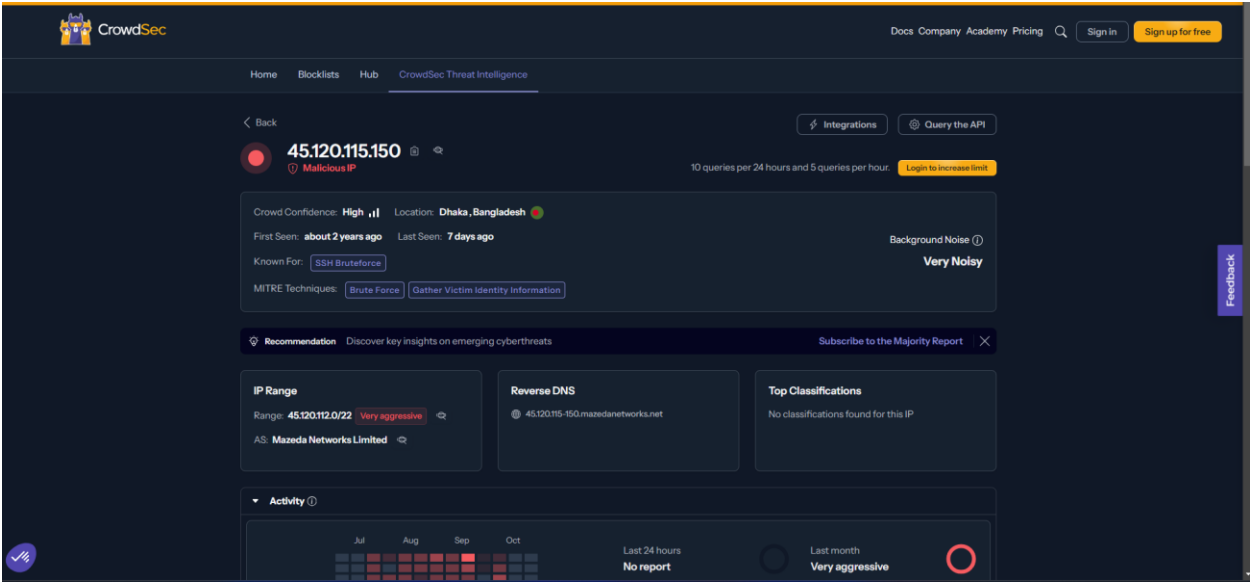
1. the event type is **flow**, which refers to network traffic monitoring. In this case, it is tracking the flow of packets between the source and destination IP addresses.
2. The event type is **SSH** for the IP 45.120.115.150 it means that this IP is attempting to connect to the target system using 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.

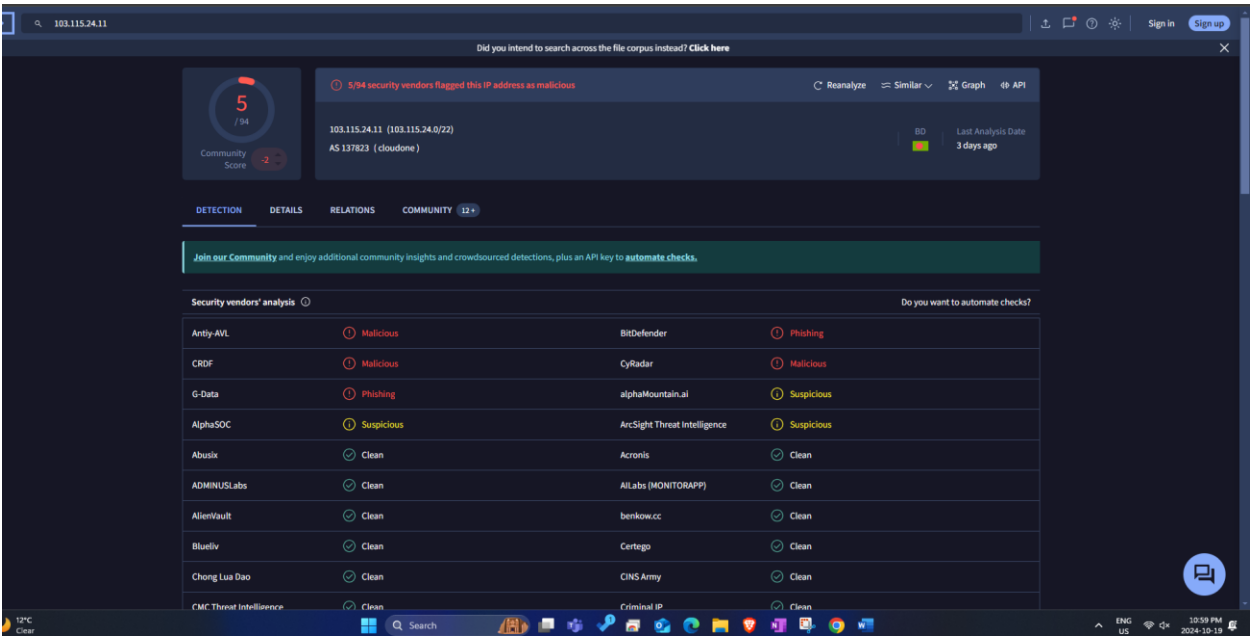


Event 26,27

1. what is the source of the attack?

103.115.24.11

26	103.115.24.11	134.209.159.78	flow	61	Bangladesh	24	98
27	103.115.24.11	134.209.159.78	ssh	61	Bangladesh	24	98



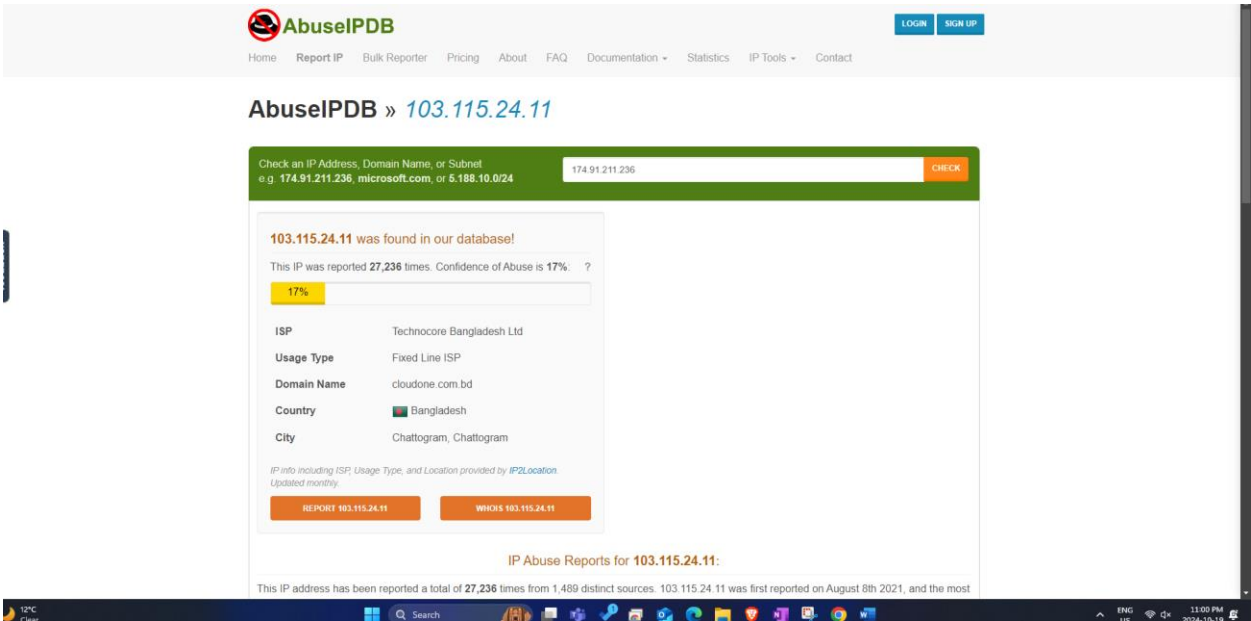
3. Why is the target being attacked?

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.

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

[illegible]

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.

The screenshot shows the CrowdSec Threat Intelligence page for the IP address 103.115.24.11. The interface is dark-themed and includes a navigation bar at the top with links to Home, Blocklists, Hub, and CrowdSec Threat Intelligence. The main content area displays the IP address with a red circle icon and the label 'Malicious IP'. Below this, there are several sections: 'Crowd Confidence' (None), 'Location' (Chittagong, Bangladesh), 'First Seen' (about 3 years ago), 'Last Seen' (3 months ago), 'Known For' (SSH Bruteforce, Exploitation attempt), and 'MITRE Techniques' (Brute Force, Exploit Public-Facing Application, Active Scanning, Command and Scripting Interpreter, Gather Victim Identity Information). A 'Recommendation' section suggests discovering key insights on emerging cyberthreats. Below this, there are three boxes: 'IP Range' (Range: 103.115.24.0/22, Very aggressive, AS: cloudone), 'Reverse DNS' (Unknown), and 'Top Classifications' (Dangerous Services Exposed, Many Services Exposed). At the bottom, there is an 'Activity' section with a calendar view showing 'No report' for the last 24 hours and 'No report' for the last month.

Event 29

1. what is the source of the attack?

103.152.18.138

The screenshot shows the VirusShare interface for the IP address 103.4.145.50. The interface is dark-themed and includes a navigation bar at the top with links to Home, Blocklists, Hub, and VirusShare. The main content area displays the IP address with a red circle icon and the label 'Malicious IP'. Below this, there are several sections: 'Community Score' (11/54), 'Security vendors' analysis' (a table of vendor detections), and 'Do you want to automate checks?'. The 'Security vendors' analysis table lists various vendors and their detection results for the IP address.

Vendor	Detection	Vendor	Detection
Antiy-AVL	Malicious	BitDefender	Phishing
CRDF	Malicious	Criminal IP	Malicious
Cyble	Malicious	CyRadar	Malicious
Fortinet	Malware	G-Data	Phishing
IPsum	Malicious	SOCradar	Malware
VIPRE	Phishing	alphaMountain.ai	Suspicious
ArcSight Threat Intelligence	Suspicious	Gridinsoft	Suspicious
Abusix	Clean	Acronis	Clean
ADMINUS Labs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	hmnkwa.cc	Clean

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.

The screenshot shows the AbuseIPDB website interface. At the top, there's a navigation bar with the AbuseIPDB logo and links for Home, Report IP, Bulk Reporter, Pricing, About, FAQ, Documentation, Statistics, IP Tools, and Contact. There are also LOGIN and SIGN UP buttons. Below the navigation bar, the main heading reads "AbuseIPDB » 103.4.145.50". A search bar is present with the text "Check an IP Address, Domain Name, or Subnet" and a "CHECK" button. Below the search bar, a message states "103.4.145.50 was found in our database!". A bar chart shows "This IP was reported 17,977 times. Confidence of Abuse is 100%". Below this, a table lists details: ISP (Plot 325 Lane 22 New DOHS), Usage Type (Fixed Line ISP), Domain Name (nextonline.com.bd), Country (Bangladesh), and City (Dhaka, Dhaka). At the bottom, there are buttons for "REPORT 103.4.145.50" and "WHOIS 103.4.145.50". A footer note says "IP Abuse Reports for 103.4.145.50".

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

