TZ-CERT HONEYPOT WEEKLY REPORT

Period: 6th – 12th July 2026 | **Report No.:** TZ-CERT/WRHP/2026/28

01: WEEKLY ATTACK SUMMARY

1,240,860	683,422	245,710	35,255
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 29.9% vs last week	↓ 11.1% vs last week	↑ 257.8% vs last week	↑ 29.6% vs last week

A total of 1,240,860 network attacks were recorded across all sensors during the period 6th – 12th July 2026, representing an overall decrease of 29.9% compared to last week's 1,770,486 attacks. While network and malware activity declined, web attacks increased significantly by 257.8% and ICS attacks rose by 29.6%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

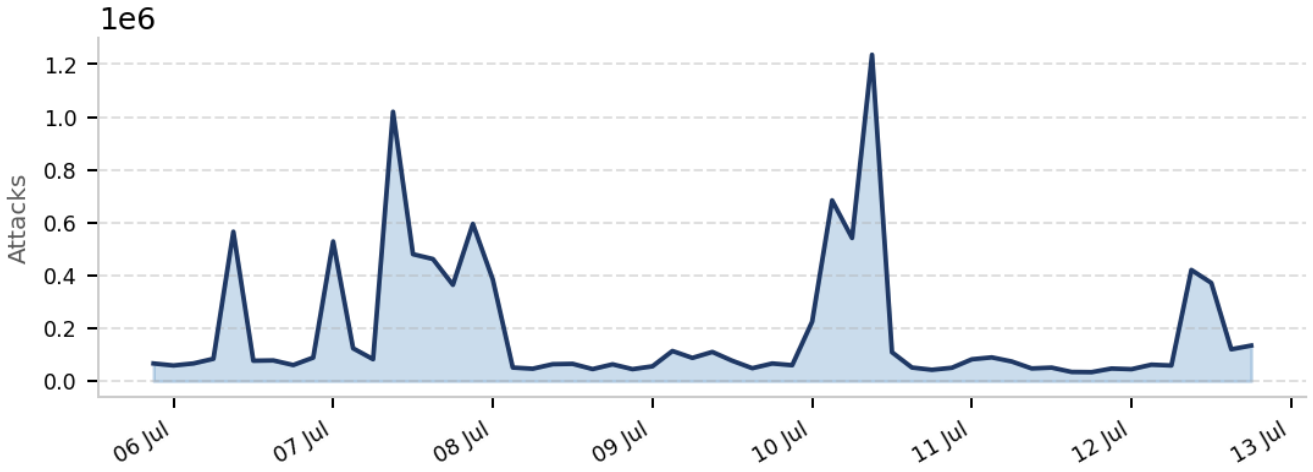

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,240,860 attacks have been recorded, down from last week's 1,770,486 by 29.9%. 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	123456

2.	5.189.187.100	admin	123
3.	207.180.229.95	support	1234
4.	173.249.56.42	ubuntu	support
5.	94.154.35.215	user	password
6.	91.92.40.25	345gs5662d34	admin
7.	155.103.69.40	test	12345678
8.	91.92.40.31	deploy	12345
9.	91.92.40.29	tim	345gs5662d34
10.	91.92.42.133	postgres	3245gs5662d34

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 683,422 malicious software samples were distributed during the week, a decrease of 11.1% compared to last week's 768,859. 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/shell	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	41.59.211.41	miner.usblfi26/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.59.196.23	trojan.usblg926/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	122.179.207.10	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.33.89.62	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.59.26.80	trojan.shell/abtrojan	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	41.231.8.19	trojan.mirai/cryp	77ed8c7518a32663fb766f729075dcdddc355c8d6ebe381092df51bb891e0cfc
8.	196.201.235.91	downloader.medusa/shell	889f8101436dbf4c3d7bf4a8ed9c399bbacedaaf0c64c731eeebcd2cee6f435b
9.	41.111.198.172	trojan.mirai/ddos	40db9279ba409757c074048529be5bf8f141fa022489a965792e7f7de2223b78

10.	41.138.55.126	trojan.mirai/ddos	7a4a3a129b726b531941b41d734521e8905d57a57a7e8a0a7e5dff41ed22f6ba

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 245,710 web attacks were recorded, an increase of 257.8% from last week's 68,676. 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.	24.50.57.216	/
2.	167.172.219.82	/users/sign_in
3.	185.177.72.23	/assets/favicon-7901bd695fb93edb07975966062049829afb56cf11511236e61bcf425070e36e.png
4.	45.148.10.201	/users
5.	185.177.72.69	/explore/projects/starred
6.	185.177.72.22	/users/password
7.	185.177.72.66	/users/confirmation
8.	185.177.72.17	/explore/projects
9.	173.249.52.2	/explore
10.	185.177.72.49	/search

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 35,255 ICS attacks were recorded, an increase of 29.6% from last week's 27,213. 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.	217.60.199.225	snmp	161
2.	69.166.3.202	ipmi	623
3.	172.69.170.228	guardian_ast	10001
4.	194.110.115.52	kamstrup_protocol	1025
5.	217.103.191.135	IEC104	2404

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)