TZ-CERT HONEYPOT WEEKLY REPORT

Period: 20th – 26th April 2026 | **Report No.:** TZ-CERT/WRHP/2026/15

01: WEEKLY ATTACK SUMMARY

967,772	573,738	38,482	24,446
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 40.2% vs last week	↓ 14.8% vs last week	↑ 59.4% vs last week	↓ 22.1% vs last week

A total of 967,772 network attacks were recorded across all sensors during the period 20th – 26th April 2026, representing an overall increase of 40.2% compared to last week's 690,372 attacks. While malware activity declined by 14.8%, web attacks increased significantly by 59.4% and ICS attacks fell by 22.1%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

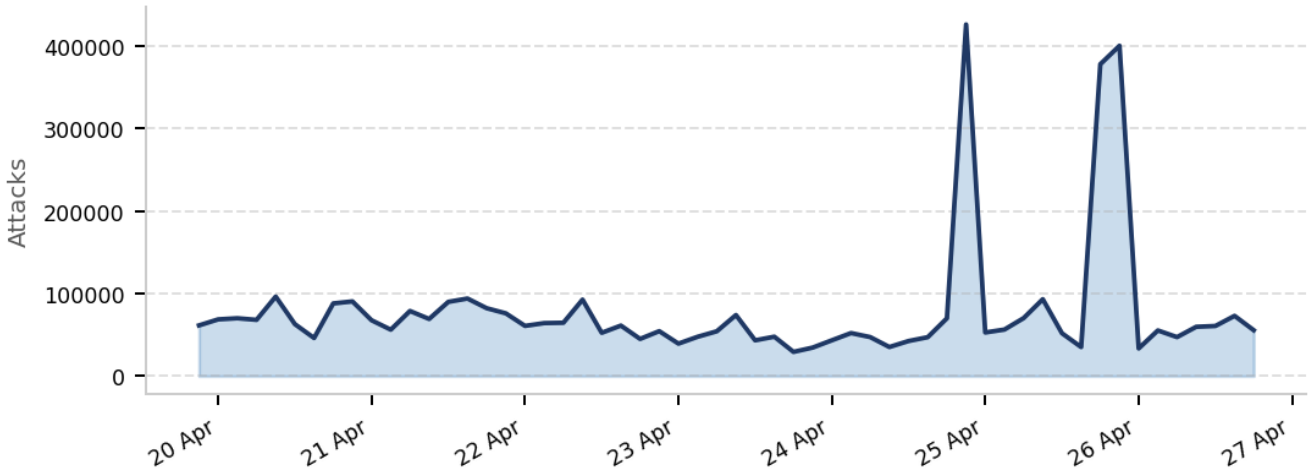

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 967,772 attacks have been recorded, up from last week's 690,372 by 40.2%. 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.	45.228.8.33	root	123456

2.	220.241.56.172	ubuntu	123
3.	195.178.110.26	admin	345gs5662d34
4.	94.154.35.215	user	3245gs5662d34
5.	176.65.132.254	345gs5662d34	0
6.	185.233.247.245	sol	admin
7.	176.65.139.95	tim	1234
8.	45.156.87.99	test	solana
9.	177.125.137.18	postgres	password
10.	14.103.78.102	0	ubuntu

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 573,738 malicious software samples were distributed during the week, a decrease of 14.8% compared to last week's 673,664. 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/wlshq	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.59.201.132	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	102.208.164.38	miner.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	92.36.168.133	trojan.malxmr/osqhr	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.33.89.62	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	186.153.132.242	trojan.azmvb	e948036f1c3b3024a6864fa1c49332c80e1fd28484cf487233a50154ffe104f8
8.	122.99.125.18	miner.multiverze	1e968044a1a92b613d1d64fd665658ef361982b450c1d3ab90ccc7822f6025ce
9.	185.133.212.78	trojan.multiverze	aeab239bc59b41c3d8a1b726c680f3086996ab00bc714668f6350f737ca4e5b8

10.	62.103.224.252	trojan.shell	148d31c590732b49fd4632ac63d4c7f0d4e56c8900204968a6adfdac1e7e7c3e

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 38,482 web attacks were recorded, an increase of 59.4% from last week's 24,140. 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.	185.177.72.53	/
2.	185.177.72.100	/admin/config.php
3.	185.177.72.11	/favicon.ico
4.	185.177.72.29	/robots.txt
5.	185.177.72.52	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
6.	204.76.203.206	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
7.	194.180.49.49	/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/%%32%65%%32%65/bin/sh
8.	195.178.110.132	/V2/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	157.245.202.214	/admin/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	147.182.156.41	/api/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 24,446 ICS attacks were recorded, a decrease of 22.1% from last week's 31,382. 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.	175.110.122.152	guardian_ast	10001
2.	175.110.122.151	kamstrup_protocol	1025
3.	175.110.122.157	IEC104	2404
4.	175.110.122.160	kamstrup_management_protocol	50100
5.	175.110.122.149	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)