TZ-CERT HONEYPOT WEEKLY REPORT

Period: 13th – 19th July 2026 | **Report No.:** TZ-CERT/WRHP/2026/29

01: WEEKLY ATTACK SUMMARY

752,662	499,668	19,930	257,001
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↓ 39.3% vs last week	↓ 26.9% vs last week	↓ 91.9% vs last week	↑ 629.0% vs last week

A total of 752,662 network attacks were recorded across all sensors during the period 13th – 19th July 2026, representing an overall decrease of 39.3% compared to last week's 1,240,860 attacks. While network and malware activity declined, web attacks decreased significantly by 91.9% and ICS attacks rose by 629.0%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

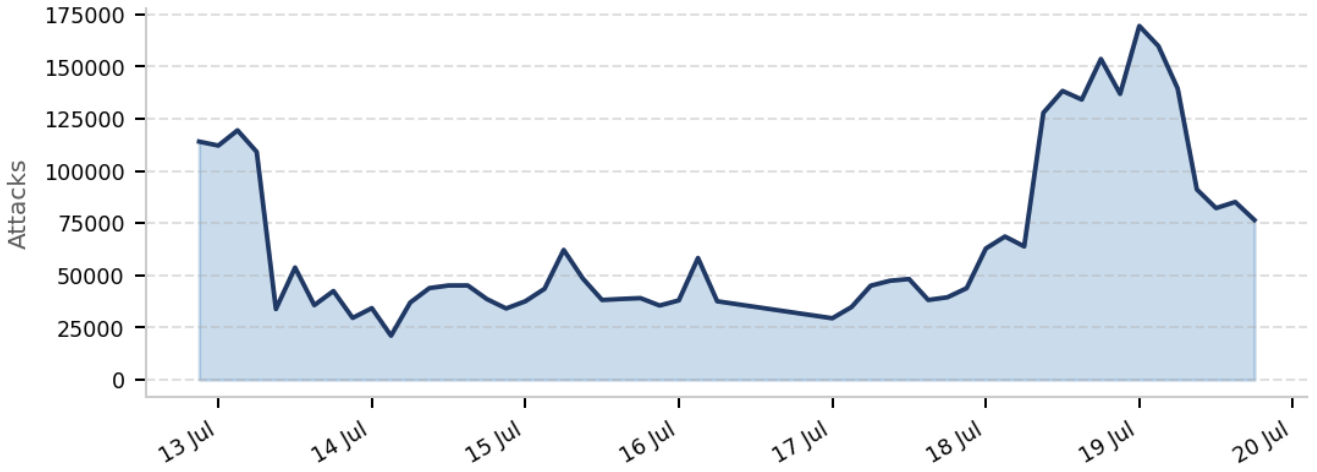

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 752,662 attacks have been recorded, down from last week's 1,240,860 by 39.3%. 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.	173.249.56.42	root	123456

2.	2.181.234.245	admin	admin
3.	157.85.97.35	support	123
4.	141.253.107.23	ubuntu	1234
5.	94.154.35.215	user	support
6.	185.246.128.133	345gs5662d34	password
7.	64.23.153.176	administrator	12345678
8.	45.156.87.254	test	root
9.	91.92.42.7	deploy	12345
10.	91.92.42.34	postgres	345gs5662d34

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 499,668 malicious software samples were distributed during the week, a decrease of 26.9% compared to last week's 683,422. 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.multiverze/shell	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	41.59.196.23	miner.usblfi26/crit	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	41.59.211.41	trojan.usblg926/mirai5	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
4.	41.59.37.21	trojan.mirai/usble726	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	102.208.164.38	trojan.usblem26/abminer	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	182.8.179.245	trojan.sagent/shell	31d4181843b1ed10a7e7cb3f108f6d6c50a7a4452ee52ddacabe8ca77260615e
7.	115.231.5.2	trojan.shell/abtrojan	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
8.	41.59.149.18	trojan.mirai/cryp	e8c0c3b714243b977d7279d191686a355c2ef73bcda1dbbca1c4f751f33c2286
9.	105.245.104.75	trojan.multiverze/abtrojan	97a1e6f817d44a4f8b07fdebaf9357786742096c470eb5d78e789b6bb53979bb

10.	41.208.153.98	miner.usblgh26/abminer	74ed8d57566e1b44f1594555727813c93f8850b5d7bd7f10a707d519b4ff95da

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 19,930 web attacks were recorded, a decrease of 91.9% from last week's 245,710. 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.	168.144.99.198	/
2.	213.209.159.175	/favicon.ico
3.	34.34.103.195	/SDK/webLanguage
4.	185.177.72.51	/robots.txt
5.	45.148.10.201	/login
6.	20.127.125.129	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
7.	172.81.129.130	/.env
8.	31.171.153.3	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
9.	20.226.66.230	/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
10.	20.220.9.199	/admin/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 257,001 ICS attacks were recorded, an increase of 629.0% from last week's 35,255. 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.	73.53.235.96	snmp	161
2.	79.9.113.8	guardian_ast	10001
3.	175.32.152.153	kamstrup_protocol	1025
4.	68.186.234.27	ipmi	623
5.	73.185.12.163	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.