TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 02nd of November to 08th of November, 2025
Report No.: TZ-CERT/WRHP/2025/44

1. NETWORK ATTACKS

A total of **607,328** attacks have been recorded compared to last week's **449,772** 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.	203.153.103.122	root	123456
2.	118.193.33.112	admin	345gs5662d34
3.	196.251.84.225	huawei	Pi123321
4.	167.250.224.25	alex	nPSpP4PBW0
5.	91.92.241.148	(empty)	postgres1234
6.	77.90.185.47	stories	Aa112233
7.	81.19.182.168	ubnt	654321
8.	41.78.73.146	test	128tRoutes
9.	210.16.184.165	teste	admin
10.	204.76.203.83	postgres	password

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 **428,522** malicious software distributed, compared to last week in which was **289,453.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.211.41	Tool.Linux.BtcMine.9999	07f79f61869a42c058c7ce0225bbe6bc7cb56ee862dca2b87f4e384150fd69da
3.	196.41.60.214	HEUR:Trojan.Linux.Agent.gen	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	41.59.201.132	Riskware.Linux.BitCoinMiner.1!c	0c7ce0368ae6fa3a1445b52c6d0e9f4a773cf0079601d0b5ece266837473c157
5.	190.64.76.90	PotentialRisk.PUA/AVI.CoinMiner.xmawi	ba1bb8a7ef31a255a52665d459bce74c9e57aec46767f93df1217f20db38fda8
6.	81.10.31.23	Trojan:Linux/CoinMiner.C12	6149d087c5267a473b7a649eef4c54cdbcd95e662e016c78f7758c3ed23a27b5
7.	193.134.208.226	BASH/Dloader.P!tr	1ebf139fe8271dd0c5ee67ae22e4d4269115508c089fb2f31143c3778ae3b193
8.	41.59.114.186	DDoS:Linux/Hajime.A	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
9.	41.59.102.74	Trojan.Elf32.Hajime.fbjkxb	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
10.	41.59.203.60	CoinMiner.Linux.Agent.Veng	ba1bb8a7ef31a255a52665d459bce74c9e57aec46767f93df1217f20db38fda8

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **23,760** web attacks compared to last week which was **47,379.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 02nd of November to 08th of November, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.112.48	/
2.	139.87.112.135	/login
3.	139.87.112.96	/robots.txt
4.	139.87.112.140	/cgi-bin/luci/;stok=/locale
5.	139.87.112.146	/.env
6.	139.87.112.40	/favicon.ico

7.	204.76.203.30	/admin/config.php
8.	77.83.240.70	/accounting/control/main
9.	204.76.203.219	/index.html
10.	13.79.87.25	/mgmt/tm/util/bash

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,334** ICS attacks compared to last week which was **2,133.**

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 02nd of November to 08th of November, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	3.131.215.38	IEC104	2404
3.	139.87.112.48	kamstrup_management_protocol	50100
4.	3.130.96.91	kamstrup_protocol	1025
5.	34.68.34.85	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.