TZ-CERT HONEYPOT WEEKLY REPORT

Period: 31st August – 6th September 2026 | **Report No.:** TZ-CERT/WRHP/2026/36

01: WEEKLY ATTACK SUMMARY

76,515	40,056	13,367	1,058
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 18.6% vs last week	↓ 81.3% vs last week	↓ 67.7% vs last week	↓ 17.3% vs last week

A total of 76,515 network attacks were recorded across all sensors during the period 31st August – 6th September 2026, representing an overall decrease of 18.6% compared to last week's 94,047 attacks. While network and malware activity declined, web attacks decreased significantly by 67.7% and ICS attacks fell by 17.3%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

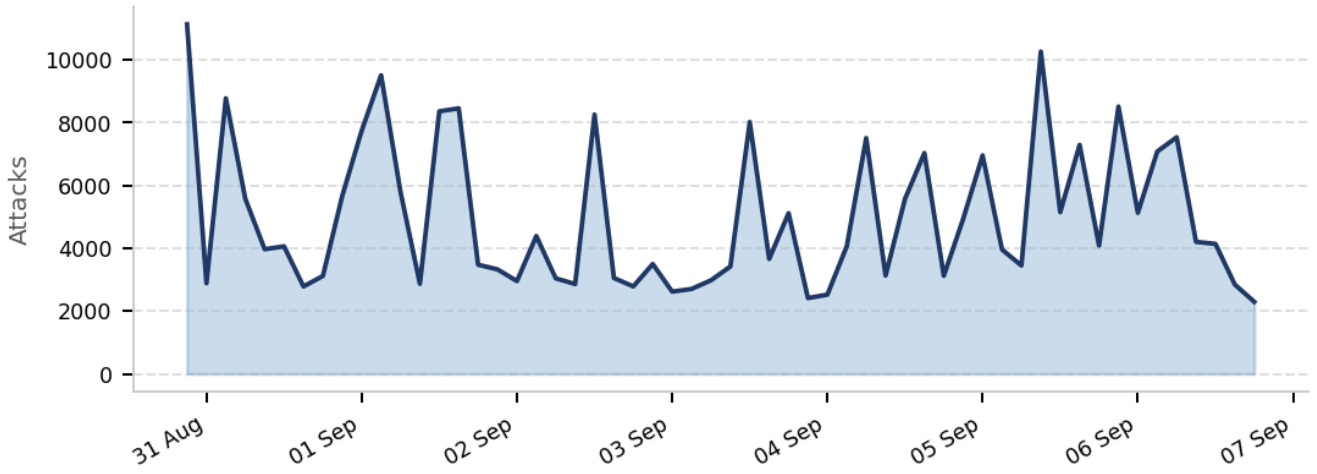

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 76,515 attacks have been recorded, down from last week's 94,047 by 18.6%. 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.	94.154.35.215	root	0
2.	77.239.124.212	admin	admin
3.	77.239.124.185	0	123456
4.	77.239.124.214	user	1234
5.	77.239.124.211	ubuntu	123
6.	77.239.124.180	monitor	monitor@123
7.	45.156.87.166	test	password
8.	45.156.87.93	deploy	12345
9.	195.178.110.232	debian	12345678
10.	185.246.128.133	postgres	root

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 40,056 malicious software samples were distributed during the week, a decrease of 81.3% compared to last week's 214,020. 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.	102.164.197.183	sshd	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
2.	102.33.154.14	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
3.	102.33.31.158	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
4.	102.141.184.217	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
5.	91.218.35.116	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
6.	102.33.152.162	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
7.	102.165.118.54	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
8.	204.157.173.61	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d

9.	189.236.43.72	miner.multiverze/r06ec0di626	0098cfff9e6056e6cf9e1e34a798110a2b6b42fca27652eeabc5bbcbe11b6be2
10.	102.213.71.210	trojan.multiverze	562b46ab24e657a837f5bdf84cbe91190aac46722c2463183e6d680b836a03f0

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 13,367 web attacks were recorded, a decrease of 67.7% from last week's 41,359. 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.	157.245.193.226	/
2.	194.180.49.37	/admin/config.php
3.	34.158.112.220	/.env
4.	35.194.98.172	/favicon.ico
5.	34.156.126.130	/robots.txt
6.	104.199.244.161	/102.214.45.254/.env
7.	45.148.10.238	/SDK/webLanguage
8.	213.209.159.154	/user/login
9.	151.243.11.168	/.git/config
10.	161.118.211.202	/fetch

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,058 ICS attacks were recorded, a decrease of 17.3% from last week's 1,280. 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.	172.104.229.235	guardian_ast	10001
2.	151.80.234.64	kamstrup_protocol	1025
3.	18.218.118.203	kamstrup_management_protocol	50100
4.	3.131.220.121	IEC104	2404
5.	3.130.168.2	ipmi	623

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)