



TZ-CERT HONEYPOT WEEKLY REPORT

Period: 12th to 18th October 2026

Report No.: TZ-CERT/WRHP/2026/42

01: WEEKLY ATTACK SUMMARY

1,696,649	1,838,238	62,209	47,322
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 10.0% vs last week	↑ 249.8% vs last week	↓ 33.5% vs last week	↓ 74.4% vs last week

A total of 1,696,649 network attacks were recorded across all sensors during the period 12th to 18th October 2026, representing an increase of 10.0% compared to last week's 1,542,850 attacks. Malware activity increased by 249.8%, web attacks decreased significantly by 33.5% and ICS attacks fell by 74.4%. This divergence indicates a shift in adversary focus toward network services and malware distribution.



Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,696,649 attacks have been recorded, up from last week's 1,542,850 by 10.0%. 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.	179.43.133.154	root	123456
2.	109.160.32.109	admin	admin
3.	77.239.124.34	0	0
4.	77.239.124.68	ubuntu	1234
5.	77.239.124.45	345gs5662d34	123
6.	77.239.124.37	user	345gs5662d34
7.	77.239.124.148	test	3245gs5662d34
8.	77.239.124.152	support	password
9.	77.239.124.40	deploy	12345
10.	109.160.32.114	enable	12345678

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 1,838,238 malicious software samples were distributed during the week, an increase of 249.8% compared to last week's 525,478. 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.	130.94.17.236	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
3.	102.208.164.221	trojan.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
4.	93.123.109.6	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
5.	197.57.136.114	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdf5e94dd39
6.	102.165.118.54	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
7.	213.209.159.136	trojan.abminer/gen3	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
8.	102.207.245.190	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987

9.	103.129.101.48	downloader.	7808ec829803b8269d7a207adb3054c87889832f345037ca4890b4b44f2eda92
10.	78.186.165.39	trojan.multiverze/abapplication	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 62,209 web attacks were recorded, a decrease of 33.5% from last week's 93,589. The top 10 attacking IPs and the most requested URIs are detailed below, each ranked independently. Notable activity includes environment file (.env) enumeration and CGI endpoint probing.

SN	ATTACKING IP	TOP URI / REQUEST
1.	91.92.47.232	/
2.	45.148.10.238	/admin/config.php
3.	87.58.199.133	/favicon.ico
4.	45.138.12.51	/robots.txt
5.	185.177.72.24	/.env
6.	185.177.72.31	/102.223.7.68/.env
7.	185.177.72.75	/102.207.206.92/.env
8.	155.117.232.31	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	147.224.153.167	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
10.	45.153.34.190	/.git/config

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 47,322 ICS attacks were recorded, a decrease of 74.4% from last week's 184,746. 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.	202.189.15.237	snmp	161
2.	43.249.194.22	ipmi	623
3.	69.166.3.202	IEC104	2404
4.	194.50.16.198	guardian_ast	10001
5.	183.129.171.170	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)