TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 16th of January – 22nd of January, 2023
Report No.: TZ-CERT/WRHP/2023/03

1. NETWORK ATTACKS

A total of **230,937** attacks have been recorded compared to last week **237,166** 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.	137.103.254.193	root	admin
2.	193.105.134.95	admin	Plcmsplp
3.	195.3.147.52	support	123456
4.	41.78.174.77	Plcmsplp	1234
5.	171.225.185.110	345gs5662d34	345gs5662d34
6.	45.249.100.22	oracle	support
7.	41.78.73.121	user	password
8.	171.225.184.148	ubuntu	P@ssw0rd
9.	171.225.184.145	supervisor	root
10.	41.78.174.124	pi	user

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 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 **144,797** malicious software distributed compared to last week in which was **88,524**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	195.135.213.241	Trojan.Generic.32974639	c801a195cb85ddc6bfe5b95114a078b9be030d80cedeceba1e4c20d3858418aa
2.	196.221.165.184	HEUR:Backdoor.Linux.Gafgyt.b	db06a40d33db2416bcc452736ad5ee7b4035c457b3f7d559b05ec200d6a8c7a5
3.	69.197.181.58	Trojan.Generic.32975353	bc5964d46a872260b429717a7263ccbece8592b34b84869563d6092

			c868a253a
4.	41.78.64.254	Trojan.GenericKD.6497586 1	7aa6518ffe1f152fe800 886311d208b4387a06 9b5b06f82a3c1c7cd61 67e90be
5.	196.41.222.98	HEUR:Trojan.Linux.Mirai.g en	5ccca568d1bbe95513a 06ce9f49d67797e6c72 a08b39f2a62f45bc018 0455e31
6.	196.41.222.5	Trojan.Linux.Generic.2461 92	1f75cc0468c6d9137bc 3de29e3674e181ea20 5eb12b93347e753810 987f56b14
7.	61.177.173.21	Trojan.Linux.Generic.2461 92	a0035ef408f06db49ad a52f30fc42451689a1b 1086759a373a056563 53a14ead
8.	41.93.47.66	Trojan.Linux.GenericKD.40 003689	c70ca8df777bfc5a77d0 6eb625a0e6d7afdcd56 3df02a2d16de95813ae 717a31
9.	78.187.174.241	HEUR:Trojan-DDoS.Linux.Xarcen.d	ea40ecec0b30982fbb1 662e67f97f0e9d6f43d2 d587f2f588525fae683a bea73
10.	109.199.253.21	Trojan.Win32.Eb.dqb	f4ac4f735b9ff260a275 734d86610dccb8558d1 a54c6d6a78a94c33b6a af6e39

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,910** web attacks compared to last week which was **5,635.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th of January – 22nd of January, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URL
1.	183.136.225.32	/
2.	54.202.241.125	/users/sign_in
3.	72.251.235.155	/boaform/admin/formLogin
4.	125.229.108.134	/favicon.ico
5.	188.166.96.85	/robots.txt

6.	3.6.155.76	/admin/config.php
7.	41.78.169.54	/.env
8.	121.173.126.140	/admin/config.php?password%5B0%5D=ZIZO&username=ad
9.	89.248.171.23	/.well-known/security.txt
10.	103.57.9.39	/recordings/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.