TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 31st March 2024 to 6th of April, 2024
Report No.: TZ-CERT/WRHP/2024/14

1. NETWORK ATTACKS

A total of **227,087** attacks have been recorded compared to last week's **707,274** 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.	193.105.134.95	root	admin
2.	218.92.0.93	user	P@ssw0rd
3.	146.190.173.46	debian	support
4.	41.78.73.146	sa	888888
5.	185.246.128.133	ubuntu	(empty)
6.	183.81.169.238	ftpuser	123admin
7.	179.43.180.106	oracle	qwerty
8.	43.156.42.52	admin	root
9.	58.246.12.85	mysql	12345678
10.	116.110.19.150	postgres	tomcat

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 **47,775** malicious software distributed, compared to last week in which was **1,131.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	124.158.150.18	TrojanDownloader:Linux/Morila!MTB	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
2.	79.106.7.183	Backdoor:Win32/Berbew	c131865d0626d9fe0ad8ac7fd68fff6334fe45bd8200da4798b5a12b58e093f2
3.	103.111.233.162	Trojan:Linux/Downldr.B!MTB	cb831b6d75c3e9ca356f2196e36bae3d069f19a8f7d2191e6fe7c43849d916fc

4.	196.202.15.15	Trojan:Linux/Downldr.B!MTB	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	196.202.91.134	Linux/Downloader.p	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
6.	178.214.254.183	DoS:Linux/Xorddos!pz	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	218.173.4.221	Trojan:Linux/Multiverze	6574c6ad164e7ab79a33f214165f5710b07439460b85111db164d6df27967109
8.	177.46.125.251	HEUR:Trojan-Downloader.Shell.Agent.p	409e6be60a200711954b03a747748ea87de1756b2ad9e81fa6454598bdefb065
9.	1.7.210.74	Trojan:Linux/Multiverze	7901ea3019dcd61d8913ba4f2cb37a5de33123b4b58482c7a96d96660c45a5a1
10.	103.153.180.171	Trojan.Gen.NPE	18e0f574bf11bc5e7de8c95b83c187649b2d87d74651e59d9c2aad53ac7bb7f1

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,462** web attacks compared to last week which was **168.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 31st March 2024 to 6th of April, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	146.19.24.28	/
2.	78.153.140.30	/users/sign_in
3.	185.224.128.43	/favicon.ico
4.	41.78.73.146	/.env
5.	27.128.234.189	/files/
6.	66.249.77.96	/info.php

7.	52.167.144.22	/systembc/password.php
8.	41.78.38.84	/bundle.js
9.	36.88.8.247	/1.php
10.	78.153.140.37	/password.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.