TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 8th October to 14th of October, 2023
Report No.: TZ-CERT/WRHP/2023/41

1. NETWORK ATTACKS

A total of **48,827** attacks have been recorded compared to last week **50,807** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	193.105.134.95	root	root
2.	185.246.128.133	admin	123123
3.	218.92.0.92	mysql	password
4.	218.92.0.93	zimbra	Admin
5.	157.245.130.144	docker	123456
6.	41.78.75.186	postgres	adminHW
7.	170.64.158.52	supervisor	Wind1doW$
8.	41.78.73.146	ubuntu	123456789a
9.	129.205.194.230	sysadmin	abc123456
10.	41.78.174.124	Administrator	factory

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of the above listed credentials and default ones. Use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **43,486** malicious software distributed compared to last week in which was **52,098.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.194.240	Riskware/CoinMiner	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
2.	41.59.203.31	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
3.	41.59.37.219	trojan.hajime/genericrxhy	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

4.	113.161.147.141	Adware/Miner	286a1eebeb4b65f34f70597d798adf6245167a16735d1e20b45db9dd5a6d0b69
5.	196.218.243.41	trojan.hajime/genericrxic	b39633ff1928c7f548c6a27ef4265cfd2c380230896b85f432ff15c7c819032c
6.	14.207.162.199	ELF/Xorddos.AB!tr	ba76ffe8c2f466442077c70ed874b2459d677cece7d36cc71e2a8542c27f8c2b
7.	42.112.227.57	trojan.xorddos/ddos	0291de841b47fe19557c2c999ae131cd571eb61782a109b9ef5b4a4944b6e76d
8.	41.59.211.144	trojan.	d7f98e379c400c13340781ccb65017c000330824ea26680866b9d3e43d641721
9.	41.59.86.254	trojan.	8b3048631a205ae64d490f8805708192a200bae303f4d138338247e5a97380e8
10.	190.203.221.171	trojan.multiverze	ce98656dba7fcf84a3c583f23fe936cc5f9d0a8332bb298063322693c4f3cf9e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,086** web attacks compared to last week which was **935.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 8th October to 14th October, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	192.18.132.173	/
2.	117.132.188.205	/users/sign_in
3.	39.102.32.203	/.env
4.	41.111.188.40	/admin/config.php
5.	109.237.96.251	/favicon.ico
6.	109.237.96.124	/DeathShop.php

7.	41.78.169.54	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	41.78.73.146	/robots.txt
9.	111.217.248.101	/cgi-bin/luci/;stok=/locale?form=country
10.	72.251.232.180	/a2billing/admin/Public/index.php

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with 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 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 counter act, 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 to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.