TZ-CERT HONEYPOT WEEKLY REPORT

Period: 11th – 17th May 2026 | **Report No.:** TZ-CERT/WRHP/2026/20

01: WEEKLY ATTACK SUMMARY

840,269	552,647	21,864	8,302
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 28.9% vs last week	↓ 15.7% vs last week	↓ 32.5% vs last week	↓ 74.6% vs last week

A total of 840,269 network attacks were recorded across all sensors during the period 11th – 17th May 2026, representing an overall decrease of 28.9% compared to last week's 1,181,749 attacks. While network and malware activity declined, web attacks decreased significantly by 32.5% and ICS attacks fell by 74.6%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 840,269 attacks have been recorded, down from last week's 1,181,749 by 28.9%. The top 10 attacking IPs with commonly exploited credentials are listed below. Most credentials used are default or weak — enforcement of password policies is strongly advised.

SN	ATTACKING IP	USERNAME USED	PASSWORD USED
1.	51.75.240.111	root	support

2.	94.154.35.215	support	123456
3.	87.251.64.176	admin	345gs5662d34
4.	176.65.132.129	ubuntu	3245gs5662d34
5.	185.246.128.133	user	123
6.	176.65.132.17	345gs5662d34	click1
7.	45.153.34.97	sol	admin
8.	5.254.56.197	sync	password
9.	195.178.110.26	tim	dqi
10.	192.109.200.237	postgres	abc123

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 552,647 malicious software samples were distributed during the week, a decrease of 15.7% compared to last week's 655,907. The top ten malware families and their SHA256 hashes are listed below for threat hunting and IOC correlation.

SN	ATTACKING IP	MALICIOUS SOFTWARE	SHA256 HASH
1.	41.59.211.41	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.203.60	miner.r06ec0dkh25	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.93.63.66	miner.r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	113.87.153.241	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	118.70.190.1	trojan.malxmr/usblkh25	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	187.235.212.12	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	196.203.231.46	miner.shell	dccfd62d350184fc137b18acbdd56fceee07f2c7b7f89eb1071e7c4eb0f01bcd
8.	197.44.212.194	trojan.multiverze/tl0101ef26zz	09b30670c1bb2cd3512bb22102e58d404ee51c14830350940a91951839a302fb
9.	102.33.155.126	Linux.Siggen.10752	5e746047cc554099cfe1d138be53ec5a25d38436cdf917bc354d0bbaeb3f9ec8

10.	41.111.198.172	trojan.multiverze	b945645a3f62bca92a3869c236bcc943e44ece04cc7da5bc9709ce1191f04b36

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 21,864 web attacks were recorded, a decrease of 32.5% from last week's 32,404. The top 10 attacking IPs and their targeted URIs are detailed below. Notable activity includes environment file (.env) enumeration, Git repository configuration exposure attempts (/.git/config), PHPUnit remote code execution exploitation attempts (CVE-2017-9841) targeting eval-stdin.php, CGI path traversal attacks attempting to invoke /bin/sh, and reconnaissance against admin panels, SDK endpoints, and common web resources.

SN	ATTACKING IP	TOP URI / REQUEST
1.	185.177.72.16	/
2.	185.177.72.58	/admin/config.php
3.	45.61.61.31	/.env
4.	45.135.193.157	/favicon.ico
5.	45.135.193.156	/SDK/webLanguage
6.	77.83.39.167	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
7.	204.76.203.206	/.git/config
8.	204.76.203.212	/robots.txt
9.	213.209.159.175	/V2/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	160.119.76.230	/api/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 8,302 ICS attacks were recorded, a decrease of 74.6% from last week's 32,637. The top 5 attacking IPs exploiting industrial protocols 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.	194.50.16.198	guardian_ast	10001
2.	77.83.240.70	kamstrup_management_protocol	50100
3.	87.249.133.69	IEC104	2404
4.	18.218.118.203	kamstrup_protocol	1025
5.	160.119.76.4	snmp	161

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)