TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 17th December to 23rd of December, 2023
Report No.: TZ-CERT/WRHP/2023/51

1. NETWORK ATTACKS

A total of **56,331** attacks have been recorded compared to last week **106,260** 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	admin	password
3.	170.64.202.140	user	user
4.	138.197.109.23	guest	root
5.	41.78.73.146	PlcmSplp	password
6.	123.30.234.78	support	(empty)
7.	170.64.210.122	vadmn	1234
8.	41.78.75.186	zyfwp	123456
9.	124.223.157.201	postgres	PlcmSplp
10.	212.70.149.150	AdminGPON	smcadmin

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 **7,478** malicious software distributed, compared to last week in which was **18,514.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	113.161.218.118	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	124.123.66.177	ELF/Xorddos.AB!tr	b927f9ff536db3dafbea0ec62c2581b3acc42da18fe6fc932be077e5e9036aaf
3.	162.19.177.251	Riskware/CoinMiner	10a1aac9eb7707893306482216b9174dde795c20dd3ea69d8c5730f5f503f33d
4.	187.144.43.83	Adware/Miner	9fa8e1aaad7c6e5fb17d

			839db348f2f063255062691754fcd11ae76d18e63a3
5.	178.59.74.177	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	151.234.87.99	trojan.xorddos/generica	0d5ba3cf3aa65d74cb6f4e90f107d2f43af373481b1a981b4f28605ef9c4c689
7.	94.158.151.213	trojan.generica/xorddos	857a73f4e00b8cee31f90b8be92c7dfc468fb2e3eca15c5955b0866d6a87b6a6
8.	213.172.83.195	trojan.xorddos/ddos	cc42731bf94ff321ee0d9c9085dde80e2ee5268d571b98594eafc5c799113cd5
9.	82.157.160.9	trojan.generica/xorddos	d2dda52df6dc7681b6bc687732dff93f8292adaa8b1ae95eb1a31c80547240d5
10.	219.138.226.132	ELF/Generic.246192!tr	5d8aab2ce5b8ba8c7b102ddaa3c89ea3ed4426acce68a64f4b1c7711a5d38308

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **954** web attacks compared to last week which was **2,164.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 17th December to 23rd December, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	69.164.194.175	/
2.	162.19.177.251	/users/sign_in
3.	47.106.35.122	/robots.txt
4.	47.78.73.146	/.env
5.	50.158.152.202	/favicon.ico
6.	41.78.73.146	/?XDEBUG_SESSION_START=phpstorm

7.	78.153.140.30	/actuator/gateway/routes
8.	101.91.107.182	/admin/config.php
9.	47.99.136.156	/systembc/password.php
10.	175.198.181.204	/cf_scripts/scripts/ajax/ckeditor/ckeditor.js

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.