TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 07th of December to 13th of December, 2025
Report No.: TZ-CERT/WRHP/2025/49

1. NETWORK ATTACKS

A total of **960,614** attacks have been recorded compared to last week's **1,864,651** 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.	141.98.19.109	ubuntu	admin
2.	45.159.112.23	user	123456
3.	185.116.161.213	root	password
4.	45.159.112.142	admin	12345
5.	103.231.179.29	oracle	12345678
6.	108.175.5.70	controll	123qwerty
7.	189.113.8.254	redis	admin123
8.	113.161.241.128	debian	111111
9.	45.226.114.110	dell	P@ssw0rd
10.	185.169.6.22	git	(empty)

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 **244,695** malicious software distributed, compared to last week in which was **233,120.**

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	05d563ca4dd86807cd5e20f4678d30ee71644137ffac807f2f5a6917fa9b78ec
2.	152.237.41.64	EXP/ELF.Coinminer.A	08b3fb745ab6db03be3460b2365ce6b4cf6975f123a114a8c9cc72fdc7e74c7b
3.	102.33.155.126	Trojan:Linux/Multiverze!rfn	41bef8b5f87c62963cdbbd6b6c5c809375d2f5338138bbcc6220ed8e253f2eee

4.	14.153.159.167	HEUR:Trojan.Linux.Miner.gen	5e23111f49b974aa5c3758309a2825bd09201be9277c6af72d6635066d8785c7
5.	41.78.227.2	Risktool.Linux.Miner.ck	84b423706bd14647300e5a5442f5451f91ced636a05f191b81fabdb1e0131642
6.	110.153.13.6	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	196.191.131.64	HackTool/Linux.BitCoinMiner.a	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
8.	116.230.249.216	Riskware.Linux.BitCoinMiner.1!c	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
9.	112.42.68.9	Miner:Multi/XmrigGo.SY	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
10.	196.41.60.214	Backdoor.Win32.Berbew	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **7,661** web attacks compared to last week which was **7,378.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 07th of December to 13th of December, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	45.148.10.247	/
2.	52.141.41.16	/robots.txt
3.	4.197.221.212	/cgi-bin/luci/;stok=/locale
4.	45.95.147.229	/help/ci/yaml/README.md
5.	196.249.113.120	/favicon.ico
6.	52.169.206.229	/help/topics/autodevops/index.md

7.	20.89.214.18	/.env
8.	4.189.145.111	/sitemap.xml
9.	172.200.135.102	/help/user/project/clusters/index.md
10.	193.142.147.209	/.well-known/security.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,527** ICS attacks compared to last week which was **3,315.**

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 07th of December to 13th of December, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	45.95.147.229	IEC104	2404
2.	159.65.69.56	guardian_ast	10001
3.	165.22.133.237	kamstrup_management_protocol	50100
4.	3.134.148.59	kamstrup_protocol	1025
5.	104.218.165.188	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.