TZ-CERT HONEYPOT WEEKLY REPORT

Period: 8th – 14th June 2026 | **Report No.:** TZ-CERT/WRHP/2026/24

01: WEEKLY ATTACK SUMMARY

1,239,226	3,024,798	70,519	25,545
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 4.9% vs last week	↑ 431.9% vs last week	↓ 27.4% vs last week	↑ 83.1% vs last week

A total of 1,239,226 network attacks were recorded across all sensors during the period 8th – 14th June 2026, representing an overall increase of 4.9% compared to last week's 1,181,047 attacks. While network and malware activity increased, web attacks decreased by 27.4% and ICS attacks rose by 83.1%, 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 1,239,226 attacks have been recorded, up from last week's 1,181,047 by 4.9%. 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.	87.251.64.176	root	(blank)

2.	103.133.160.33	admin	123456
3.	176.65.132.24	support	support
4.	94.154.35.215	(blank)	123
5.	103.64.129.98	user	admin
6.	45.156.87.93	guest	1234
7.	38.95.14.214	345gs5662d34	3245gs5662d34
8.	173.249.56.42	ubuntu	345gs5662d34
9.	91.92.42.133	test	password
10.	176.65.132.22	deploy	12345678

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 3,024,798 malicious software samples were distributed during the week, a increase of 431.9% compared to last week's 568,626. 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.	194.113.39.2	miner.r06ec0dkh25/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
2.	194.113.39.6	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
3.	194.113.39.22	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
4.	194.113.39.26	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
5.	194.113.39.14	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
6.	194.113.39.34	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	194.113.39.10	downloader.gen2/camelot	ae46e9548500ecbf07da46dd1f67c2e57639fd262d8b36ffda9042446fa4544d
8.	194.113.39.18	trojan.abrisk/qdhy	16d3440fcc067823afc44dcbccea9fbbc2f8c68ae53b7aea45f9adff4c127086
9.	194.113.39.30	trojan.multiverze/abapplication	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

10.	194.113.39.38	trojan.ddos/abtrojan	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 70,519 web attacks were recorded, a decrease of 27.4% from last week's 97,199. 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.	43.159.132.216	/
2.	163.7.3.220	/SDK/webLanguage
3.	185.177.72.23	/robots.txt
4.	185.177.72.53	/favicon.ico
5.	185.177.72.56	/.env
6.	185.177.72.67	/config.php
7.	185.177.72.70	/config.env
8.	152.42.160.206	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	69.5.20.93	/.git/config
10.	168.144.37.240	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 25,545 ICS attacks were recorded, an increase of 83.1% from last week's 13,948. 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.	193.168.198.33	snmp	161
2.	185.214.135.16	guardian_ast	10001
3.	167.86.126.236	kamstrup_protocol	1025
4.	172.59.122.139	IEC104	2404
5.	45.198.224.209	ipmi	623

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.