TZ-CERT HONEYPOT WEEKLY REPORT

Period: 10th – 16th August 2026 | **Report No.:** TZ-CERT/WRHP/2026/33

01: WEEKLY ATTACK SUMMARY

2,350,938	367,329	93,696	99,314
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 198.1% vs last week	↓ 32.9% vs last week	↑ 154.9% vs last week	↓ 1.7% vs last week

A total of 2,350,938 network attacks were recorded across all sensors during the period 10th – 16th August 2026, representing an overall increase of 198.1% compared to last week's 788,540 attacks. While malware activity declined by 32.9%, web attacks increased significantly by 154.9% and ICS attacks fell by 1.7%, 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 2,350,938 attacks have been recorded, up from last week's 788,540 by 198.1%. 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.	192.145.169.66	root	123456

2.	103.195.81.146	ubuntu	admin
3.	37.111.53.110	admin	123
4.	103.60.204.198	user	1234
5.	103.82.210.181	pi	password
6.	103.177.41.70	oracle	12345678
7.	103.77.14.62	support	12345
8.	103.204.167.40	test	root
9.	173.249.56.42	deploy	1
10.	103.149.197.34	guest	123456789

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 367,329 malicious software samples were distributed during the week, a decrease of 32.9% compared to last week's 547,245. 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.	202.166.161.10	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
2.	41.93.63.66	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
3.	102.33.155.126	trojan.abtrojan/njww	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
4.	102.208.164.38	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
5.	41.38.51.10	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	103.125.68.194	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
7.	103.9.89.84	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
8.	82.167.55.119	trojan.mirai/ddos	156ee410363b67810416d16a797225ffbaa01cf80daeaff346dabf199f75cbed
9.	102.165.118.54	downloader.shell/bash	e4eaae680e23b413ec82a1cb66b4704f2d5df913520700f15e1a65c4ce10d322

10.	114.103.230.12	trojan.multiverze/abapplication	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 93,696 web attacks were recorded, an increase of 154.9% from last week's 36,762. 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	/phpinfo.php
3.	195.178.110.28	/info.php
4.	45.148.10.238	/php.php
5.	213.209.159.154	/php_info.php
6.	80.94.95.211	/admin/phpinfo.php
7.	197.250.51.112	/test.php
8.	45.148.10.125	/p.php
9.	179.43.150.26	/administrator/phpinfo.php
10.	172.161.1.105	/i.php

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 99,314 ICS attacks were recorded, a decrease of 1.7% from last week's 100,985. 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.	174.63.229.118	snmp	161
2.	86.19.130.35	ipmi	623
3.	76.33.219.165	guardian_ast	10001
4.	154.6.145.14	kamstrup_protocol	1025
5.	69.166.3.202	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.