TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 23rd of November to 29th of November, 2025
Report No.: TZ-CERT/WRHP/2025/47

1. NETWORK ATTACKS

A total of **554,351** attacks have been recorded compared to last week's **558,015** 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	root	123456
2.	201.184.115.172	admin	password
3.	103.175.180.208	sol	admin
4.	195.154.83.112	oracle	passw0rd
5.	41.78.73.146	Test	P@ssw0rd
6.	41.78.75.186	server	Wind1doW$
7.	107.175.145.51	dspace	aquario
8.	204.76.203.83	nginx	1q2w3e4r
9.	185.246.130.20	backup	zyad1234
10.	185.246.128.133	odoo	1234qwer

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 **237,363** malicious software distributed, compared to last week in which was **295,033.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	176.52.139.71	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	216.201.224.2	Riskware.Linux.BitCoinMiner.1!c	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	14.20.138.186	Trojan:Linux/CoinMiner.C12	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

4.	196.41.253.22	Miner:Multi/XmrigGo.SY	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	196.188.243.243	Trojan.Linux.MALXMR.USBLKH25	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.111.167.49	TrojanDownloader/Linux.Agent.cn	6298d2abcfb8b5f7b010e28168ab97fd4087fbd82c39ace195c0aa813921b256
7.	196.218.200.26	HEUR:Trojan.Linux.Agent.gen	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
8.	117.141.201.194	Backdoor.Linux.HAJIME.AF	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
9.	196.41.60.214	Trojan:Linux/Downldr.B!MTB	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
10.	176.52.139.71	HEUR:Backdoor.Linux.Hajime.b	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **9,072** web attacks compared to last week which was **8,496.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 23rd of November to 29th of November, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	37.26.65.243	/
2.	149.50.97.228	/robots.txt
3.	3.84.203.101	/cgi-bin/luci/;stok=/locale
4.	4.189.145.250	/favicon.ico
5.	4.206.90.251	/.env
6.	193.142.147.209	/sitemap.xml

7.	139.162.173.209	/.well-known/security.txt
8.	141.98.10.130	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	48.210.12.181	/manager/html
10.	172.207.189.235	/ISAPI/Security/sessionLogin

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,739** ICS attacks compared to last week which was **2,786.**

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 23rd of November to 29th of November, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	45.95.147.229	guardian_ast	10001
2.	77.83.240.70	kamstrup_protocol	1025
3.	104.248.74.203	IEC104	2404
4.	173.255.204.220	kamstrup_management_protocol	50100
5.	206.189.163.249	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.