TZ-CERT HONEYPOT WEEKLY REPORT

Period: 6th – 12th April 2026 | **Report No.:** TZ-CERT/WRHP/2026/13

01: WEEKLY ATTACK SUMMARY

633,537	555,228	45,369	19,940
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 37.2% vs last week	↓ 13.0% vs last week	↑ 17.0% vs last week	↑ 4.6% vs last week

A total of 633,537 network attacks were recorded across all sensors during the period 6th – 12th April 2026, representing an overall decrease of 37.2% compared to last week's 1,008,530 attacks. While network and malware activity declined, web attacks increased by 17.0% and ICS attacks rose by 4.6%, 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 633,537 attacks have been recorded, down from last week's 1,008,530 by 37.2%. 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.	120.238.149.205	root	123456

2.	45.74.0.71	admin	345gs5662d34
3.	195.178.110.26	ubuntu	3245gs5662d34
4.	94.154.35.215	sol	123
5.	185.246.128.133	user	admin
6.	222.71.102.210	345gs5662d34	solana
7.	156.227.236.24	postgres	1234
8.	110.10.176.72	solv	broadguam1
9.	200.124.160.2	solana	ubuntu
10.	61.220.127.240	test	sol

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 555,228 malicious software samples were distributed during the week, a decrease of 13.0% compared to last week's 638,448. 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.	102.208.164.38	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.203.60	miner.r06ec0dkh25/wlshq	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.59.211.41	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	41.59.201.132	miner.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.173.197.65	trojan.malxmr/osqhr	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	31.166.153.104	Trojan/BAT.Obfuscated.aar!crit	4e168ff81d9914129f5395f6608a44d954bba043f82872a9f57573c9183dbb61
7.	213.172.84.12	trojan.shell/qwexlafiba	c8e8f6236e6bbcee6c407cdd425432e1819871ce5231a1511a0f6ae29ac4cb68
8.	41.203.223.149	trojan.tsunami/flooder	9701ae7249aa394624bf33096e3f5dd2be0bb778debba3364f5277a50874cc31
9.	190.183.61.138	trojan.shell	dccfd62d350184fc137b18acbdd56fceee07f2c7b7f89eb1071e7c4eb0f01bcd

10.	41.38.64.137	Trojan.GenericKD.74212318	32b44db3980a94e1be989a4c5605cb2b3ed2db6cfa208943c70ae2a82d983291

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 45,369 web attacks were recorded, an increase of 17.0% from last week's 38,777. 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.	185.177.72.38	/
2.	185.177.72.70	/admin/config.php
3.	185.177.72.205	/favicon.ico
4.	185.177.72.100	/robots.txt
5.	185.177.72.13	/SDK/webLanguage
6.	185.177.72.66	/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.	185.177.72.61	/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%
8.	160.119.76.250	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
9.	185.16.39.146	/V2/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	185.177.72.11	/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 19,940 ICS attacks were recorded, an increase of 4.6% from last week's 19,063. 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.	88.80.148.118	guardian_ast	10001
2.	88.80.148.153	kamstrup_protocol	1025
3.	88.80.148.93	IEC104	2404
4.	88.80.148.122	kamstrup_management_protocol	50100
5.	88.80.148.132	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)