TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 14th of December to 20th of December, 2025
Report No.: TZ-CERT/WRHP/2025/50

1. NETWORK ATTACKS

A total of **230,100** attacks have been recorded compared to last week's **960,614** 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.	62.60.131.18	root	123456
2.	41.78.75.186	admin	admin
3.	91.92.241.148	guest	password
4.	41.78.73.146	test	12345
5.	82.165.93.136	postgres	qwerty
6.	195.154.83.112	oracle	123456789
7.	196.251.100.242	(empty)	(empty)
8.	193.105.134.95	ideas	P@ssw0rd
9.	204.76.203.83	gerrit	1q2w3e4r
10.	185.246.128.133	apache	root

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 **321,171** malicious software distributed, compared to last week in which was **244,695.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.41.60.214	Trojan:Linux/Multiverze!rfn	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	178.22.24.242	Linux.Trojan.Miner.gen	0247e170f16fc586cbf818a7f9ef658dfc0d09279ed288de623fdea7ae06bc3d
3.	178.22.24.241	Risktool.Linux.Miner.ck	12097f9321ae6226dc089829d626fb9df46f34a8ba941988d1fd5f6c89d2d125

4.	178.22.24.244	Miner:Linux/CoinMiner.JUO	3474e95e102353c50c7bc0241a8e9ed6a17fa9eba072a24628c4cbb08b8ff64b
5.	178.22.24.248	Exploit.EXP/ELF.Coinminer.A	3850835d2e9d4a9e710787c0fa048c469cb6fe835e492e550f3356b6ed1dbc3d
6.	178.22.24.245	Trojan.Script.Multiverze.4!c	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	196.11.184.2	Artemis!Trojan	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
8.	178.80.75.49	TROJ_GEN.R002C0DKQ25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
9.	196.188.240.68	Backdoor:Linux/Hajime.A	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
10.	178.22.24.247	DDoS:Linux/Hajime.A	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **9,520** web attacks compared to last week which was **7,661.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 14th of December to 20th of December, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	13.245.230.248	/
2.	62.169.18.6	/robots.txt
3.	209.38.81.126	/favicon.ico
4.	172.190.142.176	////admin/config.php
5.	217.154.200.211	/.env
6.	77.83.240.70	/admin/config.php

7.	52.169.206.229	/SDK/webLanguage
8.	62.60.135.189	/sitemap.xml
9.	95.214.55.71	/.well-known/security.txt
10.	60.255.143.219	/cgi-bin/luci/;stok=/locale

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,001** ICS attacks compared to last week which was **3,527.**

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 14th of December to 20th of December, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	kamstrup_management_protocol	50100
2.	13.245.230.248	IEC104	2404
3.	167.71.19.131	guardian_ast	10001
4.	173.255.253.44	kamstrup_protocol	1025
5.	45.56.69.79	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.