TZ-CERT HONEYPOT WEEKLY REPORT

Period: 27th July – 2nd August 2026 | **Report No.:** TZ-CERT/WRHP/2026/31

01: WEEKLY ATTACK SUMMARY

1,811,213	1,035,703	73,613	867,975
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 3.3% vs last week	↑ 19.3% vs last week	↑ 34.7% vs last week	↓ 25.4% vs last week

A total of 1,811,213 network attacks were recorded across all sensors during the period 27th July – 2nd August 2026, representing an overall increase of 3.3% compared to last week's 1,753,116 attacks. While network and malware activity increased, web attacks increased significantly by 34.7% and ICS attacks fell by 25.4%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

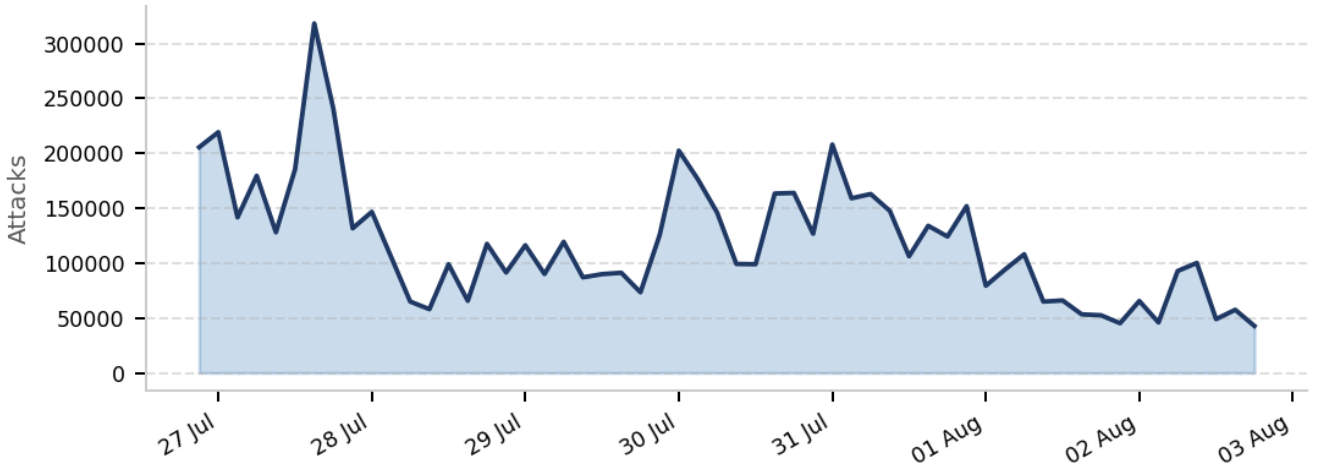

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,811,213 attacks have been recorded, up from last week's 1,753,116 by 3.3%. 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.	94.154.35.215	root	123456

2.	103.64.129.98	1111	1111
3.	179.43.139.58	redmine	admin
4.	178.16.54.226	admin	123
5.	173.249.56.42	pablo	1234
6.	94.159.116.130	user	password
7.	45.153.34.137	ubuntu	12345678
8.	93.188.83.96	proxy	12345
9.	193.32.162.27	tim	root
10.	160.119.76.10	support	1

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 1,035,703 malicious software samples were distributed during the week, a increase of 19.3% compared to last week's 868,067. 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.shell/abtrojan	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	41.59.203.60	trojan.sagent/shell	31d4181843b1ed10a7e7cb3f108f6d6c50a7a4452ee52ddacabe8ca77260615e
3.	102.33.154.14	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
4.	102.208.164.38	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
5.	152.32.77.162	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
6.	41.59.196.23	trojan.abminer/gen3	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
7.	41.59.211.41	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
8.	84.36.118.74	miner.malxmr/usblgr26	1eecf2377d20768c28d741e21affaa53cf26db0d083efdbf43a92fa938b7e4be
9.	182.184.109.220	miner.malxmr/usblgr26	be24e3ff143568fc82e42ed4aeee92e3f6f58c5fe3c5bb442cf4b998c90463d2

10.	12.97.127.122	trojan.abminer/gen3	2f206563640dd66a743ffd493ce0e3c31a8fc5a24b9f5d2b540fc22d45c13d66

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 73,613 web attacks were recorded, an increase of 34.7% from last week's 54,661. 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.	87.154.142.114	/
2.	163.7.13.2	/SDK/webLanguage
3.	94.26.88.31	/favicon.ico
4.	195.178.110.28	/robots.txt
5.	80.94.95.211	/.env
6.	104.192.3.106	/login
7.	213.209.159.154	/.env.php
8.	129.212.227.100	/.env.bak
9.	185.177.72.17	/.env.old
10.	20.48.234.177	/.env.txt

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 867,975 ICS attacks were recorded, a decrease of 25.4% from last week's 1,162,900. 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.	73.183.235.5	snmp	161
2.	89.92.69.50	ipmi	623
3.	68.161.162.126	guardian_ast	10001
4.	98.214.36.65	IEC104	2404
5.	169.136.38.36	kamstrup_protocol	1025

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.