



TZ-CERT HONEYPOT WEEKLY REPORT

Period: 28th Sept to 4th October 2026 | Report No.: TZ-CERT/WRHP/2026/40

01: WEEKLY ATTACK SUMMARY

1,797,046	737,707	118,901	669,509
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 30.0% vs last week	↑ 3.6% vs last week	↑ 11.3% vs last week	↑ 67.6% vs last week

A total of 1,797,046 network attacks were recorded across all sensors during the period 28th Sept to 4th October 2026, representing an increase of 30.0% compared to last week's 1,382,166 attacks. Malware activity increased by 3.6%, web attacks increased by 11.3% and ICS attacks rose by 67.6%. The increase was broad-based, with no category recording a decline.

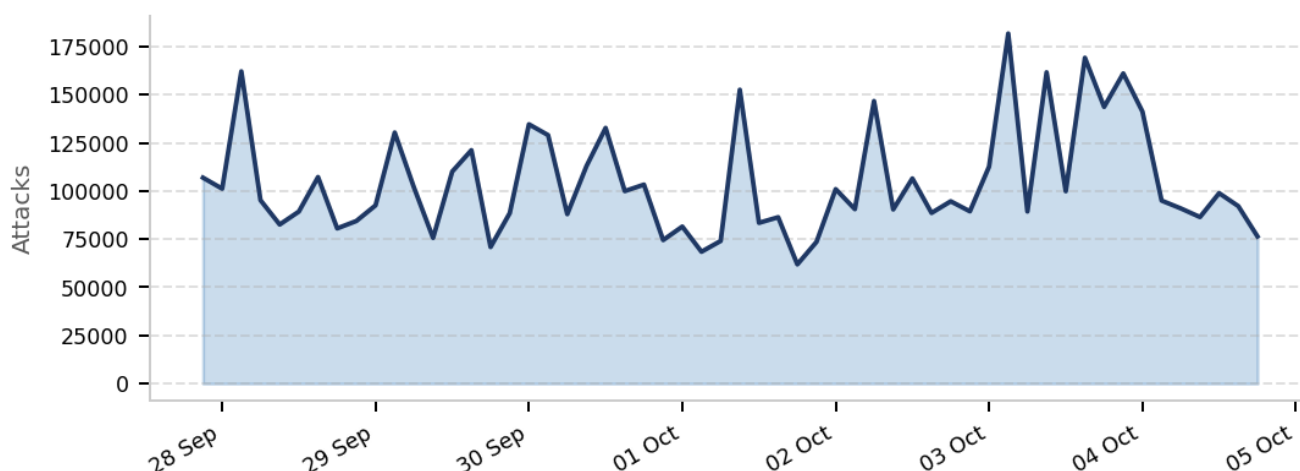


Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,797,046 attacks have been recorded, up from last week's 1,382,166 by 30.0%. 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.	185.130.83.218	root	123456
2.	185.209.72.72	admin	admin
3.	62.148.154.34	ubuntu	123
4.	77.91.122.10	user	1234
5.	137.184.226.118	345gs5662d34	345gs5662d34
6.	160.119.66.206	enable	3245gs5662d34
7.	77.239.124.144	system	linuxshell
8.	77.239.124.147	test	P@ssw0rd
9.	179.43.133.154	deploy	password
10.	109.160.32.107	support	12345678

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 737,707 malicious software samples were distributed during the week, an increase of 3.6% compared to last week's 712,394. 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.	102.214.233.188	trojan.bash/miraia	39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96
2.	138.226.239.47	trojan.sagent/shell	1e70b63472772e3f5092ffe9c3573470e73590e6ab6d93fdcede1d368a5fd72d
3.	130.12.180.51	trojan.qwexlafiba/shell	3f3a11bafabb1a35db913cfe51995f2e357d049e268860175876ae5a93d23892
4.	77.91.71.22	trojan.multiverze/usblh426	3f3bf218089d1488617d37f8a5116bb2791eb39ce06a1b5bc9a4cdf5e94dd39
5.	102.208.164.221	trojan.malxmr/usblgv26	8e1a67a5c03b3cd818f046c7a1605afccc0ee5ce437a0d099881f1872b54bc70
6.	77.91.71.15	trojan.malxmr/usblgv26	d1cac82f44b54b0fd244a9e4122811e9ae108a197c7a65a20fd2e7552683e68e
7.	185.136.15.31	trojan.r002c0xh226/abminer	d70f917e35813a7ae323e6b2b539d6dbbfc3a3a6599f1fed93430b14ca08b141
8.	102.207.245.190	trojan.malxmr/usblgv26	f0aa83bbbd2c75e2f71ec16029ee5fcad59f3a8efa30a500b815f0f6c18d987

9.	41.39.7.143	trojan.perl/shellbot	a37649842a47b8456a763c1b4878d08ea7ecee0ea861db2d7588f99f7e180cda
10.	213.209.159.136	downloader.	f74135143232bc1ac7c8c33f3394d5ffde9bef4aa4c7f4c5ad20bcde9332f5e2

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 118,901 web attacks were recorded, an increase of 11.3% from last week's 106,858. The top 10 attacking IPs and the most requested URIs are detailed below, each ranked independently. The requested paths indicate automated scanning for exposed applications and misconfigured endpoints.

SN	ATTACKING IP	TOP URI / REQUEST
1.	176.65.134.56	/login.cgi
2.	139.87.112.214	/
3.	195.178.110.53	/users/sign_in
4.	185.224.128.252	/login
5.	45.148.10.238	/user/login
6.	139.87.113.202	/Special:CreateAccount
7.	168.144.104.241	/login/
8.	217.60.76.167	/news/
9.	102.220.161.87	/assets/
10.	195.178.110.28	/comments?article_id=1

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 669,509 ICS attacks were recorded, an increase of 67.6% from last week's 399,394. 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 that requires immediate attention from critical infrastructure operators.

SN	ATTACKING IP	PROTOCOL EXPLOITED	PORT
1.	47.132.122.17	snmp	161
2.	75.185.96.114	IEC104	2404
3.	173.89.178.135	ipmi	623
4.	83.81.66.128	guardian_ast	10001
5.	174.51.118.68	kamstrup_management_protocol	50100

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)