TZ-CERT HONEYPOT WEEKLY REPORT

Period: 17th – 23rd August 2026 | **Report No.:** TZ-CERT/WRHP/2026/34

01: WEEKLY ATTACK SUMMARY

57,314	24,387	27,647	879
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 97.6% vs last week	↓ 93.4% vs last week	↓ 70.5% vs last week	↓ 99.1% vs last week

A total of 57,314 network attacks were recorded across all sensors during the period 17th – 23rd August 2026, representing an overall decrease of 97.6% compared to last week's 2,350,938 attacks. While network and malware activity declined, web attacks decreased significantly by 70.5% and ICS attacks fell by 99.1%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

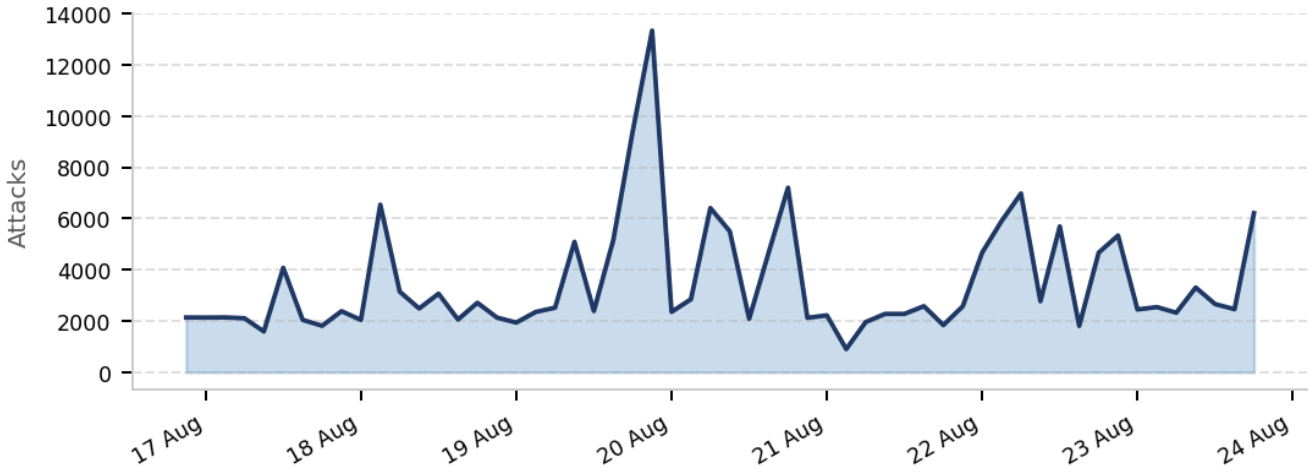

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 57,314 attacks have been recorded, down from last week's 2,350,938 by 97.6%. 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.	91.92.40.151	root	0

2.	91.92.42.7	admin	admin
3.	94.154.35.215	0	123456
4.	45.153.34.161	user	1234
5.	45.156.87.13	test	123
6.	91.92.40.124	guest	password
7.	91.92.40.29	debian	12345678
8.	91.92.42.227	support	12345
9.	45.153.34.165	unknown	root
10.	195.178.110.228	ubnt	(empty)

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 24,387 malicious software samples were distributed during the week, a decrease of 93.4% compared to last week's 367,329. 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.	102.210.31.46	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
2.	102.217.66.1	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
3.	102.182.52.250	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
4.	102.39.168.170	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
5.	213.209.159.136	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	111.46.219.233	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
7.	49.81.67.230	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
8.	3.141.247.102	miner.multiverze/r06ec0dh426	0bbee3979b0327b6c327c4522414a90d18164af3846ea6a8e62e5fee861f6d51
9.	18.116.101.220	miner.malxmr/multiverze	0f829c27b12416507d82d430160f354d13dd6946129edb49292e604d5f5f29f1

10.	3.131.220.121	trojan.multiverze/abminer	684e4d57a4b6cc37c7f87333e751c12edbbfc9cf685ebb36d563647ae6df0e17

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 27,647 web attacks were recorded, a decrease of 70.5% from last week's 93,696. 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.	45.148.10.183	/
2.	194.180.49.37	/SDK/webLanguage
3.	195.178.110.28	/favicon.ico
4.	185.177.72.54	/author/ghost/
5.	13.37.252.77	/the-editor/
6.	45.148.10.238	/using-tags/
7.	213.209.159.154	/robots.txt
8.	213.209.159.175	/welcome/
9.	45.194.67.53	/102.214.45.254/.env
10.	45.194.67.56	/.env

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 879 ICS attacks were recorded, a decrease of 99.1% from last week's 99,314. 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.	142.93.26.70	kamstrup_protocol	1025
2.	18.116.101.220	guardian_ast	10001
3.	3.129.187.38	IEC104	2404
4.	3.131.220.121	ipmi	623
5.	118.194.251.246	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.