TZ-CERT HONEYPOT WEEKLY REPORT

Period: 24th – 30th August 2026 | **Report No.:** TZ-CERT/WRHP/2026/35

01: WEEKLY ATTACK SUMMARY

94,047	214,020	41,359	1,280
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 64.1% vs last week	↑ 777.6% vs last week	↑ 49.6% vs last week	↑ 45.6% vs last week

A total of 94,047 network attacks were recorded across all sensors during the period 24th – 30th August 2026, representing an overall increase of 64.1% compared to last week's 57,314 attacks. While network and malware activity increased, web attacks increased significantly by 49.6% and ICS attacks rose by 45.6%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

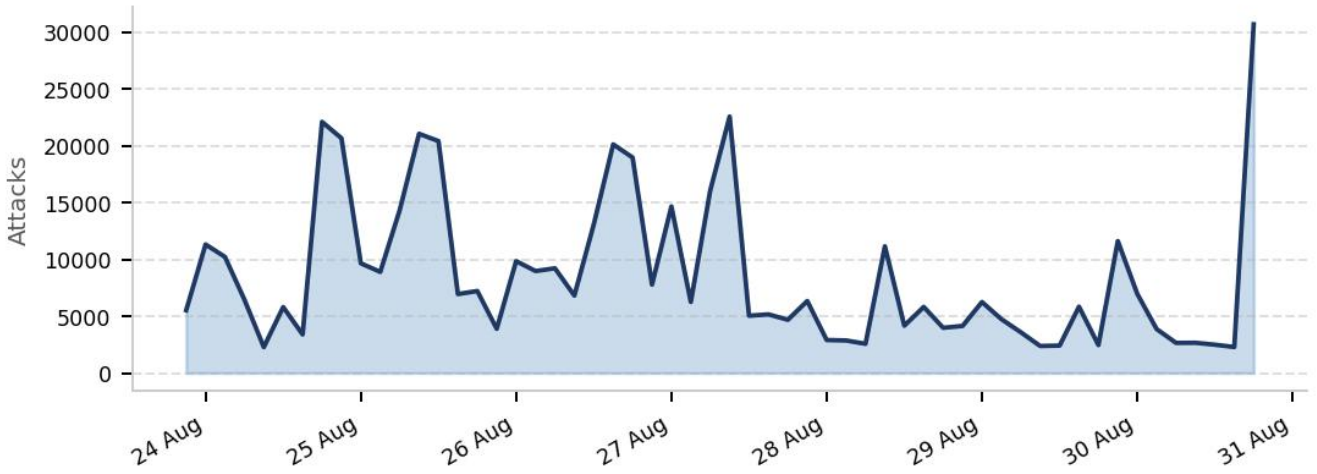

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 94,047 attacks have been recorded, up from last week's 57,314 by 64.1%. The top 10 attacking IPs with commonly exploited credentials are listed below. Most credentials used are default or weak — enforcement of password policies is strongly advised.

SN	ATTACKING IP	USERNAME USED	PASSWORD USED
1.	45.153.34.71	root	admin

2.	94.154.35.215	admin	123456
3.	91.92.42.126	user	0
4.	91.92.42.36	0	1234
5.	85.11.167.127	ubuntu	123
6.	91.92.42.19	test	12345678
7.	91.92.40.153	deploy	password
8.	91.92.40.171	debian	12345
9.	91.92.40.200	support	root
10.	91.92.40.35	ubnt	1

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 214,020 malicious software samples were distributed during the week, a increase of 777.6% compared to last week's 24,387. The top ten malware families and their SHA256 hashes are listed below for threat hunting and IOC correlation.

SN	ATTACKING IP	MALICIOUS SOFTWARE	SHA256 HASH
1.	102.214.233.160	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
2.	102.214.233.173	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
3.	102.165.118.54	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
4.	102.42.115.248	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
5.	102.97.11.179	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	102.33.154.14	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
7.	102.33.155.126	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
8.	102.214.233.152	trojan.multiverze/r002c0dgp26	3474645503ee71af316f174c9f842261a1d37bf596376c8f90483cec57333b78
9.	102.214.233.166	miner.multiverze/r06ec0dh826	76f4cff23b97b5cc222d0183a9ece353a5a36cfad2e722c6a7e00f47bf3137f0

10.	213.209.159.136	miner.multiverze/genericrxss	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 41,359 web attacks were recorded, an increase of 49.6% from last week's 27,647. The top 10 attacking IPs and their targeted URIs are detailed below. Notable activity includes brute-force attempts on WordPress login pages and environment file (.env) enumeration.

SN	ATTACKING IP	TOP URI / REQUEST
1.	194.180.49.37	/
2.	45.148.10.183	/manager/html
3.	195.178.110.28	/.git/config
4.	45.148.10.238	/102.214.45.254/.env
5.	34.140.167.71	/.aws/credentials
6.	159.195.114.28	/.env
7.	213.209.159.154	/favicon.ico
8.	45.194.67.57	/.env.backup
9.	45.194.67.66	/?fetch=file%3A%2F%2F%2Fproc%2Fself%2Fenviron
10.	151.243.11.162	/?host=file%3A%2F%2F%2Fproc%2Fself%2Fenviron

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,280 ICS attacks were recorded, an increase of 45.6% from last week's 879. The top 5 attacking IPs exploiting industrial protocols are listed below. Exposed ICS services represent a high-risk vector requiring immediate attention from critical infrastructure operators.

SN	ATTACKING IP	PROTOCOL EXPLOITED	PORT

1.	154.6.145.14	guardian_ast	10001
2.	151.80.234.64	IEC104	2404
3.	18.116.101.220	ipmi	623
4.	69.164.205.196	kamstrup_protocol	1025
5.	18.218.118.203	kamstrup_management_protocol	50100

Table 4: Top 5 ICS Attacking IPs with Protocols and Ports

06: RECOMMENDATIONS

Based on honeypot sensor data for this reporting period, the following actions are recommended for national ICT stakeholders:

1. Monitor all listed malicious IP addresses across internal networks. These IPs are also flagged by external threat intelligence sources and may be used in further attacks.

2. Enforce strong password policies and prohibit usage of the listed credentials (usernames and passwords). Deploy mechanisms to monitor and alert on excessive login attempts.

3. Scan all systems for files matching the SHA256 hashes listed in the Malware section (Table 2) and quarantine any matches immediately.

4. Deploy or update Intrusion Detection Systems (IDS) with rules to flag the IP addresses, web request patterns, and ICS protocols identified in this report.