TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 25th February 2024 to 2nd of March, 2024
Report No.: TZ-CERT/WRHP/2024/9

1. NETWORK ATTACKS

A total of **87,681** attacks have been recorded compared to last week's **78,186** 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	admin1234
2.	185.246.128.133	user	Pass1234
3.	162.240.146.93	admin	r00t
4.	170.64.142.230	hadoop	123456
5.	170.64.173.192	ftpuser	(empty)
6.	41.78.75.186	centos	!Q2w3e4r
7.	64.23.192.86	telnet	qwertyuiop123
8.	41.78.73.146	oracle	Win1d0W$
9.	41.78.38.139	Administrator	default
10.	43.156.225.133	mysql	p@ssw0rd!

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 **49,519** malicious software distributed, compared to last week in which was **96,384.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.250	trojan.billgates/ganiw	b43f51ff2d22190de7506715402aa89521a55d2a24f15044103dfe6fb2cb860c
2.	12.221.179.173	GenericRXIC-BY!B8ED2CB3E9FE	acb409c5449410611540005b4582cb4d1610ed0c0cf7f57fe02c305a275e1053f
3.	213.91.210.115	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

4.	41.33.207.69	Mal/Generic-S	320b50faf5bcabf75f9547829ee288e09f654db2e8af4d1f2be555ae23a6e85b
5.	196.221.166.70	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	125.164.0.143	Trojan.Linux.Generic.208033	298fbd37bd095c2fb15cf2eb742be22ba2679027f692e8bf25e392273844259c
7.	197.53.110.67	Trojan.Gen.NPE	3974a1757c786c61c5cec40d6f3af66aec799459cc51af15dca88ac3c927115d
8.	41.78.73.146	Trojan Horse	42e021e3bf960f45b0419df3134c5cf4740e6b76ab1931ac4660148794a64d88
9.	41.78.38.139	CoinMiner/Linux.Agent.30304472	62ae36274d9e33b704ce1485952cb76dea26dd84a6bf18c870db21ae1c3b7528
10.	43.156.225.133	Trojan:Linux/Multiverze	9cd71443cf6a3b601e0f9514ba1caa2f58a8fe7ea691d48f3813827525a5139b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,553** web attacks compared to last week which was **2,097.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 25th February 2024 to 2nd of March, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	63.251.106.21	/
2.	112.133.211.220	/users/sign_in
3.	146.19.24.28	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	41.78.75.186	/admin/config.php
5.	41.78.38.139	/.env

6.	41.78.73.146	/favicon.ico
7.	78.153.140.30	/etc/passwd
8.	195.3.220.159	/robots.txt
9.	20.194.236.89	/recordings/index.php
10.	66.249.64.225	/a2billing/admin/Public/index.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.