TZ-CERT HONEYPOT WEEKLY REPORT

Period: 15th – 21st June 2026 | **Report No.:** TZ-CERT/WRHP/2026/25

01: WEEKLY ATTACK SUMMARY

1,094,669	760,082	38,164	21,279
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 11.7% vs last week	↓ 74.9% vs last week	↓ 45.9% vs last week	↓ 16.7% vs last week

A total of 1,094,669 network attacks were recorded across all sensors during the period 15th – 21st June 2026, representing an overall decrease of 11.7% compared to last week's 1,239,226 attacks. While network and malware activity declined, web attacks decreased significantly by 45.9% and ICS attacks fell by 16.7%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

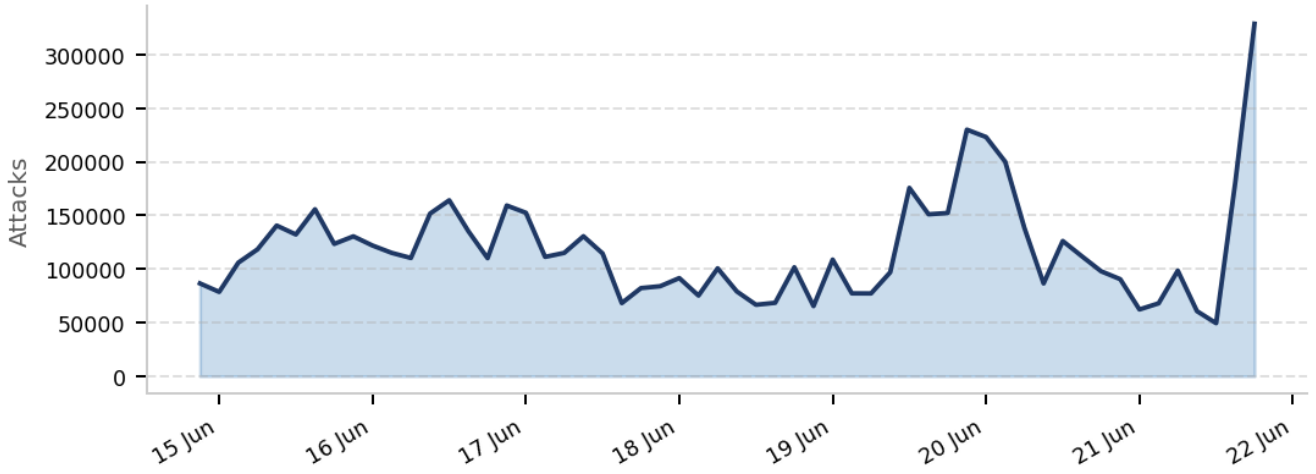

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,094,669 attacks have been recorded, down from last week's 1,239,226 by 11.7%. 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.	93.188.83.96	root	kisan
2.	185.16.38.216	admin	123456
3.	94.154.35.215	user	support
4.	87.251.64.176	support	admin
5.	173.249.56.42	ubuntu	123
6.	123.27.168.40	contec	1234
7.	45.153.34.114	345gs5662d34	password
8.	185.246.128.133	test	contec
9.	45.154.244.2	administrator	345gs5662d34
10.	45.161.6.11	postgres	3245gs5662d34

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 760,082 malicious software samples were distributed during the week, a decrease of 74.9% compared to last week's 3,024,798. 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	miner.usblfi26/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
2.	41.59.211.41	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
3.	102.208.164.38	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
4.	41.13.28.251	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
5.	41.59.149.187	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
6.	179.63.36.5	trojan.shell/abtrojan	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
7.	49.207.181.92	trojan.abrisk/qdhy	16d3440fcc067823afc44dcbccea9fbbc2f8c68ae53b7aea45f9adff4c127086
8.	187.205.3.57	sshd	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

9.	84.36.118.74	trojan.multiverze/r002c0db126	04a87c3c7f46947bdf38a2bc33a3b9c5bb32f6c43a04222459cc31b344300ca7
10.	41.32.15.166	trojan.ddos/abtrojan	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 38,164 web attacks were recorded, a decrease of 45.9% from last week's 70,519. 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.	69.5.20.93	/
2.	185.177.72.12	/SDK/webLanguage
3.	128.136.131.84	/robots.txt
4.	217.217.124.16	/favicon.ico
5.	188.166.176.239	/admin/config.php
6.	152.42.160.206	/cgi-bin/luci/;stok=/locale
7.	213.209.159.175	/config.php
8.	93.123.109.10	/.env
9.	209.97.175.120	/login
10.	80.94.95.211	/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 21,279 ICS attacks were recorded, a decrease of 16.7% from last week's 25,545. 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.	20.51.151.18	snmp	161
2.	34.166.142.134	guardian_ast	10001
3.	66.42.90.88	IEC104	2404
4.	45.205.1.211	kamstrup_protocol	1025
5.	45.198.224.209	kamstrup_management_protocol	50100

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)