TZ-CERT HONEYPOT WEEKLY REPORT

Period: 16th – 22nd March 2026 | **Report No.:** TZ-CERT/WRHP/2026/10

01: WEEKLY ATTACK SUMMARY

858,485	766,774	55,872	9,736
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 25.2% vs last week	↓ 30.4% vs last week	↑ 48.1% vs last week	↑ 14.7% vs last week

A total of 858,485 network attacks were recorded across all sensors during the period 16th–22nd March 2026, representing an overall decrease of 25.2% compared to last week's 1,146,005 attacks. While network and malware activity declined, web attacks increased significantly by 48.1% and ICS attacks rose by 14.7%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

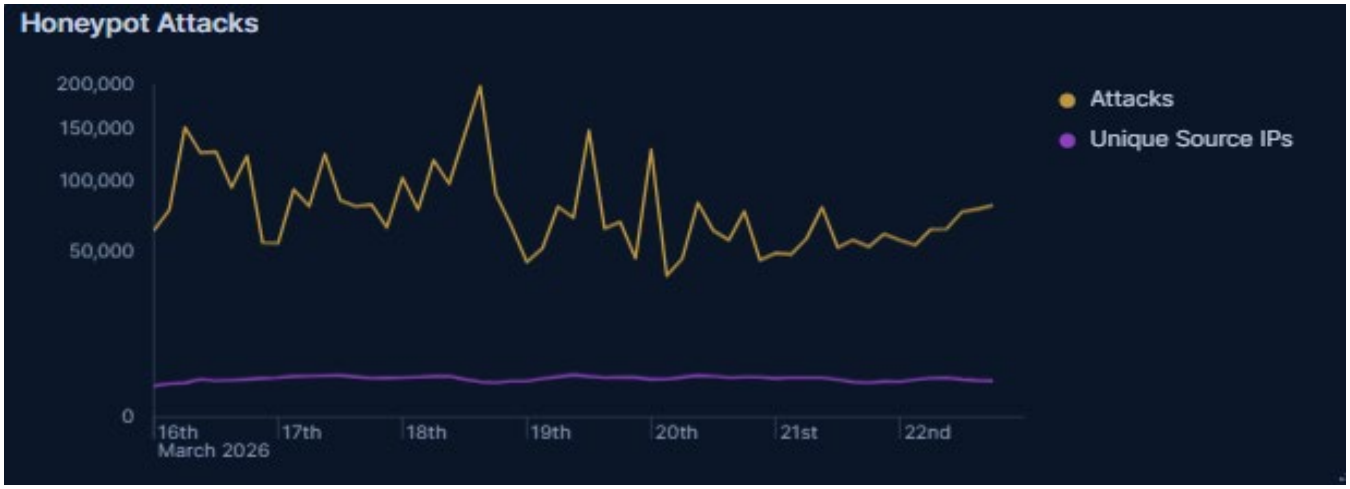

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 858,485 attacks have been recorded, down from last week's 1,146,005. 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.	94.154.35.215	root	password
2.	195.178.110.26	admin	admin
3.	14.225.2.66	user	12345678
4.	142.171.95.117	sol	12345
5.	139.59.100.63	ubuntu	click1
6.	118.26.110.171	git	git

7.	185.246.128.133	sync	admin!@#
8.	2.57.121.25	router	solana
9.	178.16.54.226	test	root
10.	2.57.121.112	oracle	P@ssw0rd

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 766,774 malicious software samples were distributed during the week, compared to 1,102,091 the prior week. 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.	41.59.203.60	adware.multiverze/r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
2.	41.59.211.41	E64/ABTrojan.KIAZ-	31384110975802292bbfa8301113a4bb857cc1acb8b820e5459eab283646d79a
3.	102.208.164.38	HEUR:Trojan.Linux.Miner.gen	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c
4.	41.93.63.66	trojan.multiverze/malxmr	765289f938cc2bd64c9778dbabe048afa8ac3277a150c940d2730c14d24687b5
5.	41.59.201.132	Trojan.Linux.Mirai	8f13032297194947c6fc736026b1ce19981e17b83c9adf3e73768a5d265268b6
6.	41.59.201.7	Generic.Linux.Medusa.C.24BBA57E	13d6e7ca20160d2fe3b730ee3af14c740e51a46292b3c00a1c210f87fccaac83
7.	41.59.108.114	Trojan:Script/Wacatac.C!ml	14490a91934bd6970bbaae15009065283ca22a38bd22a738647e769920f86e16
8.	41.139.177.151	Downloader/Shell.ElfMiner.S1139	0ab70183d671b0a054def272c335ee93306e11573e346c59419656f54726aaa1
9.	125.209.92.84	Trojan.Script.Multiverze.4!c	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
10.	81.20.195.202	TrojanDownloader:Script/Iranbot.A	5992b0575201555ed33defd0f9d989627c295f4f7bd2522f787b11f8a15b61d8

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 55,872 web attacks were recorded, a significant increase from last week's 37,736. 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.	41.59.108.114	/
2.	209.38.224.165	/wp-login.php
3.	185.177.72.13	/admin/config.php
4.	159.195.42.18	/robots.txt
5.	196.192.78.138	/wp-login.php?action=lostpassword
6.	185.177.72.52	/favicon.ico
7.	185.177.72.56	/.env
8.	185.177.72.51	/.env.bak

9.	195.178.110.199	/config.php
10.	195.178.110.109	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 9,736 ICS attacks were recorded, up from last week's 8,488. 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	guardian_ast	5900
2.	41.59.108.114	kamstrup_protocol	64294
3.	37.19.195.84	IEC104	443
4.	16.58.56.214	kamstrup_management_protocol	445
5.	139.59.97.94	snmp	1433

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.

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM (TZ-CERT)