TZ-CERT HONEYPOT WEEKLY REPORT

Period: 29th June – 5th July 2026 | **Report No.:** TZ-CERT/WRHP/2026/27

01: WEEKLY ATTACK SUMMARY

1,770,486	768,859	68,676	27,213
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 99.4% vs last week	↑ 20.4% vs last week	↑ 187.8% vs last week	↓ 88.0% vs last week

A total of 1,770,486 network attacks were recorded across all sensors during the period 29th June – 5th July 2026, representing an overall increase of 99.4% compared to last week's 887,731 attacks. While network and malware activity increased, web attacks increased significantly by 187.8% and ICS attacks fell by 88.0%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

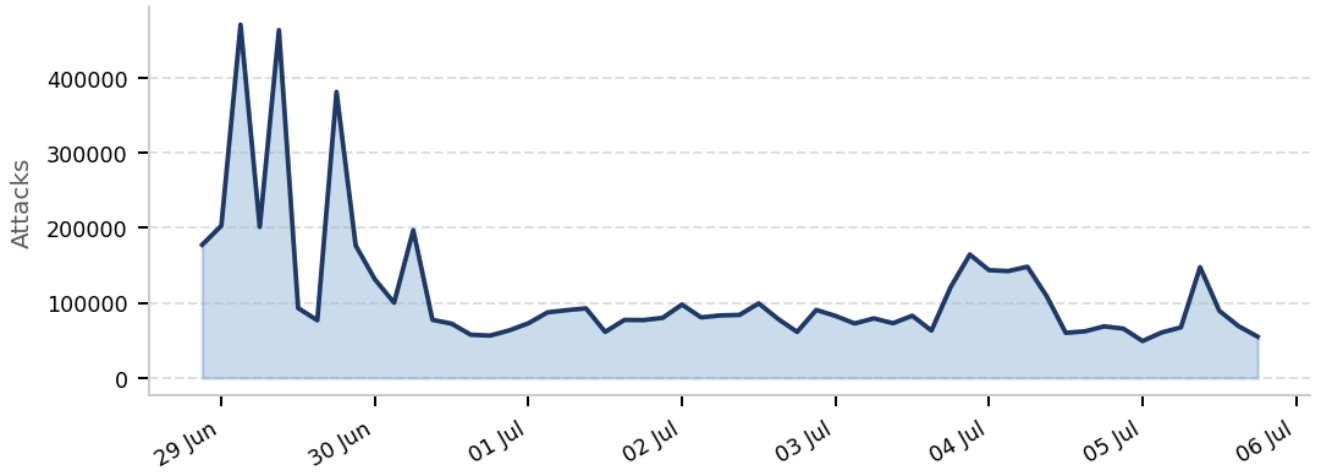

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,770,486 attacks have been recorded, up from last week's 887,731 by 99.4%. 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.	173.249.34.168	root	admin

2.	94.154.35.215	admin	123456
3.	203.145.47.222	user	password
4.	206.189.138.149	345gs5662d34	123
5.	45.142.142.140	ubuntu	345gs5662d34
6.	124.223.117.84	support	3245gs5662d34
7.	112.26.45.228	test	12345
8.	173.249.56.42	deploy	1234
9.	45.153.34.161	postgres	12345678
10.	45.153.34.167	tim	root

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 768,859 malicious software samples were distributed during the week, a increase of 20.4% compared to last week's 638,387. 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.shell/abtrojan	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	41.59.211.41	miner.usblfi26/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	125.62.195.4	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	112.133.193.230	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.59.196.23	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	102.208.164.38	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	41.111.198.198	trojan.	2d3211d104d3491df44ffcff9276f442c724d7fa9f4397a41746b588bb37f0c2
8.	196.201.235.78	trojan.abrisk/puwaders	f4efa9279ff58c03e75631fca5293c64d25f5eab9584a820dfefd6244b433bb6
9.	156.205.31.102	trojan.gafgyt/mirai	58e335e52961295e3bf5d35f3e2dfa9f53eaeebbdc961defa3887465040f7481

10.	4.235.0.198	7z.exe	ac9674feb8f2fad20c1e046de67f899419276ae79a60e8cc021a4bf472ae044f

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 68,676 web attacks were recorded, an increase of 187.8% from last week's 23,864. 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.	185.177.72.70	/
2.	185.177.72.52	/SDK/webLanguage
3.	163.7.11.230	/admin/config.php
4.	185.177.72.12	/robots.txt
5.	185.177.72.53	/favicon.ico
6.	185.177.72.29	/.env
7.	161.97.83.190	/login
8.	185.177.72.49	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	185.177.72.54	/vendor/phpunit/phpunit/Util/PHP/eval-stdin.php
10.	172.81.129.130	/laravel/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 27,213 ICS attacks were recorded, a decrease of 88.0% from last week's 227,236. 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.	45.198.224.209	snmp	161
2.	45.205.1.211	guardian_ast	10001
3.	193.168.198.33	IEC104	2404
4.	185.165.50.30	ipmi	623
5.	69.166.3.202	kamstrup_protocol	1025

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)