



TZ-CERT HONEYPOT WEEKLY REPORT

Period: 5th to 11th October 2026

Report No.: TZ-CERT/WRHP/2026/41

01: WEEKLY ATTACK SUMMARY

1,542,850	525,478	93,589	184,746
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 14.1% vs last week	↓ 28.8% vs last week	↓ 21.3% vs last week	↓ 72.4% vs last week

A total of 1,542,850 network attacks were recorded across all sensors during the period 5th to 11th October 2026, representing a decrease of 14.1% compared to last week's 1,797,046 attacks. Malware activity declined by 28.8%, web attacks decreased by 21.3% and ICS attacks fell by 72.4%. The decline was broad-based, with no category recording an increase.

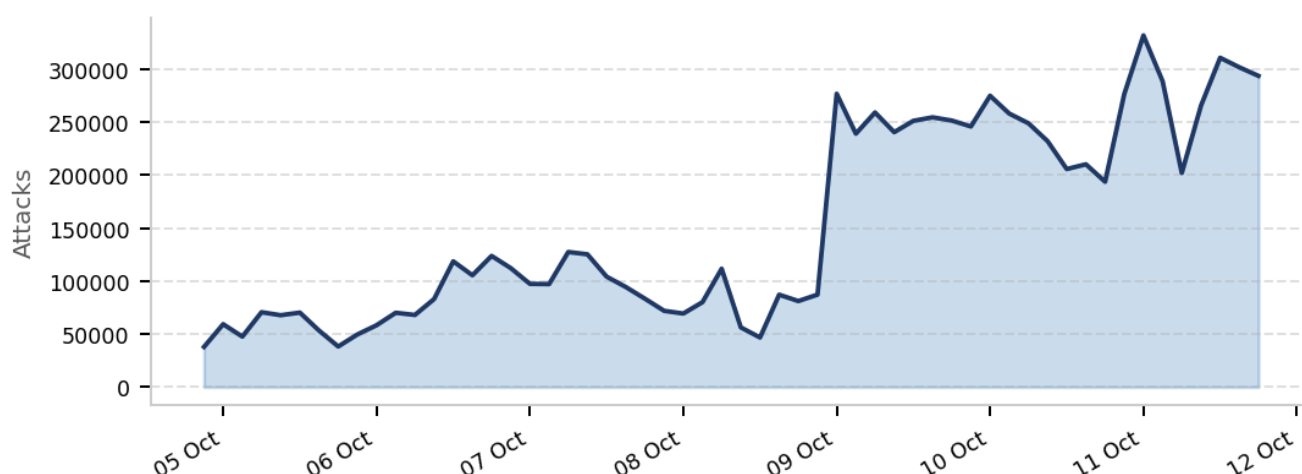


Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,542,850 attacks have been recorded, down from last week's 1,797,046 by 14.1%. The top 10 attacking IPs and the most frequently attempted usernames and passwords are listed below; each column is ranked independently by frequency. Most credentials used are default or weak, so enforcement of password policies is strongly advised.

SN	ATTACKING IP	TOP USERNAMES	TOP PASSWORDS
----	--------------	---------------	---------------

1.	160.119.66.206	root	admin
2.	179.43.133.154	admin	123456
3.	34.56.229.114	enable	linuxshell
4.	77.239.124.205	system	sh
5.	186.182.105.49	ubuntu	1234
6.	109.160.32.144	345gs5662d34	345gs5662d34
7.	109.160.32.165	user	3245gs5662d34
8.	109.160.32.125	0	123
9.	109.160.32.127	a	password
10.	109.160.32.102	test	12345

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 525,478 malicious software samples were distributed during the week, a decrease of 28.8% compared to last week's 737,707. The top ten attacking IPs and, ranked separately, the ten most frequently downloaded malware samples with their SHA256 hashes are listed below for threat hunting and IOC correlation.

SN	ATTACKING IP	MALICIOUS SOFTWARE	SHA256 HASH
1.	130.94.17.236	trojan.bash/miraia	39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96
2.	41.230.10.221	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
3.	102.208.164.221	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
4.	41.93.63.66	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdf5e94dd39
5.	102.204.162.45	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
6.	130.94.17.139	trojan.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
7.	213.209.159.136	trojan.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
8.	179.63.84.194	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987

9.	130.94.123.239	Unidentified	b554626d55b7f6104c10217c4f3d61dec4228e803cf9ac4aa4051d6df681ce37
10.	114.143.191.142	downloader.medusa/shell	61aeef0d535d309f4bdda6278a7da4ef9d67674a46b619065b88171ee5c0f581

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 93,589 web attacks were recorded, a decrease of 21.3% from last week's 118,901. The top 10 attacking IPs and the most requested URIs are detailed below, each ranked independently. Notable activity includes environment file (.env) enumeration.

SN	ATTACKING IP	TOP URI / REQUEST
1.	176.65.134.56	/login.cgi
2.	139.87.112.212	/
3.	139.87.112.167	/login
4.	102.220.161.102	/favicon.ico
5.	185.177.72.75	/robots.txt
6.	185.177.72.56	/admin/config.php
7.	45.148.10.238	/.env
8.	195.178.110.28	/config.php
9.	217.60.76.167	/users/sign_in
10.	159.65.123.254	/userlogin.action

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 184,746 ICS attacks were recorded, a decrease of 72.4% from last week's 669,509. The top 5 attacking IPs and, ranked separately, the most targeted industrial protocols with their ports 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.	217.154.232.129	snmp	161
2.	68.66.226.115	ipmi	623
3.	43.249.194.22	IEC104	2404
4.	43.249.195.72	kamstrup_protocol	1025
5.	102.220.163.10	guardian_ast	10001

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)