TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 3rd March 2024 to 9th of March, 2024
Report No.: TZ-CERT/WRHP/2024/10

1. NETWORK ATTACKS

A total of **86,154** attacks have been recorded compared to last week's **87,681** 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.	185.246.128.133	root	admin
2.	193.105.134.95	user	password
3.	41.78.73.146	admin	support
4.	41.78.38.139	supervisor	123456
5.	41.78.75.186	ubuntu	(empty)
6.	2.57.122.244	support	123admin
7.	213.109.202.127	postgres	1234567890
8.	156.146.57.68	Admin	<No Pass>
9.	139.59.235.116	deployer	default
10.	43.134.79.95	config	User

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 **33,226** malicious software distributed, compared to last week in which was **49,519.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.250	TrojanDownloader:Linux/Morila!MTB	acb409c544941061154005b4582cb4d1610ed0c0cf7f57fe02c305a275e1053f
2.	85.95.188.80	Backdoor:Win32/Berbew	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
3.	81.251.100.203	Trojan:Linux/Downldr.B!MTB	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

4.	171.252.154.62	Trojan:Linux/Downldr.B!MTB	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	103.184.236.178	Backdoor:Win32/Berbew	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
6.	176.120.32.251	DoS:Linux/Xorddos!pz	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	13.38.26.129	Trojan:Linux/Multiverze	8a20aea398f7452fdb51e94661baa3a402da3201c5d5edf191711c7c5e27b382
8.	103.230.107.236	Trojan:Linux/Multiverze	409e6be60a200711954b03a747748ea87de1756b2ad9e81fa6454598bdefb065
9.	202.179.76.68	Trojan:Linux/Multiverze	7901ea3019dcd61d8913ba4f2cb37a5de33123b4b58482c7a96d96660c45a5a1

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **7,533** web attacks compared to last week which was **1,553.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 3rd March 2024 to 9th of March, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	13.38.26.129	/
2.	146.19.24.28	/users/sign_in
3.	66.154.113.9	/favicon.ico
4.	78.129.165.238	/admin/config.php and /.git/config
5.	41.78.75.186	/.env
6.	41.78.73.146	/favicon.ico
7.	41.78.38.139	/etc/passwd
8.	63.251.106.21	/robots.txt

9.	8.213.27.99	/info.php
10.	78.153.140.37	/1.php

Table3: Top 10 web attacking IP

4. 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: -

4.1 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.

4.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

4.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

4.4 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.