TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 09th of March to 15th of March, 2025
Report No.: TZ-CERT/WRHP/2025/11

1. NETWORK ATTACKS

A total of **310,358** attacks have been recorded compared to last week's **322,489** 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.	103.56.30.34	root	admin
2.	189.44.214.26	admin	(empty)
3.	62.149.25.72	Administrator	1234567890
4.	185.233.247.245	telnetadmin	p@55w0rd
5.	45.249.8.86	postgres	abc123456
6.	45.226.53.7	superadmin	123qwe!@#
7.	62.171.130.190	guest	anonymous
8.	177.11.49.133	supportadmin	helpme
9.	87.98.138.86	ubuntu	root
10.	141.94.188.7	telecomadmin	telnetadmin

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 **57,844** malicious software distributed, compared to last week in which was **108,878.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	14.99.147.98	trojan.xorddos/ddos	73ce06c5eccf5a9035fa0d795d14e3ee488932176f14049f0d03768518d6647d
3.	196.202.22.211	HackTool/Linux.BitCoinMiner.a	15df367d98a807d1c41b677e17b4e73b7f99657c3966542180e0535bc138d43c

4.	188.187.108.76	DDoS:Linux/XorDDoS	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
5.	59.88.167.182	trojan.adzox/r002c0xc125	5f85bbb2f68df12de19dad2367ce920cc99fcb583aa963c7791633f4c86bd88a
6.	190.104.47.238	trojan.mluxb/r002c0xc125	6148113073dd1e9138660134605768d9ae635c9399d4f296f5d75b347fc0872f
7.	41.32.42.227	Backdoor:Linux/Hajime.A	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
8.	45.240.34.74	downloader.shell/bash	4e0b27339e784ecfec59332890bec0c7cd664b60416f61c9fef79d936e12d173
9.	80.191.171.230	trojan.hajime/mirai	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
10.	36.64.210.218	Backdoor.Win32.Berbew.CNYY	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **100,894** web attacks compared to last week which was **3,575.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 09th of March to 15th of March, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	193.41.206.202	/prod/.env
2.	193.41.206.176	/public/.env
3.	193.41.206.246	/config/application.yml
4.	193.41.206.12	/
5.	45.148.10.35	/private/.env
6.	144.126.146.166	/prisma/.env

7.	45.196.222.235	/psnlink/.env
8.	78.153.140.37	/processor/.env
9.	45.148.10.235	/project_root/.env
10.	179.43.175.246	/pt2/countries/src/.env

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,223** ICS attacks compared to last week which was **2,186.**

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 09th of March to 15th of March, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	152.32.206.74	kamstrup_protocol	1025
2.	152.32.130.247	IEC104	2404
3.	35.180.203.18	kamstrup_management_protocol	50100
4.	118.26.36.206	snmp	161
5.	118.26.36.195	guardian_ast	10001

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.