TZ-CERT HONEYPOT WEEKLY REPORT

Period: 7th – 13th September 2026 | **Report No.:** TZ-CERT/WRHP/2026/37

01: WEEKLY ATTACK SUMMARY

135,672	288,278	8,770	999
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 77.3% vs last week	↑ 619.7% vs last week	↓ 34.4% vs last week	↓ 5.6% vs last week

A total of 135,672 network attacks were recorded across all sensors during the period 7th – 13th September 2026, representing an overall increase of 77.3% compared to last week's 76,515 attacks. While network and malware activity increased, web attacks decreased significantly by 34.4% and ICS attacks fell by 5.6%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

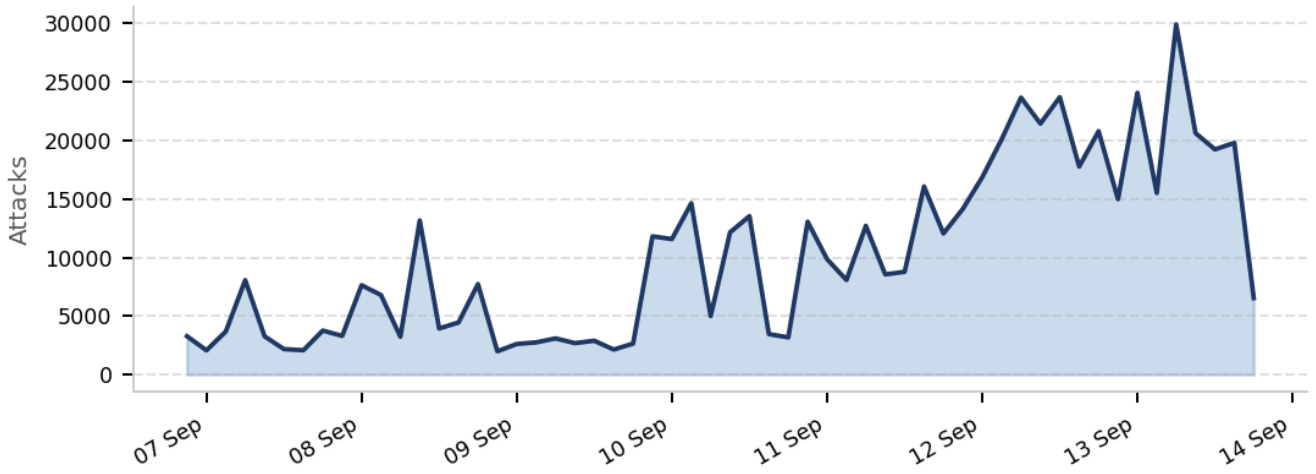

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 135,672 attacks have been recorded, up from last week's 76,515 by 77.3%. 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.	109.160.32.73	root	admin
2.	109.160.32.78	admin	123456
3.	109.160.32.72	ubuntu	123
4.	109.160.32.101	user	1234
5.	77.239.124.184	deploy	password
6.	77.239.124.205	test	12345678
7.	77.239.124.210	0	12345
8.	77.239.124.178	bitrix	root
9.	77.239.124.201	postgres	1
10.	77.239.124.173	guest	0

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 288,278 malicious software samples were distributed during the week, a increase of 619.7% compared to last week's 40,056. 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.	102.214.233.167	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
2.	102.165.118.54	miner.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
3.	102.164.197.183	miner.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
4.	102.214.233.161	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
5.	102.33.31.174	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	102.85.116.8	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
7.	102.88.109.159	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
8.	102.214.233.138	miner.multiverze/usblfg26	337ae3a4fe38c75acad6fac00db69046a8da0341524df34431a8b46f90896022

9.	102.214.233.129	trojan.multiverze/malxmr	629db57b96d6e965401d866f895d86c542efe344b3d489630a6ec09d643add76
10.	102.214.233.148	trojan.multiverze/usblfj26	c949ac977d557d58529d098862ae8a257474f2600b4afedac0c8b5b543d07035

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 8,770 web attacks were recorded, a decrease of 34.4% from last week's 13,367. 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.	34.83.179.105	/
2.	34.84.2.226	/admin/config.php
3.	195.178.110.28	/favicon.ico
4.	213.209.159.175	/.env
5.	151.243.11.159	/SDK/webLanguage
6.	151.243.11.156	/robots.txt
7.	151.243.11.152	/modules/faxnew/lang
8.	151.243.11.157	/boaform/admin/formLogin
9.	151.243.11.166	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	151.243.11.161	/.env.local

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 999 ICS attacks were recorded, a decrease of 5.6% from last week's 1,058. 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.	45.79.2.244	kamstrup_protocol	1025
2.	45.205.1.242	guardian_ast	10001
3.	18.116.101.220	IEC104	2404
4.	3.129.187.38	ipmi	623
5.	3.130.168.2	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)