TZ-CERT HONEYPOT WEEKLY REPORT

Period: 18th – 24th May 2026 | **Report No.:** TZ-CERT/WRHP/2026/21

01: WEEKLY ATTACK SUMMARY

772,057	496,550	74,647	5,711
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 8.1% vs last week	↓ 10.2% vs last week	↑ 241.4% vs last week	↓ 31.2% vs last week

A total of 772,057 network attacks were recorded across all sensors during the period 18th – 24th May 2026, representing an overall decrease of 8.1% compared to last week's 840,269 attacks. While network and malware activity declined, web attacks increased significantly by 241.4% and ICS attacks fell by 31.2%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

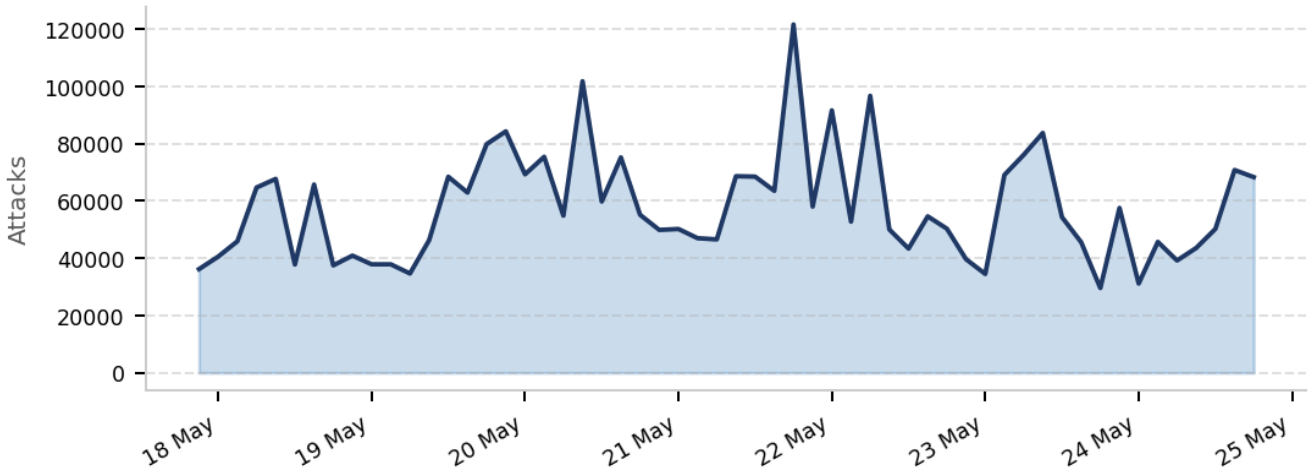

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 772,057 attacks have been recorded, down from last week's 840,269 by 8.1%. 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.	45.156.87.147	root	123456

2.	51.38.168.115	support	support
3.	185.233.247.245	admin	345gs5662d34
4.	94.154.35.215	user	3245gs5662d34
5.	45.156.87.253	345gs5662d34	a
6.	176.65.139.118	a	git
7.	45.153.34.112	sftp_user	user
8.	87.251.64.176	ubuntu	123
9.	89.163.135.198	git	admin!@#
10.	176.65.132.17	router	password

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 496,550 malicious software samples were distributed during the week, a decrease of 10.2% compared to last week's 552,647. 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.	41.59.203.60	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.211.41	miner.r06ec0dkh25/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.33.89.62	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	197.17.34.229	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.90.13.170	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	85.185.30.130	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	197.58.180.60	trojan.malxmr/usblci26	d7f98e379c400c13340781ccb65017c000330824ea26680866b9d3e43d641721
8.	203.204.185.62	downloader.medusa/shell	6a51fd1a8e7c45633fc4ca2b49a616326089d12a737720396c50f3484e178dae
9.	200.111.23.89	trojan.multiverze/usblbs26	27d205dc183ea2fad0e55e10b206404be20908e39a74569ff99182d7326ed9c0

10.	81.10.102.134	trojan.multiverze	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 74,647 web attacks were recorded, an increase of 241.4% from last week's 21,864. 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.	185.177.72.10	/cgi-bin/luci/;stok=/locale
3.	185.177.72.66	/admin/config.php
4.	38.147.161.99	/.env
5.	143.198.166.222	/favicon.ico
6.	20.12.236.157	/.aws/credentials
7.	20.151.117.104	/robots.txt
8.	213.209.159.175	/config.php
9.	45.135.193.157	/info
10.	139.59.224.14	/SDK/webLanguage

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 5,711 ICS attacks were recorded, a decrease of 31.2% from last week's 8,302. 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.	45.95.147.229	kamstrup_management_protocol	50100
3.	160.119.76.4	kamstrup_protocol	1025
4.	87.249.133.69	IEC104	2404
5.	89.187.168.52	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.