TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 16th of March to 22nd of March, 2025
Report No.: TZ-CERT/WRHP/2025/12

1. NETWORK ATTACKS

A total of **305,018** attacks have been recorded compared to last week's **310,358** 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.	219.138.76.105	root	123456
2.	185.233.247.245	support	(empty)
3.	45.249.8.86	admin	admin
4.	203.190.10.113	guest	password
5.	62.171.130.190	user	abc123456
6.	45.222.101.85	ubnt	root
7.	218.92.0.178	default	anonymous
8.	45.224.131.227	vadmin	helpme
9.	87.98.138.86	supervisor	root
10.	200.124.160.2	hadoop	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 **88,435** malicious software distributed, compared to last week in which was **57,844.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	219.138.76.105	trojan.multiverze/vsnw01j24	71e446c7cb1e7eb7bd7c11a08ec7f37d7b65db00eb0e0c525775d9f2c2d8dc2f
2.	185.233.247.245	trojan.r002c0db725	0bc58e58275d6ecca05335aac681a0352173e19d8718230c1902c2bf99d8782f
3.	45.249.8.86	trojan.r002c0dli24	149a188531fb921122e1c5fd7efed1e3981d45572a0fe14dce7afc6e2c0f12b2

4.	203.190.10.113	trojan.r002c0dbc25	1bd3745a4f9043ead807d7777669b0dbf5b56985e5b3dd9d7cff8384154ea4a8
5.	62.171.130.190	Trojan:Linux/Multiverze	27d205dc183ea2fad0e55e10b206404be20908e39a74569ff99182d7326ed9c0
6.	45.222.101.85	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	218.92.0.178	miner.gikam	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf
8.	45.224.131.227	Trojan:Linux/CoinMiner!rfn	15df367d98a807d1c41b677e17b4e73b7f99657c3966542180e0535bc138d43c
9.	87.98.138.86	miner.pvcyv/r002c0dcl25	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a
10.	200.124.160.2	trojan.adzox/r002c0xc125	5f85bbb2f68df12de19dad2367ce920cc99fcb583aa963c7791633f4c86bd88a

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 16th of March to 22nd of March, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	193.41.206.98	/
2.	170.39.218.98	/.git/HEAD
3.	193.41.206.176	/?url=/var/www/html/config.php
4.	193.41.206.138	/.env
5.	193.41.206.189	/?uri=/var/www/html/config.php
6.	170.39.218.202	/?file=/var/www/html/config.php

7.	41.78.65.2	/.env.production
8.	134.209.221.228	/api/.env
9.	124.128.219.196	/db.ini
10.	173.231.185.164	/config/.env

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,370** ICS attacks compared to last week which was **4,223.**

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 16th of March to 22nd of March, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.120.13	kamstrup_protocol	1025
2.	147.182.247.10	IEC104	2404
3.	199.45.154.158	kamstrup_management_protocol	50100
4.	101.36.120.74	snmp	161
5.	118.26.36.171	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.