TZ-CERT HONEYPOT WEEKLY REPORT

Period: 23rd – 29th March 2026 | **Report No.:** TZ-CERT/WRHP/2026/11

01: WEEKLY ATTACK SUMMARY

949,122	675,826	25,352	34,381
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 10.6% vs last week	↓ 11.9% vs last week	↓ 54.6% vs last week	↑ 253.1% vs last week

A total of 949,122 network attacks were recorded across all sensors during the period 23rd – 29th March 2026, representing an overall increase of 10.6% compared to last week's 858,487 attacks. While malware activity declined by 11.9%, web attacks decreased significantly by 54.6% and ICS attacks rose by 253.1%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

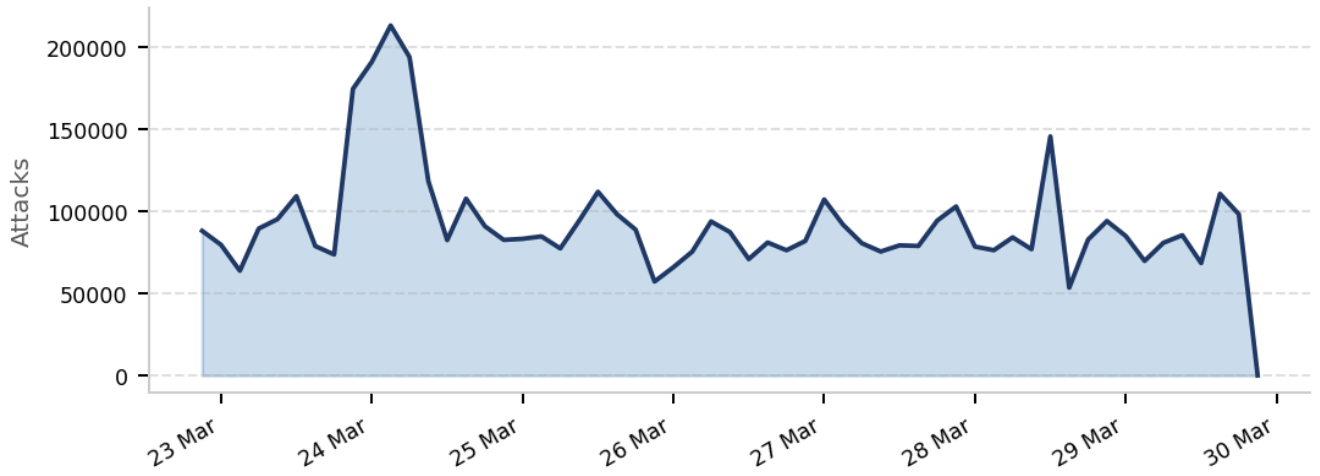

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 949,122 brute force attacks have been recorded, up from last week's 858,487 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.

#	ATTACKING IP	USERNAME USED	PASSWORD USED
1.	118.26.110.171	root	123456
2.	156.238.253.198	admin	345gs5662d34
3.	51.75.127.207	user	3245gs5662d34

4.	197.242.182.66	345gs5662d34	admin
5.	195.178.110.26	ubuntu	123
6.	94.154.35.215	sol	1234
7.	185.246.128.133	postgres	12345678
8.	194.50.16.198	oracle	password
9.	104.105.81.126	sftp_user	solana
10.	172.235.168.222	router	12345

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 675,826 malicious software samples were distributed during the week, a decrease of 11.9% compared to last week's 766,774. The top ten malware families and their SHA256 hashes are listed below for threat hunting and IOC correlation.

#	ATTACKING IP	MALICIOUS SOFTWARE	SHA256 HASH
1.	41.59.211.41	trojan.shell/malkey	a8460f446be540410004b1a8db4083773fa46f7fe76fa84219c93daa1669f8f2
2.	41.59.201.132	Win32/evader	01ba4719c80b6fe911b091a7c05124b64eeece964e09c058ef8f9805daca546b
3.	41.59.203.60	trojan.shell/qwexlafiba	c8e8f6236e6bbcee6c407cdd425432e1819871ce5231a1511a0f6ae29ac4cb68
4.	41.59.201.7	miner.wlshq/r06ec0dkh25	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
5.	102.208.98.158	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	41.33.89.62	Miner:Multi/XMRig	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
7.	102.208.164.38	miner.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
8.	81.195.134.218	Trojan:Linux/Multiverze!rfn	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
9.	41.111.206.97	Trojan:Win32/Alevaul!rfn	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
10.	41.59.196.23	Linux/Dropper	1b20a210fe96e5a8abc347dfb91d7befecb4b5f9b7ed40d856410fac15952057

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 25,352 web attacks were recorded, a decrease of 54.6% from last week's 55,872. 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.

#	ATTACKING IP	TOP URI / REQUEST
1.	185.177.72.51	/
2.	195.178.110.109	/robots.txt
3.	194.50.16.198	/favicon.ico
4.	185.177.72.49	/SDK/webLanguage
5.	185.177.72.22	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
6.	20.48.232.178	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
7.	64.181.201.187	/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%
8.	20.151.201.236	/lib/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	41.242.48.18	/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
10.	157.245.151.235	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 34,381 ICS attacks were recorded, an increase of 253.1% from last week's 9,736. 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.

#	ATTACKING IP	PROTOCOL EXPLOITED	PORT
1.	194.50.16.198	kamstrup_protocol	5900
2.	118.194.250.232	guardian_ast	443
3.	45.194.70.252	kamstrup_management_protocol	64294
4.	152.32.149.35	IEC104	445
5.	165.154.11.206	snmp	5060

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.