TZ-CERT HONEYPOT WEEKLY REPORT

Period: 27th April – 3rd May 2026 | **Report No.:** TZ-CERT/WRHP/2026/18

01: WEEKLY ATTACK SUMMARY

1,345,929	471,166	22,777	28,451
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 39.1% vs last week	↓ 17.9% vs last week	↓ 40.8% vs last week	↑ 16.4% vs last week

A total of 1,345,929 network attacks were recorded across all sensors during the period 27th April – 3rd May 2026, representing an overall increase of 39.1% compared to last week's 967,772 attacks. While malware activity declined by 17.9%, web attacks decreased significantly by 40.8% and ICS attacks rose by 16.4%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

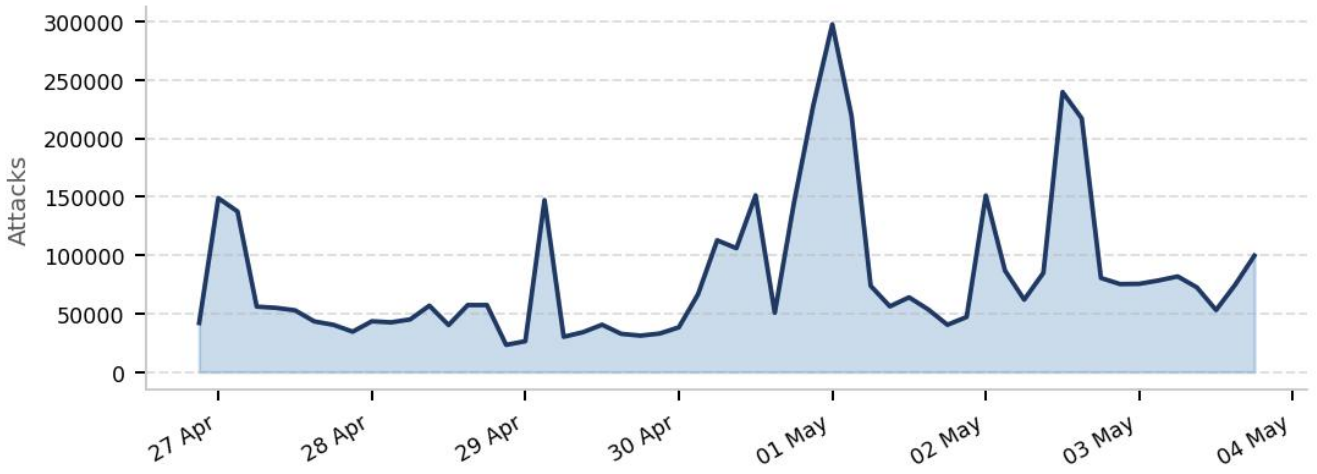

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,345,929 attacks have been recorded, up from last week's 967,772 by 39.1%. 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.	194.233.87.143	root	123456

2.	94.154.35.215	admin	admin
3.	177.125.137.18	ubuntu	123
4.	185.233.247.245	user	3245gs5662d34
5.	195.178.110.26	sol	345gs5662d34
6.	121.7.235.42	345gs5662d34	admin!@#
7.	157.90.89.51	postgres	0
8.	179.43.139.58	router	1234
9.	185.148.3.54	0	support
10.	216.238.81.205	test	git

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 471,166 malicious software samples were distributed during the week, a decrease of 17.9% compared to last week's 573,738. 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.	102.208.164.38	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	95.131.148.235	adware.mirai/cciiu	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	204.11.92.62	trojan.malxmr/osqhr	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.111.165.15	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	41.59.201.7	trojan.shell	148d31c590732b49fd4632ac63d4c7f0d4e56c8900204968a6adfdac1e7e7c3e
8.	113.161.28.255	trojan.eddci	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
9.	102.141.170.73	trojan.multiverze/nvgnb	97a1e6f817d44a4f8b07fdebaf9357786742096c470eb5d78e789b6bb53979bb

10.	41.139.177.151	trojan.multiverze	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 22,777 web attacks were recorded, a decrease of 40.8% from last week's 38,482. 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.	194.180.49.49	/
2.	155.94.139.220	/favicon.ico
3.	167.99.147.201	/robots.txt
4.	94.26.106.155	/vendor/phpunit/phpunit/Util/PHP/eval-stdin.php
5.	204.76.203.206	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
6.	77.83.39.167	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
7.	185.177.72.16	/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
8.	185.177.72.30	/.env
9.	157.245.202.214	/anthropic/v1/models
10.	172.173.121.85	/V2/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 28,451 ICS attacks were recorded, an increase of 16.4% from last week's 24,446. 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.	175.110.122.151	guardian_ast	10001
2.	175.110.122.159	kamstrup_protocol	1025
3.	175.110.122.163	IEC104	2404
4.	175.110.122.158	kamstrup_management_protocol	50100
5.	175.110.122.160	—	—

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.