TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 02nd of March to 08th of March, 2025
Report No.: TZ-CERT/WRHP/2025/10

1. NETWORK ATTACKS

A total of **322,489** attacks have been recorded compared to last week's **319,605** 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	123456
2.	177.11.49.133	admin	admin
3.	218.92.0.179	superadmin	password
4.	27.133.152.57	test	3245gs5662d34
5.	45.249.8.86	cs2server	345gs5662d34
6.	5.161.181.1	ftp	12345
7.	185.233.247.245	telecomadmin	(empty)
8.	62.171.130.190	dev	root
9.	41.73.132.4	postgres	1234
10.	103.105.177.58	guest	pass

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 **108,878** malicious software distributed, compared to last week in which was **69,315.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	196.202.34.60	Trojan-Downloader.Linux.Sh	4e0b27339e784ecfec59332890bec0c7cd664b60416f61c9fef79d936e12d173
3.	68.228.123.83	BASH/Dloader.AAN!tr.dldr	10874d6a1da9b33cc80c5082f8e4c5d870518884c602dafb87815f091353cc47

4.	58.56.44.118	Trojan:Win32/Vigorf.A	47eda32af60fe513d6edabf8ab322e18d45619663040a1c294a93b91d6386601
5.	171.224.219.80	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	118.163.39.49	HEUR:TrojanDownloader/BAT.Agent.dc	229022b01619739c182d59433ae8ebe87d299175a938e344f569dfc060cab870
7.	41.38.220.96	Trojan:Linux/Sshscan.X	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
8.	196.189.198.60	Trojan/Linux.CoinMiner.ah	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
9.	80.78.71.190	TrojanDownloader:Linux/Dwnlodr.PC!MTB	3749a82f427fb0542ce6b3a24146e5eb3c14831bb18b1826fce8281a7871b0e7
10.	193.227.47.118	Trojan.GenericKDZ.109484	0fd1c384f4f0aaffadd55c41df59a8a559d5faf6ba5eb579cf15d4061f747b9e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,575** web attacks compared to last week which was **2,771.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 02nd of March to 08th of March, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	188.166.254.66	/
2.	193.41.206.72	/users/sign_in
3.	162.217.96.20	/admin/config.php
4.	45.148.10.35	/cgi-bin/luci/;stok=/locale
5.	193.68.89.10	/.env
6.	204.76.203.15	/favicon.ico

7.	217.76.50.24	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	45.148.10.34	/robots.txt
9.	78.153.140.30	/login.rsp
10.	121.159.71.249	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,186** ICS attacks compared to last week which was **3,012.**

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 02nd of March to 08th of March, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.41.6	IEC104	2404
2.	87.98.236.89	kamstrup_protocol	1025
3.	45.33.22.67	kamstrup_management_protocol	50100
4.	45.79.68.194	guardian_ast	10001
5.	103.149.26.131	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.