TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 17th March 2024 to 23rd of March, 2024
Report No.: TZ-CERT/WRHP/2024/12

1. NETWORK ATTACKS

A total of **430,656** attacks have been recorded compared to last week's **93,791** 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	123456
2.	193.105.134.95	admin	admin
3.	188.17.143.44	user	1234
4.	41.78.75.186	support	user
5.	41.78.73.146	ubuntu	root
6.	170.64.128.231	support	password
7.	213.109.202.127	postgres	support
8.	41.78.38.139	guest	345gs5662d34
9.	167.71.107.93	centos	3245gs5662d34
10.	134.122.43.239	oracle	12345

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 **5,027** malicious software distributed, compared to last week in which was **10,514.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.160.98.218	HEUR:Trojan-Downloader.Shell.Agent.p	cb831b6d75c3e9ca356f2196e36bae3d069f19a8f7d2191e6fe7c43849d916fc
2.	196.189.130.38	HEUR:Trojan-Downloader.Shell.Agent.p	acb409c544941061154005b4582cb4d1610ed0c0cf7f57fe02c305a275e1053f
3.	27.81.92.118	HEUR:Trojan-Downloader.Shell.Agent.p	078688efd30f25ff39d687e7a867ed9314cce33e2fc7b0e8c9c54314a4d8cf35

4.	41.38.163.71	HEUR:Trojan-Downloader.Shell.Agent.a	da5459bec0c519261d38635a328490996400f99c434bd1724f11198104a87c48
5.	109.75.36.126	Trojan-Downloader.Shell.Agent.bi	e334b7bb3d687f84b56d007a0e6f0344721916223bf3faaf44f83780487589e2
6.	118.68.165.197	Trojan-Downloader.Shell.Agent.bi	86a0e1c100dee0656823940d8b09abbe9b7f681310fb085ea8e08d20318447ec
7.	112.12.60.112	HEUR:Backdoor.Linux.Hajime.b	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
8.	120.253.19.234	HEUR:Trojan-DDoS.Linux.Xarcen.d	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
9.	94.143.198.145	HEUR:Trojan-DDoS.Linux.Xorddos.gen	320b50faf5bcabf75f9547829ee288e09f654db2e8af4d1f2be555ae23a6e85b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,539** web attacks compared to last week which was **1,521**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th March 2024 to 23rd of March, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	197.248.78.86	/
2.	63.251.106.21	/favicon.ico
3.	124.220.176.53	/admin/config.php
4.	139.59.26.221	/users/sign_in
5.	185.229.236.146	/admin/config.php?password%5B0%5D=ZIZO&username=admin
6.	20.187.100.29	/.git/config
7.	146.19.24.28	/.env
8.	150.158.55.114	/logon.htm

9.	101.36.126.204	/info.php
10.	185.224.128.43	/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.