TZ-CERT HONEYPOT WEEKLY REPORT

Period: 16th to 22nd November 2026 | **Report No.:** TZ-CERT/WRHP/2026/47

01: WEEKLY ATTACK SUMMARY

2,108,234	1,406,376	113,604	1,666,738
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 21.2% vs last week	↓ 59.9% vs last week	↑ 322.1% vs last week	↑ 44.6% vs last week

A total of 2,108,234 network attacks were recorded across all sensors during the period 16th to 22nd November 2026, representing an increase of 21.2% compared to last week's 1,739,117 attacks. Malware activity declined by 59.9%, web attacks increased significantly by 322.1% and ICS attacks rose by 44.6%. This divergence indicates a shift in adversary focus toward network services, web-facing assets and industrial control systems.

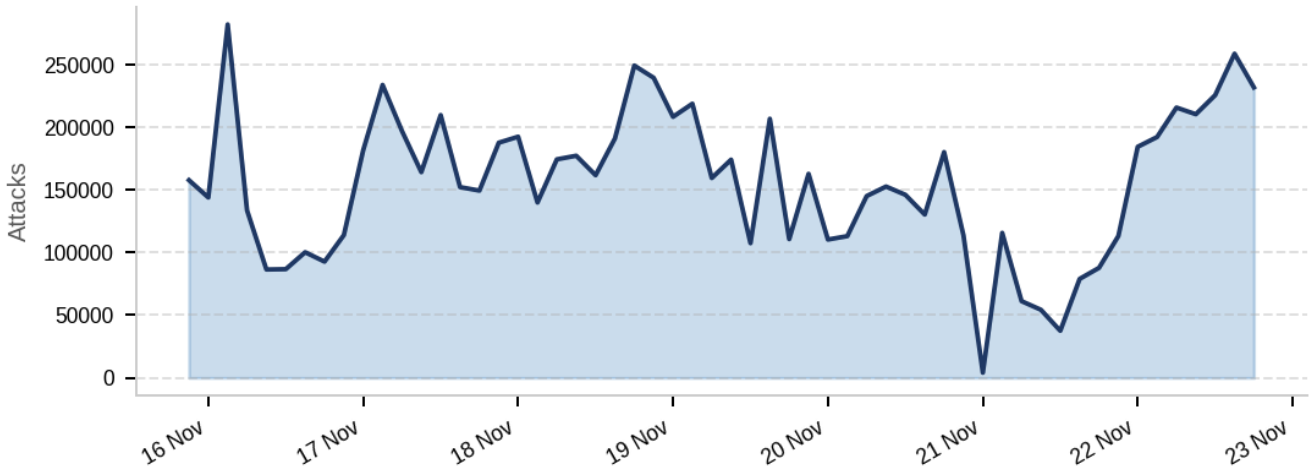


Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 2,108,234 attacks have been recorded, up from last week's 1,739,117 by 21.2%. 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.	103.174.238.226	root	123456
2.	103.163.215.105	admin	admin
3.	109.194.2.176	ubuntu	1234
4.	185.119.119.192	enable	linuxshell
5.	42.51.49.64	user	123
6.	177.39.159.245	system	sh
7.	160.119.66.206	deploy	root
8.	20.3.253.156	test	12345
9.	77.239.124.252	support	12345678
10.	179.43.133.154	0	password

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 1,406,376 malicious software samples were distributed during the week, a decrease of 59.9% compared to last week's 3,505,959. 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	downloader.bash/miraia	39be6853a8204ce6455a373a6ffb4cb4672d4a62d90be69f7d6eeb66cda10b96
2.	41.59.203.60	trojan.shell/vimw	d518ed82ee82796bcbf52bd8cd2c1a676d39e56efa97d47dfd0a8d7739adb1ff
3.	41.93.68.98	downloader.medusa/shell	dfa5c7a015b9c915a98388548fe708e8c816c0b7ee7464febafc463530ce75a1
4.	41.59.196.23	trojan.camelot/ktgl	28536204a1922034ce95fb20c72d13eefc867cf353136f029c5aa3d6c973e077
5.	41.10.182.159	trojan.	32b44db3980a94e1be989a4c5605cb2b3ed2db6cfa208943c70ae2a82d983291
6.	93.123.109.6	trojan.tsunami/flooder	9701ae7249aa394624bf33096e3f5dd2be0bb778debba3364f5277a50874cc31
7.	102.217.66.1	trojan.shell/czlw	c813b812f9383c189a840e0cffd8868ccd1989b3db0b56fc0f337495417ffee1
8.	201.97.67.200	trojan.multiverze/usblgj26	3f97d465f56417e08438bad7dc3c562293526826ae76d551267286b91d42822a

9.	93.110.131.106	trojan.mirai/multiverze	5fc5b46d8cd6e954aa74291e43ccb51d3d20eb0e4395032a5ff1d487977ffd07
10.	102.165.118.54	trojan.shell/camelot	809e8460deac450628a33b62cd7842201f033c346492941eff082817f914c0d6

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 113,604 web attacks were recorded, an increase of 322.1% from last week's 26,912. 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.	31.70.113.190	/
2.	45.198.224.153	/account/register
3.	94.26.106.224	/login
4.	185.224.128.198	/favicon.ico
5.	185.177.72.64	/admin/config.php
6.	195.178.110.28	/account/lost_password
7.	45.148.10.238	/robots.txt
8.	167.104.160.76	/.env
9.	85.11.167.204	/SDK/webLanguage
10.	102.220.163.241	/boaform/adminformLogout//boaform/admin/login.asp

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,666,738 ICS attacks were recorded, an increase of 44.6% from last week's 1,152,417. 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.	173.21.0.206	snmp	161
2.	97.97.206.118	guardian_ast	10001
3.	83.81.66.128	ipmi	623
4.	68.95.174.72	kamstrup_protocol	1025
5.	100.36.63.118	IEC104	2404

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)