TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 30th of November to 06th of December, 2025
Report No.: TZ-CERT/WRHP/2025/48

1. NETWORK ATTACKS

A total of **1,864,651** attacks have been recorded compared to last week's **554,351** 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.	185.116.161.213	root	123456
2.	45.159.112.23	admin	(empty)
3.	84.36.108.43	ubuntu	123
4.	141.98.19.109	linuxadmin	P@ssw0rd
5.	185.169.6.22	odoo	admin
6.	103.231.179.29	Huawei	1234
7.	192.145.169.91	master	password
8.	114.121.248.251	solana	Admin@123
9.	189.113.8.254	user	qwerty
10.	157.230.40.249	apache	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 **233,120** malicious software distributed, compared to last week in which was **237,363.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.41.60.214	Trojan.Script.Multiverze.4!c	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.111.198.209	Trojan:Linux/CoinMiner.C12	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	182.93.35.250	TROJ_GEN.R002C0DKQ25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

4.	41.111.190.185	Generik.MQRITUJ Trojan	048e374baac36d8cf68d d32e48313ef8eb517d64 7548b1bf5f26d2d0e2e3 cdc7
5.	196.191.131.64	HackTool/Linux.BitCoinMi ner.a	59c29436755b0778e96 8d49feeae20ed65f5fa5e 35f9f7965b8ed93420db 91e5
6.	41.224.4.204	Shell.trojan.generic	278397c326d2cd30140 b645a5186834a2b3841 13ef64bbc1a247e9c3e6 bde1ec
7.	114.38.108.44	DDoS:Linux/Hajime.A	a04ac6d98ad98931278 3d4fe3456c53730b212c 79a426fb215708b6c6da a3de3
8.	14.241.119.115	Backdoor.Linux.bbxo	020f1fa6072108c79ed6f 553f4f8b08e157bf17f9c 260a76353300230fed09 f0
9.	196.202.91.164	Backdoor.Linux.Hajime.V8 2n	d5601202dff3017db238 145ff21857415f663031a ca9b3d534bec8991b12 179a
10.	196.41.60.214	HackTool/Linux.BitCoinMi ner.a	dbb7ebb960dc0d5a480f 97ddde3a227a2d83fcac a7d37ae672e6a0a6785 631e9

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **7,378** web attacks compared to last week which was **9,072.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 30th of November to 06th of December, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	104.219.238.86	/
2.	45.148.10.250	/robots.txt
3.	149.50.97.177	/cgi-bin/luci/;stok=/locale
4.	4.218.20.75	/.env
5.	4.189.128.136	/favicon.ico
6.	159.203.106.159	/196.41.76.20/.env

7.	193.142.147.209	/.well-known/security.txt
8.	45.8.19.120	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	124.198.131.159	/sitemap.xml
10.	37.26.65.243	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,315** ICS attacks compared to last week which was **2,739.**

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 30th of November to 06th of December, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	IEC104	2404
2.	45.95.147.229	guardian_ast	10001
3.	137.184.75.250	kamstrup_management_protocol	50100
4.	139.177.206.224	kamstrup_protocol	1025
5.	3.134.148.59	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.