TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 26th November to 2nd of December, 2023
Report No.: TZ-CERT/WRHP/2023/48

1. NETWORK ATTACKS

A total of **140,817** attacks have been recorded compared to last week **126,022** 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.	116.110.81.144	root	admin
2.	193.105.134.95	admin	qwerty123456
3.	185.246.128.133	mysql	P@ssw0rd!
4.	171.251.23.231	ftpuser	666666
5.	116.98.169.53	oracle	1234567890
6.	116.98.165.43	testuser	abc123
7.	170.64.146.197	cameras	PlcmSplp
8.	116.110.216.29	administrator	test123
9.	178.128.101.209	centos	123123
10.	41.78.73.146	webmaster	cameras

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 **269,083** malicious software distributed compared to last week in which was **195,395.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.202.15.137	downloader.bash/miraib	1276e2b8c6b6eaa3b894dc0dc5d537c19b1d8a0e9a82943b364e1c2605e38ed8
2.	182.75.41.42	Scr.Malcode!gen107	edf5f138cbae2adbe677c7e17814e4259aa68cbac2e28b59e65fb6779f81ad4a
3.	103.105.227.18	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
4.	217.64.18.107	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

5.	112.12.0.110	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	41.59.86.254	trojan.generica/xorddos	0b00e66a921aad0f036c20a7c5f3fcd1fb44b5db77248f6d6aa5cd37730a0ec4
7.	77.236.64.250	trojan.xorddos/ddos	8b2da61a9dff50b3ad272832f29cd02cedd1ce593b18f51a7bc49d3852870956
8.	41.78.64.252	trojan.	3f97d465f56417e08438bad7dc3c562293526826ae76d551267286b91d42822a
9.	213.55.92.81	trojan.genericrxss/r002c0pjf23	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
10.	37.238.90.9	trojan.mirai/uselvi223	d16bffbd3ba31504aea1fc01e66e29ad5927830ea5e2cc49369e82a7c68ec5c0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,221** web attacks compared to last week which was **3,426.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th November to 2nd December, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	172.16.37.39	/
2.	72.251.232.180	/admin/config.php
3.	141.98.11.107	/users/sign_in
4.	125.254.33.115	/favicon.ico
5.	138.68.5.135	/admin/config.php?password%5B0%5D=ZIZO&username=admin
6.	144.126.223.151	/robots.txt
7.	170.253.22.48	/.env
8.	177.54.147.173	/a2billing/admin/Public/index.php
9.	200.105.172.195	/recordings/index.php
10.	68.183.81.47	/boaform/admin/formLogin

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.