TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 21st of December to 27th of December, 2025
Report No.: TZ-CERT/WRHP/2025/51

1. NETWORK ATTACKS

A total of **517,365** attacks have been recorded compared to last week's **230,100** 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.	91.92.241.148	sa	123456
2.	176.65.132.95	root	admin
3.	185.11.61.226	anonymous	(empty)
4.	94.26.106.81	MSSQL	anonymous@
5.	204.76.203.83	sqladmin	p@55w0rd
6.	193.105.134.95	(empty)	!QAZ2wsx
7.	167.172.33.249	admin	Admin@123
8.	41.78.73.146	administrator	P@ssw0rd!!
9.	165.232.91.114	ec2-user	123qwe!@#
10.	185.11.61.151	postgres	12345678

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 **359,900** malicious software distributed, compared to last week in which was **321,171.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Tool.Linux.BtcMine.9999	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
2.	41.59.203.60	Trojan/Linux.CoinMiner.ao	433dd4cb63851f2b06eef7b7cc9c08b5fbcac933fc9abbad9126a545683e011f
3.	2.39.162.247	Trojan.Elf64.Miner.kuglfi	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

4.	189.204.221.234	Risktool.Linux.Miner.ck	09805e2bf3d471395caa6406a11f45f211f4faec19187713550bc816b50698a7
5.	196.41.60.214	HEUR:Trojan.Linux.Miner.gen	0bbee3979b0327b6c327c4522414a90d18164af3846ea6a8e62e5fee861f6d51
6.	41.13.24.55	HackTool/Linux.BitCoinMiner.a	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
7.	200.75.2.138	Trojan:Linux/CoinMiner.C12	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
8.	196.210.110.68	TrojanDownloader:SH/SAgent.B!MTB	55478ba26121a160ac9fa3680c430c1ae64a4f46a3c5d2e24cae99a44a2aecb4
9.	123.27.3.39	Trojan.UKP.Mirai.4!c	17d81812e7b630388fb61ca8f25ca799cbdf19f70f9e77dc734da837ecc80780
10.	41.59.211.41	Trojan[downloader]:Win/Agent.a	665655d45ccb6398fca5c9f077b3533cd3e80dc786fdbf6736e2a751e35af067

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **9,453** web attacks compared to last week which was **9,520.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 21st of December to 27th of December, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	195.178.110.192	/
2.	213.209.159.150	/robots.txt
3.	204.76.203.219	/favicon.ico
4.	77.83.240.70	/.env
5.	95.214.55.71	/sitemap.xml
6.	172.190.142.176	/.well-known/security.txt

7.	185.243.5.43	/cgi-bin/luci/;stok=/locale
8.	204.76.203.212	/SDK/webLanguage
9.	136.144.33.251	/admin/config.php
10.	139.59.111.105	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,597** ICS attacks compared to last week which was **4,001.**

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 21st of December to 27th of December, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	45.95.147.229	kamstrup_management_protocol	50100
3.	3.137.73.221	IEC104	2404
4.	68.183.138.85	kamstrup_protocol	1025
5.	45.82.78.102	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.