TZ-CERT HONEYPOT WEEKLY REPORT

Period: 20th – 26th July 2026 | **Report No.:** TZ-CERT/WRHP/2026/30

01: WEEKLY ATTACK SUMMARY

1,753,116	868,067	54,661	1,162,900
NETWORK ATTACKS	MALWARE SAMPLES	WEB ATTACKS	ICS ATTACKS
↑ 132.9% vs last week	↑ 73.7% vs last week	↑ 174.3% vs last week	↑ 352.5% vs last week

A total of 1,753,116 network attacks were recorded across all sensors during the period 20th – 26th July 2026, representing an overall increase of 132.9% compared to last week's 752,662 attacks. While network and malware activity increased, web attacks increased significantly by 174.3% and ICS attacks rose by 352.5%, indicating a shift in adversary focus toward web-facing assets and industrial systems.

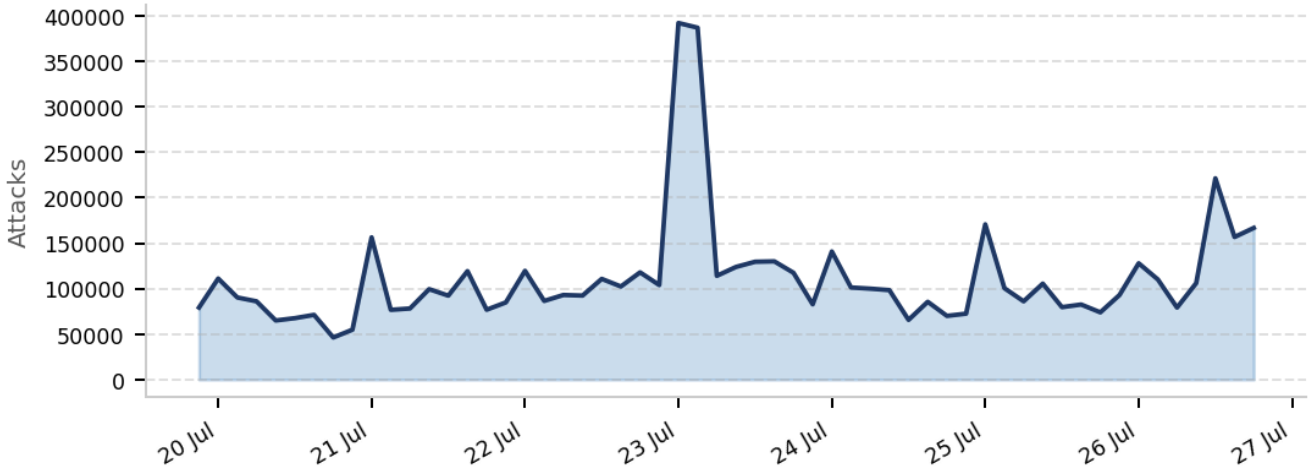

Figure 1: Daily trend of Honeypot attacks

02: NETWORK ATTACKS

A total of 1,753,116 attacks have been recorded, up from last week's 752,662 by 132.9%. 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.	200.88.91.83	root	123456

2.	104.36.229.14	admin	123
3.	94.159.116.130	ubuntu	1234
4.	202.158.50.118	user	admin
5.	173.249.56.42	support	password
6.	93.188.83.96	test	12345678
7.	91.92.42.126	deploy	12345
8.	24.144.82.155	345gs5662d34	1
9.	93.96.188.226	postgres	root
10.	91.92.47.140	git	support

Table 1: Top 10 Network Attacking IPs

03: MALICIOUS SOFTWARE (MALWARE)

A total of 868,067 malicious software samples were distributed during the week, a increase of 73.7% compared to last week's 499,668. 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.	102.214.233.160	trojan.multiverze/shell	197c74408e15bd1168105f564f96aace4fd4819961b724630bf5a6be4878daf8
2.	41.59.203.60	trojan.sagent/shell	31d4181843b1ed10a7e7cb3f108f6d6c50a7a4452ee52ddacabe8ca77260615e
3.	41.59.196.23	trojan.mirai/cryp	3eab3901798ec748895b2dca4b8762aec553d2966112999c60061d4599b599a0
4.	41.59.211.41	miner.malxmr/usblgn26	efa731b59f9e2f277336072fe5c72b488793c842e2efeedf5cb571a0eeb224e2
5.	102.208.50.58	miner.malxmr/usblgo26	3edfb02c0e6b2fe4894425cd0d4d2507f7cb11e0958674422729366a0d885c7e
6.	102.208.164.38	trojan.alien/malxmr	b3232d2cd03b051c59aef952ecfea3358c172351a27a989df31720395c3cbb4a
7.	102.33.154.14	trojan.malxmr/usblgo26	e2bc7981064d3c9ed898a0f62d659fdc2fc9646dee47a9ca92b9b28b96c27a3b
8.	5.202.60.88	trojan.alien/usblgn26	63be5f38b520b3143732962a5f8fec1f9abd1f483dbc741ed324e58f955dd35e
9.	41.203.223.149	miner.usblgj26/abminer	f3a8ffee82d63d285245f66f82f7add5a056a20f4b339e8cdd218ffd3ac6314d

10.	139.196.203.238	miner.malxmr/usblgn26	8ec920a35a7c6dd60e4aeb3b1ed09cd344f4c5191d4314a05ce72bf757377c86

Table 2: Top 10 Malware Samples with SHA256 Hashes

04: WEB ATTACKS

A total of 54,661 web attacks were recorded, an increase of 174.3% from last week's 19,930. 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.	101.47.155.116	/
2.	195.178.110.28	/script
3.	185.177.72.56	/SDK/webLanguage
4.	185.177.72.29	/favicon.ico
5.	47.253.4.207	/robots.txt
6.	94.154.43.120	/.env
7.	213.209.159.175	/login
8.	80.94.95.211	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	185.177.72.58	/.env.local
10.	185.177.72.205	/.env.old

Table 3: Top 10 Web Attacking IPs and URI Targets

05: ICS / INDUSTRIAL CONTROL SYSTEMS ATTACKS

A total of 1,162,900 ICS attacks were recorded, an increase of 352.5% from last week's 257,001. 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.	82.67.150.155	snmp	161
2.	73.183.235.5	guardian_ast	10001
3.	97.97.230.189	kamstrup_protocol	1025
4.	99.37.202.32	IEC104	2404
5.	128.78.99.52	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.