TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 23rd of March to 29th of March, 2025
Report No.: TZ-CERT/WRHP/2025/13

1. NETWORK ATTACKS

A total of **167,181** attacks have been recorded compared to last week's **305,018** 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.	203.190.10.113	root	123456
2.	45.249.8.86	admin	admin
3.	45.224.131.227	ubuntu	password
4.	62.171.130.190	user	guest
5.	87.98.138.86	guest	pass
6.	80.73.95.46	user1	12345
7.	218.92.0.244	user2	root
8.	193.105.134.95	supervisor	juantech
9.	185.246.128.133	Administrator	(empty)
10.	183.218.88.24	support	3245gs5662d34

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 **110,470** malicious software distributed, compared to last week in which was **88,435.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan.GenericKD.74003008	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	203.146.249.79	miner.gikam/r002c0dcq25	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf
3.	80.21.50.56	RiskWare[RiskTool]/Linux.BitCoinMiner	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a

4.	125.228.157.189	Trojan.Linux.GenericKD.43816	7780e72f7dea978946d4615c8db1b239d3e2c742cfc8be2934006b1fd6071110
5.	113.110.146.62	Miner:Multi/XmrigGo.SY	b6ee8e08f1d4992ca85770e6883c1d2206ebbaf42f99d99aba0e26278de8bffb
6.	46.201.149.28	Tool.Linux.BtcMine.9999	70cb20d3a168b27d6147727024086a015cb243788ceb46644daddb7945987027
7.	116.227.124.181	Generic.Bash.MiraiA.4CB61706	42fa2db62f271b57cdfd7e1957693de96d711eff3c0fdd089c9482091bbedaef
8.	196.249.246.66	Generic.Linux.Medusa.C.F161EC4E	7b707f877544b367864e3dbb19e79c811b4464ba2f86c72b728b118874294c74
9.	41.38.8.44	Linux/TrojanDownloader.SH.DNG	7cc0addbe77dcd94ee4636584b53ef329c485313ff2566b7a0bfa7683c64543b
10.	190.106.101.24	Trojan:SH/Geninst.JA	151824c3382e4b9b920c8de4a85fc705a904a99570aec4c182d66527e96eba1b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,475** web attacks compared to last week which was **100,894.**

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

SN	ATTACKING IPS	TOP URI
1.	170.39.218.189	/
2.	154.83.103.18	/admin/config.php
3.	173.231.185.164	/users/sign_in
4.	45.148.10.235	/.env
5.	195.178.110.163	/admin/assets/js/views/login.js
6.	170.39.218.176	/logon.htm

7.	195.178.110.159	/favicon.ico
8.	43.153.77.94	/login.rsp
9.	78.153.140.30	/admin/config.php?password%5B0%5D=ZIZO&username=admin
10.	137.184.2.69	/admin/modules/framework/amp_conf/htdocs/admin/config.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,568** ICS attacks compared to last week which was **2,370.**

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 March to 29th of March, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	8.219.185.110	snmp	161
2.	8.222.181.184	IEC104	2404
3.	8.219.251.143	kamstrup_protocol	1025
4.	47.236.28.83	guardian_ast	10001
5.	165.154.118.26	kamstrup_management_protocol	50100

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.