TZ-CERT HONEYPOT WEEKLY REPORT

Period: 13th – 19th April 2026 | **Report No.:** TZ-CERT/WRHP/2026/14

01: WEEKLY ATTACK SUMMARY

690,372	673,664	24,140	31,382
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 9.0% vs last week	↑ 21.3% vs last week	↓ 46.8% vs last week	↑ 57.4% vs last week

A total of 690,372 network attacks were recorded across all sensors during the period 13th – 19th April 2026, representing an overall increase of 9.0% compared to last week's 633,537 attacks. While network and malware activity increased, web attacks decreased significantly by 46.8% and ICS attacks rose by 57.4%, 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 690,372 attacks have been recorded, up from last week's 633,537 by 9.0%. 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.	159.203.120.106	root	123

2.	109.172.93.21	ubuntu	123456
3.	195.178.110.26	admin	3245gs5662d34
4.	177.125.137.18	user	345gs5662d34
5.	45.228.8.33	sol	solana
6.	94.154.35.215	345gs5662d34	admin
7.	213.125.209.110	postgres	1234
8.	185.246.128.133	tim	click1
9.	45.156.87.99	validator	ubuntu
10.	179.8.5.21	solana	sol

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 673,664 malicious software samples were distributed during the week, a increase of 21.3% compared to last week's 555,228. 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.	41.59.211.41	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.203.60	miner.wlshq/r06ec0dkh25	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.59.201.132	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	102.208.164.38	miner.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.139.177.151	trojan.malxmr/osqhr	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	102.208.50.58	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	197.245.172.94	trojan.bash/shell	e16a3a60f39ce83cfa19ba50fe88b109cb02096126ac9e1c7cfeb8f64a432618
8.	60.251.111.38	trojan.multiverze	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c
9.	223.206.10.148	downloader.bash/miraia	1b3ba6b3b880ac4d194ed3d97cb0ad83ce7b28a301bab59f34c7fd3b2aff3cd2

10.	156.199.167.77	downloader.medusa/shell	dfc3975a32648e030e179a9d941422ca66755ce6121d5be17e3c4c4330f4a1fc

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 24,140 web attacks were recorded, a decrease of 46.8% from last week's 45,369. 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.	185.177.72.9	/
2.	185.177.72.61	/favicon.ico
3.	185.16.39.146	/admin/config.php
4.	35.90.224.79	/robots.txt
5.	20.48.184.58	/.env
6.	94.26.88.31	/.git/config
7.	188.166.234.144	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
8.	20.43.19.237	/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
9.	176.65.148.177	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
10.	155.94.139.220	/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 31,382 ICS attacks were recorded, an increase of 57.4% from last week's 19,940. 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.	88.80.148.153	guardian_ast	10001
2.	88.80.148.122	kamstrup_protocol	1025
3.	88.80.148.104	IEC104	2404
4.	88.80.148.91	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)