TZ-CERT HONEYPOT WEEKLY REPORT

Period: 25th – 31st May 2026 | **Report No.:** TZ-CERT/WRHP/2026/22

01: WEEKLY ATTACK SUMMARY

853,976	376,611	112,919	4,928
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 10.6% vs last week	↓ 24.2% vs last week	↑ 51.3% vs last week	↓ 13.7% vs last week

A total of 853,976 network attacks were recorded across all sensors during the period 25th – 31st May 2026, representing an overall increase of 10.6% compared to last week's 772,057 attacks. While malware activity declined by 24.2%, web attacks increased significantly by 51.3% and ICS attacks fell by 13.7%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

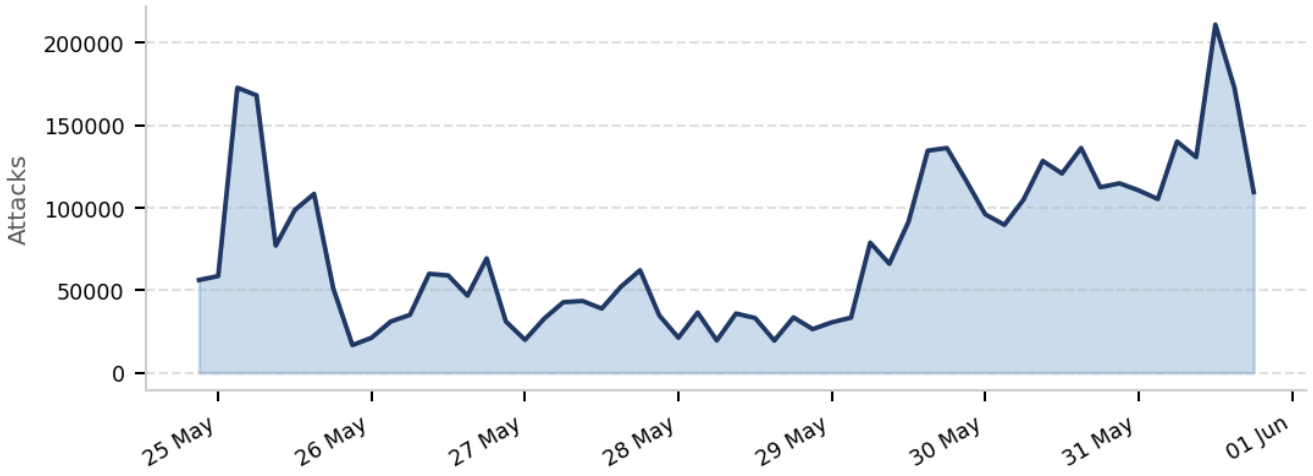

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 853,976 attacks have been recorded, up from last week's 772,057 by 10.6%. 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.	201.184.172.174	root	

2.	85.100.120.193	admin	support
3.	45.156.87.147		123456
4.	88.138.20.172	support	3245gs5662d34
5.	94.154.35.215	user	345gs5662d34
6.	87.251.64.176	345gs5662d34	123
7.	60.163.139.198	ubuntu	12345
8.	192.109.200.220	postgres	1234
9.	185.246.128.133	deploy	postgres1234
10.	45.153.34.71	test	password

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 376,611 malicious software samples were distributed during the week, a decrease of 24.2% compared to last week's 496,550. 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/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	2.50.174.152	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	41.93.63.66	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	102.208.164.38	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.59.10.22	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	194.113.39.26	trojan.mirai	45bff40a22d87575c6dd47fb5a1cdade428c08771f50c357ac9001f3f6f1279a
8.	194.113.39.38	trojan.abtrojan/lnrc	266fb0afe7c2a853d436625aed3adf2748fc3636268d3b15f92f20d430b5274e
9.	194.113.39.34	trojan.	d346fbb0c89b901e31f2c1247a99f9eab58fdba110f63edb4974d8205c196003

10.	194.113.39.6	trojan.multiverze/tl0101dr26zz	24820fbb2208b8cc97f8478ffe4f7187e0951427a9f98b0b0b6e73cae47cd508

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 112,919 web attacks were recorded, an increase of 51.3% from last week's 74,647. 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.	93.123.109.10	/
2.	151.104.32.9	/login
3.	168.144.37.240	/admin/config.php
4.	101.47.23.214	/login/
5.	185.38.150.28	/news/
6.	178.128.98.102	/robots.txt
7.	151.243.150.23	/public_html.zip
8.	34.107.110.242	/web.zip
9.	34.125.86.206	/wp-admin.zip
10.	34.153.185.52	/api.zip

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 4,928 ICS attacks were recorded, a decrease of 13.7% from last week's 5,711. 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.	45.95.147.229	guardian_ast	10001
2.	89.187.168.240	IEC104	2404
3.	89.187.168.42	kamstrup_protocol	1025
4.	77.83.240.70	kamstrup_management_protocol	50100
5.	51.68.207.118	snmp	161

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.