



TZ-CERT HONEYPOT WEEKLY REPORT

Period: 1st – 7th June 2026 | Report No.: TZ-CERT/WRHP/2026/23

01: WEEKLY ATTACK SUMMARY

1,181,047	568,626	97,199	13,948
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 38.3% vs last week	↑ 51.0% vs last week	↓ 13.9% vs last week	↑ 183.0% vs last week

A total of 1,181,047 network attacks were recorded across all sensors during the period 1st – 7th June 2026, representing an overall increase of 38.3% compared to last week's 853,976 attacks. While network and malware activity increased, web attacks decreased by 13.9% and ICS attacks rose by 183.0%, 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 1,181,047 attacks have been recorded, up from last week's 853,976 by 38.3%. 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.	38.95.14.214	root	(blank)

2.	37.120.214.30	(blank)	123456
3.	124.228.139.47	admin	support
4.	87.251.64.176	support	123
5.	103.64.129.98	user	3245gs5662d34
6.	139.59.86.13	345gs5662d34	345gs5662d34
7.	94.154.35.215	ubuntu	1234
8.	45.87.249.200	test	admin
9.	176.65.132.149	deploy	password
10.	176.65.132.24	0	1

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 568,626 malicious software samples were distributed during the week, a increase of 51.0% compared to last week's 376,611. 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/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.33.100.50	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	173.230.225.13	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	102.208.164.38	trojan.usblem26/abminer	59c29436755b0778e968d49feae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.59.149.85	trojan.alevail/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e5086528eeedeab7e0d59
7.	41.90.15.238	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
8.	185.155.14.112	miner.r06ec0dkh25/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
9.	41.111.224.129	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

10.	160.30.109.30	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
-----	---------------	-----------------------	--

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 97,199 web attacks were recorded, a decrease of 13.9% from last week's 112,919. 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.	163.7.5.166	/
2.	151.104.34.102	/login
3.	93.123.109.10	/robots.txt
4.	185.177.72.38	/.git/config
5.	185.177.72.13	/cgi-bin/luci;/stok=/locale
6.	163.7.3.220	/SDK/webLanguage
7.	101.47.29.104	/admin/config.php
8.	185.177.72.53	/.git/config
9.	185.177.72.16	/admin/.git/config
10.	185.177.72.24	/administrator/.git/config

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 13,948 ICS attacks were recorded, an increase of 183.0% from last week's 4,928. 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.	45.95.147.229	snmp	161
2.	45.205.1.211	guardian_ast	10001
3.	45.198.224.209	ipmi	623
4.	185.214.135.16	kamstrup_protocol	1025
5.	167.86.126.236	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)