TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 30th of March to 05th of April, 2025
Report No.: TZ-CERT/WRHP/2025/14

1. NETWORK ATTACKS

A total of **95,070** attacks have been recorded compared to last week's **167,181** 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.	87.98.138.86	sa	(empty)
2.	203.190.10.113	root	anonymous@
3.	45.249.8.86	bob	Ab123321
4.	218.92.0.244	anonymous	123456
5.	185.233.247.245	(empty)	vcsnfaM$1
6.	80.73.95.46	appdbuserprod	Smart@123
7.	193.105.134.95	vishal_uat	p@$$w0rd
8.	185.246.128.133	tableau_sa	Mdt3727248!*-
9.	45.144.29.201	datakod	12345678
10.	41.78.74.39	Elias Caetano	3t9z12Bt5015

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 **38,404** malicious software distributed, compared to last week in which was **110,470.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Generic.Bash.MiraiA.F9F0BC8A	7cc0addbe77dcd94ee4636584b53ef329c485313ff2566b7a0bfa7683c64543b
2.	86.122.186.47	EXP/ELF.Coinminer.A	5e21f3eb4a63f6a468835123bcc91daa6847bd838baf6bcf42a86080edcea9d4
3.	195.182.136.122	Adware/Miner	89eda5fcd3f3862c2f320b645a34a2125dfec3ac7aca126ce8b990b3d5ddea1c

4.	58.181.99.73	HEUR:Trojan.Linux.Miner.gen	9042a88cff4d55a15b8f7faf216baa176e2e4d14141902589d8ce2cab7cd8767
5.	58.181.99.75	Trojan:Linux/Multiverze	9781af4ccf02f5098e9c4c41f8afebedca6a46fb68e9f6b100e43c66087cbc69
6.	61.222.153.80	Script.Troj.multiverze.v	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	66.17.113.57	miner.gikam/r002c0dcq25	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf
8.	122.4.103.18	Tool.Linux.BtcMine.9999	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a
9.	41.38.128.64	Miner:Multi/XmrigGo.SY	7780e72f7dea978946d4615c8db1b239d3e2c742cfc8be2934006b1fd6071110
10.	125.209.111.150	Backdoor.Linux.ayjk	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,351** web attacks compared to last week which was **3,475.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 30th of March to 05th of April, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.185.164	/
2.	45.148.10.235	/admin/config.php
3.	154.83.103.15	/users/sign_in
4.	195.178.110.159	/.env
5.	45.148.10.90	/admin/config.php?password%5B0%5D=ZIZO&username=admin

6.	154.81.156.35	/favicon.ico
7.	154.83.103.13	/robots.txt
8.	154.83.103.14	/login.rsp
9.	154.83.103.17	/admin/modules/framework/amp_conf/htdocs/admin/config.php
10.	78.153.140.30	/logon.htm

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,129** ICS attacks compared to last week which was **4,568.**

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 March to 05th of April, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	23.239.12.21	snmp	161
2.	45.56.110.153	Kamstrup_protocol	1025
3.	8.219.223.155	kamstrup_management_protocol	50100
4.	8.222.133.173	IEC104	2404
5.	47.236.23.25	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.