TZ-CERT HONEYPOT WEEKLY REPORT

Period: 21st to 27th September 2026 | **Report No.:** TZ-CERT/WRHP/2026/39

01: WEEKLY ATTACK SUMMARY

1,382,166	712,394	106,858	399,394
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 899.2% vs last week	↑ 91.7% vs last week	↑ 1238.4% vs last week	↑ 36609.0% vs last week

A total of 1,382,166 network attacks were recorded across all sensors during the period 21st to 27th September 2026, representing an increase of 899.2% compared to last week's 138,331 attacks. Malware activity increased by 91.7%, web attacks increased significantly by 1238.4% and ICS attacks rose by 36609.0%. The increase was broad-based, with no category recording a decline.

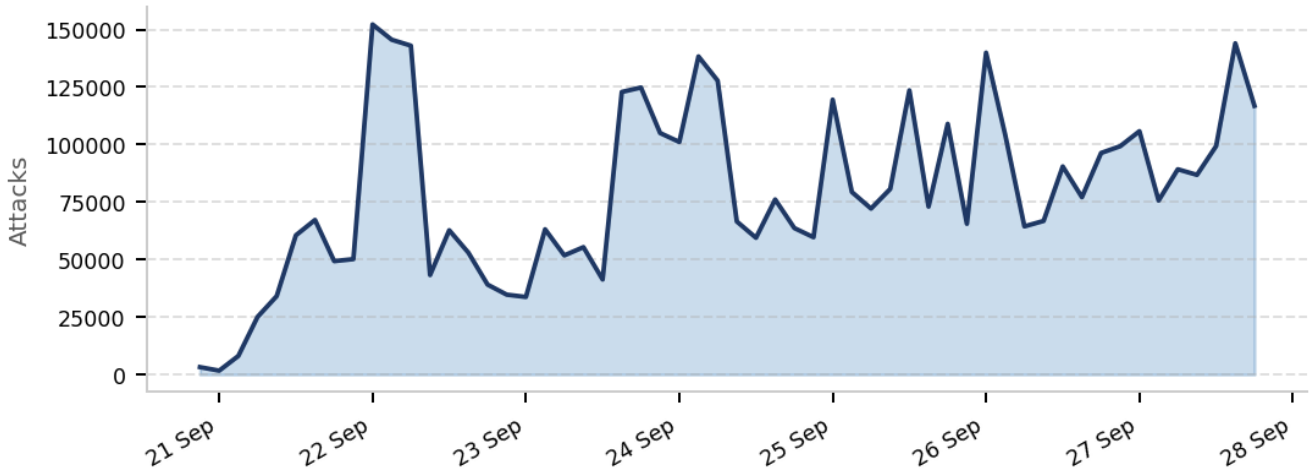

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,382,166 attacks have been recorded, up from last week's 138,331 by 899.2%. 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.	185.209.72.72	root	123456
2.	160.119.66.206	admin	admin
3.	154.18.197.29	ubuntu	1234
4.	91.92.242.247	user	123
5.	109.160.32.32	enable	password
6.	109.160.32.117	345gs5662d34	linuxshell
7.	109.160.32.19	deploy	345gs5662d34
8.	138.68.53.50	test	3245gs5662d34
9.	109.160.32.69	support	root
10.	109.160.32.17	postgres	12345678

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 712,394 malicious software samples were distributed during the week, an increase of 91.7% compared to last week's 371,714. 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.	113.80.87.224	Unidentified	7b4ae04eb682d8e28213d4fbc71ae63cb758535a00d28f1a5ea8b14a074736b0
3.	41.38.51.10	trojan.zapchast/abtrojan	37dd737a342729c7b8c4e6f28140f2ff977a433793482b6bd488efd56a20812e
4.	41.90.13.170	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
5.	103.59.75.63	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
6.	41.90.15.238	trojan.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
7.	31.166.16.185	trojan.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
8.	122.226.121.202	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdfe5e94dd39

9.	113.128.231.132	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
10.		Unidentified	a0b1be4b7ce45dfaf73072f253164bf213e8f41e30d7f2512e9a208254356729

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 106,858 web attacks were recorded, an increase of 1238.4% from last week's 7,984. 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.	176.65.134.56	/login.cgi
2.	198.58.161.203	/
3.	195.178.110.211	/favicon.ico
4.	185.177.72.23	/admin/config.php
5.	185.177.72.56	/robots.txt
6.	185.177.72.67	/digium_phones/ajax.php
7.	185.177.72.9	/SDK/webLanguage
8.	102.220.161.87	/logon.htm
9.	213.209.159.154	/.env
10.	185.177.72.64	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 399,394 ICS attacks were recorded, an increase of 36609.0% from last week's 1,088. 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.	73.245.133.130	snmp	161
2.	69.250.106.128	ipmi	623
3.	76.118.154.160	guardian_ast	10001
4.	76.236.228.92	IEC104	2404
5.	181.228.93.198	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)