TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 17th of August to 23rd of August, 2025
Report No.: TZ-CERT/WRHP/2025/33

1. NETWORK ATTACKS

A total of **1,255,003** attacks have been recorded compared to last week's **409,654** 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.	45.14.245.67	root	123456
2.	45.144.29.201	admin	admin
3.	103.91.140.28	(empty)	root
4.	196.251.88.103	user	1234
5.	213.133.109.79	test	abc123
6.	1.34.6.225	esuser	1234
7.	190.99.72.251	oracle	(empty)
8.	173.231.185.164	ahmed	password
9.	80.94.95.112	hadoop	P@ssw0rd
10.	204.76.203.83	ftpuser	!QAZ@WSX

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 **866,432** malicious software distributed, compared to last week in which was **576,816.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan:Linux/Sshscan.X	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
2.	41.59.211.41	trojan.multiverze/r002c0dgc25	12de77bef9500e41c76a2200bc6fa712e7e3fc188dfdd92a764a22c3421b7208
3.	41.59.201.132	miner.r002c0dc725	079b5572f35d9de8cdfcdd1d0dbdc395753f1c9bcb474f18dac752842f745b07

4.	41.59.201.7	trojan.r002c0ddf25	1191c37f1446692ed0ae4eac2aee323352bc8dbc413499d4acd6cea14256b6de
5.	41.59.203.60	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	41.59.102.74	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	85.104.201.202	miner.r002c0dh925/vxoac	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
8.	94.255.36.221	Trojan:Linux/CoinMiner.C12	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
9.	41.231.84.241	Trojan:Linux/CoinMiner.C12	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
10.	116.233.255.89	BASH/Mirai.AEH!tr.dldr	f96d1c5a55998bfab0f2c8a504bbb741f8cc093cc4e45e20d9f74adff0fbf5a2

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **35,919** web attacks compared to last week which was **35,199.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 17th of August to 23rd of August, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	64.39.106.126	/
2.	64.39.106.79	/login
3.	185.177.72.46	/manager/
4.	64.39.106.28	/news/
5.	185.177.72.10	/admin/config.php
6.	64.39.106.36	/favicon.ico

7.	185.177.72.7	/favicon.ico?1528612569
8.	178.128.53.123	/.env
9.	185.177.72.52	/users/sign_in
10.	204.76.203.206	/config.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,469** ICS attacks compared to last week which was **5,190.**

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 17th of August to 23rd of August, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	3.130.96.91	kamstrup_protocol	1025
2.	3.137.73.221	guardian_ast	10001
3.	118.193.43.158	IEC104	2404
4.	165.154.135.215	snmp	161
5.	3.131.215.38	kamstrup_ management_protocol	50100

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.