TZ-CERT HONEYPOT WEEKLY REPORT

Period: 4th – 10th May 2026 | **Report No.:** TZ-CERT/WRHP/2026/19

01: WEEKLY ATTACK SUMMARY

1,181,749	655,907	32,404	32,637
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 12.2% vs last week	↑ 39.2% vs last week	↑ 42.3% vs last week	↑ 14.7% vs last week

A total of 1,181,749 network attacks were recorded across all sensors during the period 4th – 10th May 2026, representing an overall decrease of 12.2% compared to last week's 1,345,929 attacks. While malware activity increased by 39.2%, web attacks increased significantly by 42.3% and ICS attacks rose by 14.7%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

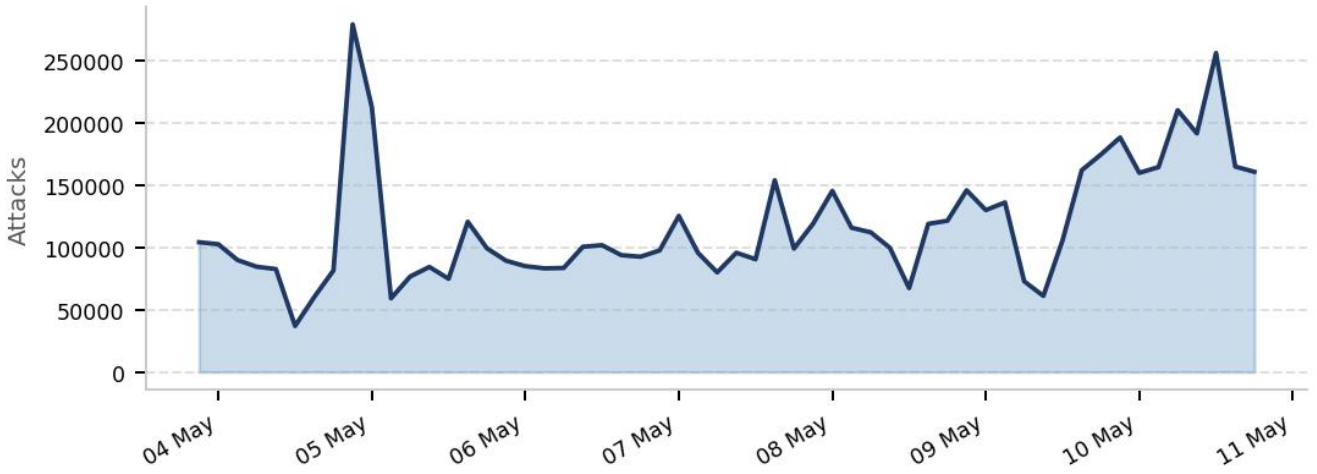

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,181,749 attacks have been recorded, down from last week's 1,345,929 by 12.2%. 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.	45.155.65.19	root	support

2.	159.65.8.74	admin	123456
3.	195.178.110.26	ubuntu	123
4.	94.154.35.215	support	admin
5.	87.251.64.176	user	3245gs5662d34
6.	154.58.202.40	sol	345gs5662d34
7.	185.246.128.133	postgres	1234
8.	176.65.132.129	test	solana
9.	45.153.34.112	345gs5662d34	password
10.	45.156.87.254	oracle	12345678

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 655,907 malicious software samples were distributed during the week, a increase of 39.2% compared to last week's 471,166. 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.	41.59.211.41	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.203.60	miner.r06ec0dkh25/wlshq	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	5.77.195.43	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	102.208.50.58	trojan.mirai/cciiu	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.93.63.66	trojan.malxmr/osqhr	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.33.89.62	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	14.240.3.53	sshd	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
8.	188.19.161.242	trojan.multiverze	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c
9.	102.208.164.38	trojan.multiverze/nyayh	47b268c21591069bfe4099833ad66b8138a53ab2dcb866e040d466aee1f8624c

10.	78.186.55.8	trojan.malxmr/usblci26	d7f98e379c400c13340781ccb65017c000330824ea26680866b9d3e43d641721

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 32,404 web attacks were recorded, an increase of 42.3% from last week's 22,777. 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.	94.26.106.155	/
2.	185.177.72.31	/favicon.ico
3.	41.59.86.254	/robots.txt
4.	194.180.49.49	/SDK/webLanguage
5.	204.76.203.206	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
6.	146.190.16.201	/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/bin/sh
7.	104.248.225.45	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
8.	45.148.10.5	/.env
9.	77.83.39.167	/V2/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	74.249.238.26	/admin/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 32,637 ICS attacks were recorded, an increase of 14.7% from last week's 28,451. 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.	77.83.240.70	guardian_ast	10001
2.	175.110.122.159	IEC104	2404
3.	175.110.122.162	kamstrup_protocol	1025
4.	175.110.122.151	kamstrup_management_protocol	50100
5.	175.110.122.149	—	—

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.