TZ-CERT HONEYPOT WEEKLY REPORT

Period: 19th to 25th October 2026 | **Report No.:** TZ-CERT/WRHP/2026/43

01: WEEKLY ATTACK SUMMARY

2,368,754	1,358,815	73,695	223,626
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 39.6% vs last week	↓ 26.1% vs last week	↑ 18.5% vs last week	↑ 372.6% vs last week

A total of 2,368,754 network attacks were recorded across all sensors during the period 19th to 25th October 2026, representing an increase of 39.6% compared to last week's 1,696,649 attacks. Malware activity declined by 26.1%, web attacks increased by 18.5% and ICS attacks rose by 372.6%. This divergence indicates a shift in adversary focus toward network services, web-facing assets and industrial control systems.



Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 2,368,754 attacks have been recorded, up from last week's 1,696,649 by 39.6%. 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.	94.101.184.248	root	123456
2.	217.60.255.130	admin	345gs5662d34
3.	164.30.17.82	ubuntu	3245gs5662d34
4.	160.119.66.206	345gs5662d34	123
5.	103.119.142.252	user	1234
6.	179.43.133.154	enable	linuxshell
7.	39.125.93.26	system	admin
8.	179.41.10.172	deploy	password
9.	109.160.32.173	test	12345678
10.	109.160.32.48	0	root

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 1,358,815 malicious software samples were distributed during the week, a decrease of 26.1% compared to last week's 1,838,238. 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.	162.250.126.218	trojan.bash/miraia	39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96
2.	41.59.203.60	Unidentified	3accfc75eafdd42868d76890ac0d8610c27757bda1180d8e8141aeef3ef149f4
3.	102.208.164.221	trojan.abtrojan/njww	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
4.	93.123.109.6	miner.abminer/eezv	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
5.	41.111.198.102	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	41.59.196.23	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
7.	94.153.202.122	trojan.abminer/gen3	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
8.	41.112.173.136	trojan.sagent/abtrojan	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d

9.	88.30.66.3	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
10.	95.9.227.252	miner.malxmr/rootkit	a151d3f4f2422531f30a843ffb35479596c86722bb103bdf8591105687f9b125

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 73,695 web attacks were recorded, an increase of 18.5% from last week's 62,209. 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.	102.220.163.155	/
2.	77.90.185.244	/admin/config.php
3.	195.178.110.137	/robots.txt
4.	77.90.185.243	/favicon.ico
5.	185.177.72.38	/index.php
6.	217.60.77.84	/.env
7.	45.148.10.238	/SDK/webLanguage
8.	87.58.199.133	/.git/config
9.	185.177.72.64	/images
10.	91.92.47.232	/contact

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 223,626 ICS attacks were recorded, an increase of 372.6% from last week's 47,322. 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.	83.81.66.128	snmp	161
2.	184.57.175.112	IEC104	2404
3.	47.221.75.43	guardian_ast	10001
4.	98.121.52.145	ipmi	623
5.	47.184.47.80	kamstrup_protocol	1025

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)