TZ-CERT HONEYPOT WEEKLY REPORT

Period: 3rd – 9th August 2026 | **Report No.:** TZ-CERT/WRHP/2026/32

01: WEEKLY ATTACK SUMMARY

788,540	547,245	36,762	100,985
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 56.5% vs last week	↓ 47.2% vs last week	↓ 50.1% vs last week	↓ 88.4% vs last week

A total of 788,540 network attacks were recorded across all sensors during the period 3rd – 9th August 2026, representing an overall decrease of 56.5% compared to last week's 1,811,213 attacks. While network and malware activity declined, web attacks decreased significantly by 50.1% and ICS attacks fell by 88.4%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

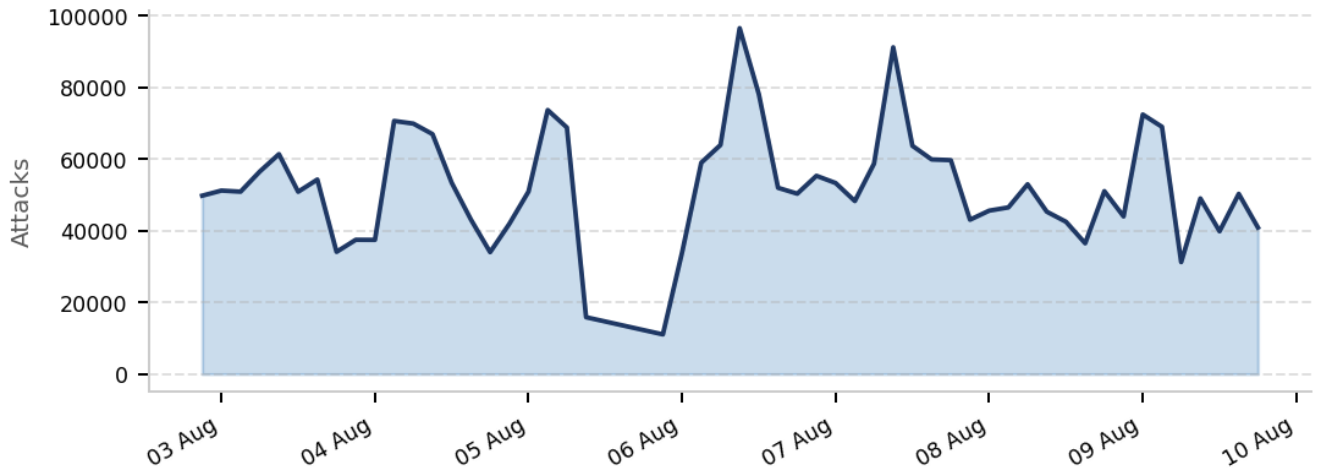

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 788,540 attacks have been recorded, down from last week's 1,811,213 by 56.5%. 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.	173.249.56.42	root	123456

2.	45.153.34.71	admin	123
3.	91.92.47.55	user	admin
4.	77.239.124.237	ubuntu	1234
5.	45.153.34.137	test	password
6.	45.153.34.112	deploy	12345678
7.	119.148.8.66	support	12345
8.	91.92.42.64	guest	1
9.	91.92.47.123	postgres	root
10.	91.92.47.53	uname -m	123456789

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 547,245 malicious software samples were distributed during the week, a decrease of 47.2% compared to last week's 1,035,703. 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.vigorf/shell	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	102.208.164.38	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
3.	102.33.154.14	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
4.	2.182.84.3	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
5.	41.33.89.62	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	102.23.194.195	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
7.	102.208.50.58	trojan.sagent/shell	31d4181843b1ed10a7e7cb3f108f6d6c50a7a4452ee52ddacabe8ca77260615e
8.	14.216.14.111	trojan.mirai/shell	df78602fd918d9e393d5d8aaf01fa76e01b615578cdbf513589319932fe3099b
9.	45.115.85.93	trojan.xorddos/ddos	6f45c6d9c70d97f695cb7bbef362812a17f8ed4d37dafc342c26c86ed9b43638

10.	102.33.152.194	trojan.multiverze/abapplication	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 36,762 web attacks were recorded, a decrease of 50.1% from last week's 73,613. 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.	45.148.10.238	/
2.	163.7.12.173	/script
3.	185.177.72.66	/manager/html
4.	185.177.72.68	/favicon.ico
5.	213.209.159.175	/SDK/webLanguage
6.	213.209.159.154	/robots.txt
7.	195.178.110.28	/.env
8.	94.154.43.120	/dispatch.asp
9.	80.94.95.211	/login
10.	146.56.54.22	/admin/config.php

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 100,985 ICS attacks were recorded, a decrease of 88.4% from last week's 867,975. 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.	27.131.66.109	snmp	161
2.	99.98.233.240	ipmi	623
3.	47.132.122.17	guardian_ast	10001
4.	37.66.197.125	kamstrup_protocol	1025
5.	70.126.89.159	IEC104	2404

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.