TZ-CERT HONEYPOT WEEKLY REPORT

Period: 22nd – 28th June 2026 | **Report No.:** TZ-CERT/WRHP/2026/26

01: WEEKLY ATTACK SUMMARY

887,731	638,387	23,864	227,236
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 18.9% vs last week	↓ 16.0% vs last week	↓ 37.5% vs last week	↑ 967.9% vs last week

A total of 887,731 network attacks were recorded across all sensors during the period 22nd – 28th June 2026, representing an overall decrease of 18.9% compared to last week's 1,094,669 attacks. While network and malware activity declined, web attacks decreased significantly by 37.5% and ICS attacks rose by 967.9%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

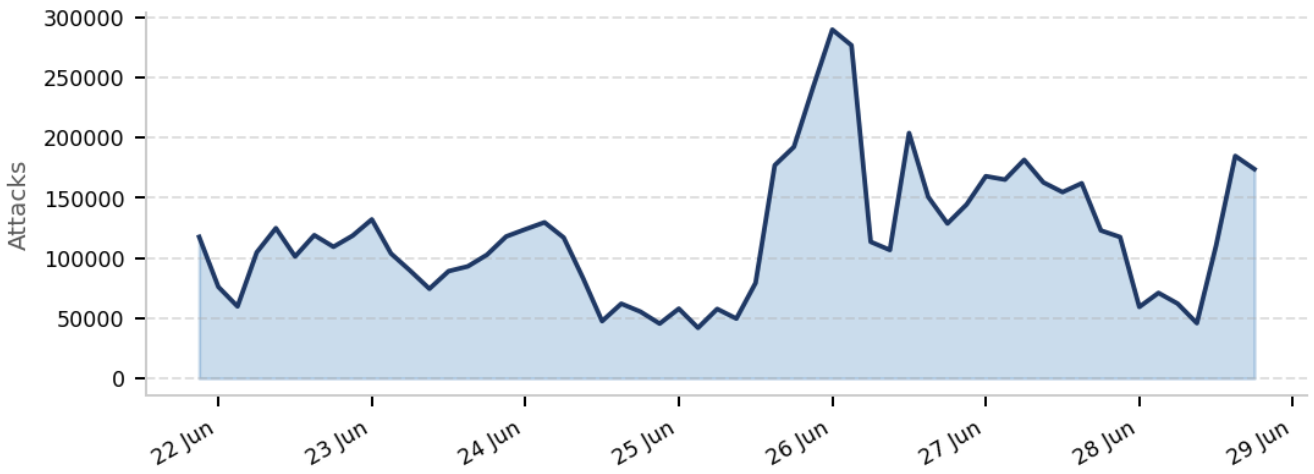

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 887,731 attacks have been recorded, down from last week's 1,094,669 by 18.9%. 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.	154.72.198.44	root	123456

2.	36.91.6.68	admin	123
3.	173.249.56.42	user	password
4.	45.153.34.112	contec	1234
5.	94.154.35.215	ubuntu	admin
6.	176.65.139.215	support	contec
7.	45.156.87.254	345gs5662d34	12345
8.	176.65.132.24	test	12345678
9.	45.142.142.140	deploy	support
10.	91.92.40.29	landscape	345gs5662d34

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 638,387 malicious software samples were distributed during the week, a decrease of 16.0% compared to last week's 760,082. 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.	41.59.203.60	trojan.shell/abtrojan	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	41.59.211.41	miner.usblfi26/abapplication	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	102.208.164.38	trojan.r002c0dkq25/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	168.197.24.152	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	111.7.106.18	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	196.219.148.244	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
7.	41.139.197.151	trojan.mirai/usblfe26	c8545034cd4fe71eeadb24dacddc5da95c4311c7112c299f1325801f3e06f928
8.	118.70.190.1	Trojan:Linux/Multiverze!rfn	f14937a19cf690d6b3f74315cb08c2af4172827e87437fd3a462dfde22e78503
9.	154.192.222.81	trojan.ddos/abtrojan	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a

10.	54.255.129.67	trojan.multiverze/malxmr	eaf9adb4bb80316a3aafceabc0f2ed2aed7c76cf134b9b7c66226fc4f003aa97

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 23,864 web attacks were recorded, a decrease of 37.5% from last week's 38,164. The top 10 attacking IPs and their targeted URIs are detailed below. Notable activity includes brute-force attempts on WordPress login pages and environment file (.env) enumeration.

SN	ATTACKING IP	TOP URI / REQUEST
1.	154.74.175.8	/
2.	103.168.67.159	/admin/config.php
3.	160.119.76.230	/SDK/webLanguage
4.	213.209.159.175	/robots.txt
5.	134.199.206.4	/favicon.ico
6.	80.94.95.211	////
7.	77.83.240.70	/.env
8.	34.148.156.95	/cgi-bin/luci/;stok=/locale
9.	34.148.193.123	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
10.	45.95.147.229	/cgi-bin/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/%%32%65%%32%65/bin/sh

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 227,236 ICS attacks were recorded, an increase of 967.9% from last week's 21,279. 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.	1.71.169.21	snmp	161
2.	220.194.187.155	guardian_ast	10001
3.	1.71.168.157	kamstrup_protocol	1025
4.	59.49.36.119	IEC104	2404
5.	1.71.169.54	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.