TZ-CERT HONEYPOT WEEKLY REPORT

Period: 26th October to 1st November 2026 | **Report No.:** TZ-CERT/WRHP/2026/44

01: WEEKLY ATTACK SUMMARY

2,224,859	874,348	65,903	2,822,022
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 6.1% vs last week	↓ 35.7% vs last week	↓ 10.6% vs last week	↑ 1161.9% vs last week

A total of 2,224,859 network attacks were recorded across all sensors during the period 26th October to 1st November 2026, representing a decrease of 6.1% compared to last week's 2,368,754 attacks. Malware activity declined by 35.7%, web attacks decreased by 10.6% and ICS attacks rose by 1161.9%. This divergence indicates a shift in adversary focus toward industrial control systems.

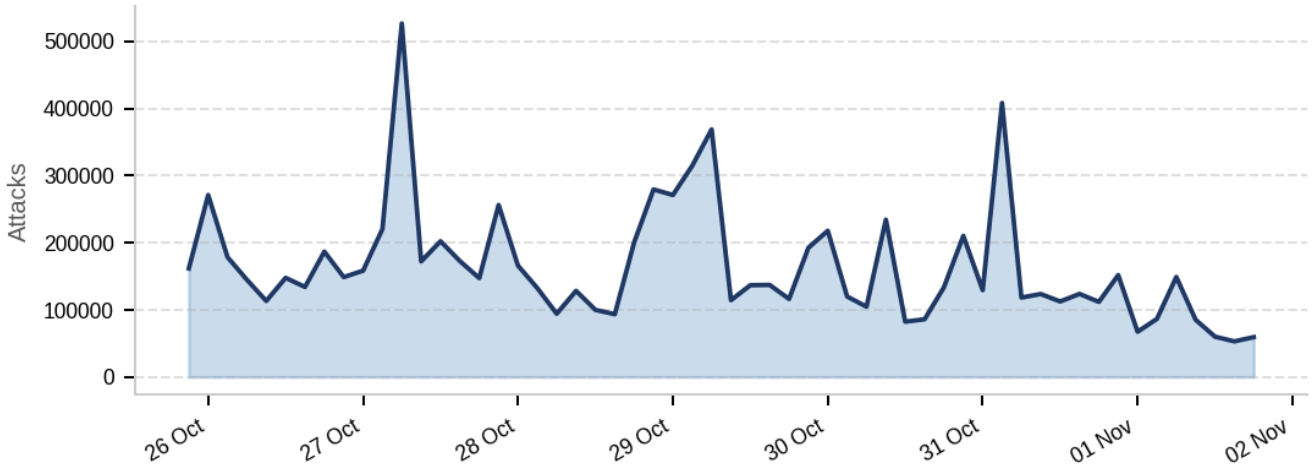


Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 2,224,859 attacks have been recorded, down from last week's 2,368,754 by 6.1%. 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.	94.101.184.248	root	123456
2.	196.191.44.250	admin	345gs5662d34
3.	95.81.101.173	user	3245gs5662d34
4.	109.160.32.148	ubuntu	123
5.	109.160.32.36	345gs5662d34	1234
6.	109.160.32.165	deploy	admin
7.	109.160.32.200	0	password
8.	77.239.124.147	test	12345678
9.	109.160.32.162	support	0
10.	109.160.32.108	user1	12345

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 874,348 malicious software samples were distributed during the week, a decrease of 35.7% compared to last week's 1,358,815. 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.	41.59.203.60	miner.malxmr/rootkit	a151d3f4f2422531f30a843ffb35479596c86722bb103bdf8591105687f9b125
2.	138.226.239.47	trojan.mirai/ddos	45075a965b00a8f0248dd4f40ea3621d58cefad5329ac86bf42caacc95729090
3.	41.93.68.98	trojan.sagent/abtrojan	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
4.	185.136.15.31	trojan.qwexlafiba/abtrojan	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
5.	102.208.164.221	trojan.multiverze/abminer	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
6.	103.183.15.11	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
7.	41.59.196.23	trojan.abminer/gen3	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
8.	194.8.129.16	trojan.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141

9.	138.226.239.46	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987
10.	138.226.239.44	trojan.shell/sbadur	17bcfccaff1a9aee3dfdc17e38ee5017d6a88e39594c1ec0859e18d5e259c6af

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 65,903 web attacks were recorded, a decrease of 10.6% from last week's 73,695. 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.	195.178.110.247	/
2.	45.148.10.238	/.aws/config
3.	185.177.72.64	/admin/config.php
4.	102.220.163.241	/favicon.ico
5.	93.152.223.44	/.env
6.	45.61.178.105	/robots.txt
7.	193.47.62.29	/logon.htm
8.	103.215.74.112	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	217.60.76.167	/.git/config
10.	45.138.12.51	/contact

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 2,822,022 ICS attacks were recorded, an increase of 1161.9% from last week's 223,626. 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.	104.220.45.158	snmp	161
2.	35.214.45.45	IEC104	2404
3.	141.153.237.4	kamstrup_protocol	1025
4.	70.179.242.118	guardian_ast	10001
5.	172.249.143.85	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)