TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 10th of August to 16th of August, 2025

Report No.: TZ-CERT/WRHP/2025/32

1. NETWORK ATTACKS

A total of **409,654** attacks have been recorded compared to last week's **634,455** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	101.124.0.149	root	123456
2.	63.250.32.79	admin	admin
3.	213.133.109.79	(empty)	P@ssw0rd
4.	107.150.47.166	gitlab	qwerty123
5.	196.251.88.103	lighthouse	(empty)
6.	173.231.185.164	support	admin!@#
7.	204.76.203.83	postgres	123
8.	170.187.145.157	wang	1qaz@WSX
9.	196.251.84.225	unknown	raspberry
10.	185.93.89.4	ftp	Passw0rd

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and passwords be made to avoid use of the above listed credentials and default ones. The use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **576,816** malicious software distributed, compared to last week in which was **517,775.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	trojan.shell/bashdlod	f20683549de48f308cadf501eb8bcc5225572f5354f60310b68f199c908f31ae
2.	41.59.211.41	Trojan:Linux/Sshscan.X	05107cd7d97c5735f95cf0460ce1da2db4631abbc167c0b21842949bdca6651c
3.	41.59.203.60	CoinMiner/Linux.Agent.30304472	1d27289b1bc725c3ff2eac41a1b95036db76c3e4e40d3f227a92bf8274e6d6f9

4.	41.59.201.132	EXP/ELF.Coinminer.A	2b2197cda3a741416d8aa165b152742bd336c3692524dde93ea943ed4d9e5dd9
5.	41.59.201.7	trojan.multiverze/r002c0de925	31384110975802292bbfa8301113a4bb857cc1acb8b820e5459eab283646d79a
6.	93.118.138.181	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	177.222.43.106	Trojan:Linux/CoinMiner.C12	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
8.	36.92.98.135	Riskware.Linux.BitCoinMiner.1!c	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
9.	89.213.142.174	Malware.LINUX/AVI.Agent.jggty	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
10.	41.78.76.190	BASH/Mirai.AEH!tr.dldr	f96d1c5a55998bfab0f2c8a504bbb741f8cc093cc4e45e20d9f74adff0fbf5a2

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **35,199** web attacks compared to last week which was **25,621.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 10th of August to 16th of August, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	35.180.79.191	/
2.	64.39.98.183	/assets/
3.	139.87.112.113	/login
4.	128.199.195.217	/admin/config.php
5.	152.42.249.165	/favicon.ico
6.	178.128.53.123	/.env

7.	93.123.109.245	/sysmgmt/2015/bmc/info
8.	173.231.185.164	/.git/config
9.	185.177.72.113	/login.asp
10.	185.177.72.54	/index.html

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **5,190** ICS attacks compared to last week which was **14,860.**

From the table below these are the top 5 ICS attacks and their associated attacking IP, exploited protocols and exploited ports as detailed for the period between 10th of August to 16th of August, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	45.95.147.229	kamstrup_protocol	1025
2.	45.141.24.163	guardian_ast	10001
3.	3.130.96.91	IEC104	2404
4.	118.193.64.15	kamstrup_ management_protocol	50100
5.	45.194.70.250	snmp	161

Table4: Top 5 ICS attacking IP

5. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with the most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

5.1 Note that most of the malicious IP addresses captured are also listed as malicious IP addresses in other sources that are also observing security attacks; thus, security measures should be considered to counteract, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

5.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

5.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

5.4 Deploy Intrusion Detection System (IDS) and configure it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.