TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 06th of April to 12th of April, 2025
Report No.: TZ-CERT/WRHP/2025/15

1. NETWORK ATTACKS

A total of **54,207** attacks have been recorded compared to last week's **95,070** 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.	62.149.25.72	root	root
2.	149.56.31.77	admin	admin
3.	87.98.138.86	(empty)	123456
4.	80.73.95.46	Administrator	(empty)
5.	45.144.29.201	guest	1234
6.	185.246.128.133	supervisor	password
7.	193.105.134.95	admin1	12345
8.	41.78.74.39	support	supervisor
9.	209.38.28.212	default	1234567890
10.	41.78.73.146	anonymous	1234admin

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 **50,528** malicious software distributed, compared to last week in which was **38,404.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Mal/Generic-S	51b052a524af278366fb5527d4a5eee949b63f85168c37d4f97aefe3e73fe66a
2.	86.122.186.47	HEUR:Trojan.Linux.Miner.gen	8a5a71d459fa12a3a04be9cf1acb488dd1afe8948f422f97658cc8952bf57fc2
3.	41.13.92.248	Linux/CoinMiner.ABF	7b8116a244dc9b35dc7286c030149eec4c58ba77d9ded8c11ba93bc87ef3928f

4.	85.152.107.190	Risktool.Linux.Miner.ck	9c3060c05a562582122094ea02e6fafff303839ab2fa08f1333919e160d5ed0b
5.	185.146.166.239	Static AI - Malicious ELF	9f6fa0544c67bd2d3c59f031c2d9ba107312772aaa7852ddb6cb6d9e94bbeb2a
6.	41.108.86.6	Shell.trojan.multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	41.155.51.68	Adware/Miner	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf
8.	156.213.104.93	Generic Reputation PUA (PUA)	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a
9.	203.146.249.79	HackTool/Linux.BitCoinMiner.a	7780e72f7dea978946d4615c8db1b239d3e2c742cfc8be2934006b1fd6071110
10.	58.181.99.75	Generic.Bash.MiraiA.7D844DFB	aff538d6b5b0c58f881f11de50f67baed41ccbdca3d4ba73b94c9300f343d900

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,064** web attacks compared to last week which was **2,351.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 06th of April to 12th of April, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	154.83.103.108	/
2.	154.81.156.54	/users/sign_in
3.	143.198.138.171	/admin/config.php
4.	173.231.185.164	/.env
5.	154.81.156.35	/41.78.64.60/.env
6.	154.81.156.34	/robots.txt

7.	162.19.211.112	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	78.153.140.30	/.git/config
9.	195.178.110.163	/boaform/admin/formLogin
10.	195.178.110.159	/admin/assets/js/views/login.js

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **771** ICS attacks compared to last week which was **2,129.**

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 06th of April to 12th of April, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	207.90.244.2	IEC104	2404
2.	207.90.244.5	Kamstrup_management_protocol	50100
3.	152.32.180.86	kamstrup_protocol	1025
4.	207.90.244.10	guardian_ast	10001
5.	118.26.36.9	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.