TZ-CERT HONEYPOT WEEKLY REPORT

Period: 30th March – 5th April 2026 | **Report No.:** TZ-CERT/WRHP/2026/12

01: WEEKLY ATTACK SUMMARY

1,008,530	638,448	38,777	19,063
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 6.3% vs last week	↓ 5.5% vs last week	↑ 53.0% vs last week	↓ 44.6% vs last week

A total of 1,008,530 network attacks were recorded across all sensors during the period 30th March – 5th April 2026, representing an overall increase of 6.3% compared to last week's 949,125 attacks. While malware activity declined by 5.5%, web attacks increased significantly by 53.0% and ICS attacks fell by 44.6%, 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 1,008,530 attacks have been recorded, up from last week's 949,125 by 6.3%. 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.	167.114.38.196	root	345gs5662d34
2.	207.6.36.82	admin	3245gs5662d34

3.	171.211.125.105	ubuntu	123456
4.	195.178.110.26	user	solana
5.	61.220.127.240	345gs5662d34	123
6.	105.155.165.177	sol	1234
7.	110.10.176.72	postgres	admin
8.	94.154.35.215	solana	ubuntu
9.	160.177.67.84	solv	sol
10.	41.142.215.250	validator	broadguam1

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 638,448 malicious software samples were distributed during the week, a decrease of 5.5% compared to last week's 675,826. 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	trojan.multiverze/malxmr	765289f938cc2bd64c9778dbabe048afa8ac3277a150c940d2730c14d24687b5
2.	41.59.211.41	HEUR:Trojan.Linux.Miner.gen	897ea7b1ff1c13db7f2e05b9463b7d516893add639bfe7cb12226608df95a542
3.	102.208.164.38	Trojan:Linux/Multiverze!rfn	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c
4.	180.250.204.97	Trojan.Linux.Multiverze.4!c	aa85190274311673a61039d434c6b30a0f694ce645a0340f0c11424d0eff8f87
5.	219.85.219.128	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	46.235.137.206	miner.r06ec0dkh25/wlshq	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
7.	41.59.201.132	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
8.	41.59.196.23	adware.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
9.	41.33.136.154	trojan.shell/qwexlafiba	c8e8f6236e6bbcee6c407cdd425432e1819871ce5231a1511a0f6ae29ac4cb68
10.	49.207.181.92	downloader.medusa/shell	2ee89245c6dd3edd3e14f8bc52c866757ad98b97955b181d0cd5dc719004b893

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 38,777 web attacks were recorded, an increase of 53.0% from last week's 25,352. The top 10 attacking IPs and their targeted URIs are detailed below. Notable activity includes attempts to exploit remote code execution vulnerabilities (e.g., cgi-bin traversal and php://input injection), probing for

sensitive configuration files (such as /admin/config.php and PHPUnit eval endpoints), and reconnaissance of common files like /robots.txt and /favicon.ico.

#	ATTACKING IP	TOP URI / REQUEST
1.	185.177.72.13	/
2.	185.177.72.52	/robots.txt
3.	185.177.72.205	/admin/config.php
4.	185.177.72.23	/favicon.ico
5.	185.177.72.24	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
6.	185.177.72.61	/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/%%32%65%%32%65/bin/sh
7.	150.241.124.122	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
8.	185.16.39.146	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	160.119.76.250	/SDK/webLanguage
10.	194.50.16.198	/hello.world?%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 19,063 ICS attacks were recorded, a decrease of 44.6% from last week's 34,381. 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	10001
2.	176.120.22.52	kamstrup_protocol	1025
3.	88.80.148.153	kamstrup_management_protocol	50100
4.	88.80.148.108	IEC104	2404
5.	88.80.148.93	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.

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM (TZ-CERT)