TZ-CERT HONEYPOT WEEKLY REPORT

Period: 14th to 20th September 2026 | **Report No.:** TZ-CERT/WRHP/2026/38

01: WEEKLY ATTACK SUMMARY

138,331	371,714	7,984	1,088
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 2.0% vs last week	↑ 28.9% vs last week	↓ 9.0% vs last week	↑ 8.9% vs last week

A total of 138,331 network attacks were recorded across all sensors during the period 14th to 20th September 2026, representing an increase of 2.0% compared to last week's 135,672 attacks. Malware activity increased by 28.9%, web attacks decreased by 9.0% and ICS attacks rose by 8.9%. This divergence indicates a shift in adversary focus toward network services, malware distribution and industrial control systems.

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 138,331 attacks have been recorded, up from last week's 135,672 by 2.0%. 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.	109.160.32.40	root	123456
2.	109.160.32.109	admin	admin
3.	109.160.32.102	ubuntu	123
4.	109.160.32.32	user	1234
5.	109.160.32.107	0	0
6.	109.160.32.23	deploy	password
7.	109.160.32.67	test	12345678
8.	77.239.124.202	system	1
9.	109.160.32.210	enable	12345
10.	77.239.124.179	claude	root

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 371,714 malicious software samples were distributed during the week, an increase of 28.9% compared to last week's 288,278. 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.	102.214.233.167	downloader.bash/miraia	39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96
2.	165.165.145.171	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
3.	102.165.118.54	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
4.	102.214.233.161	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39
5.	102.214.233.138	trojan.abminer/gen3	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
6.	102.47.37.64	trojan.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
7.	41.38.21.187	miner.abminer/eezv	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
8.	102.214.233.148	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcfad59f3a8efa30a500b815f0f6c18d987

9.	102.214.233.129	miner.multiverze/usblf426	0670da04a700a5e7ec0ca80de285d75985116b669dc02c61cebfc22b5b3edab3
10.	102.214.233.176	miner.camelot/mirai	28536204a1922034ce95fb20c72d13eefc867cf353136f029c5aa3d6c973e077

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 7,984 web attacks were recorded, a decrease of 9.0% from last week's 8,770. 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.	196.251.121.237	/
2.	169.58.252.154	/admin/config.php
3.	188.166.248.40	/SDK/webLanguage
4.	2.58.56.69	/favicon.ico
5.	146.235.21.143	/.env
6.	213.209.159.154	/config.json
7.	193.24.123.123	/contact
8.	45.198.224.234	/core/misc/favicon.ico
9.	151.243.11.169	/user/login
10.	45.198.224.238	/.aws/credentials

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,088 ICS attacks were recorded, an increase of 8.9% from last week's 999. 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.	165.227.19.8	IEC104	2404
2.	45.79.143.28	guardian_ast	10001
3.	3.129.187.38	kamstrup_protocol	1025
4.	216.180.246.84	kamstrup_management_protocol	50100
5.	45.40.57.23	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)