TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 15th of January – 21st of January, 2023
Report No.: TZ-CERT/WRHP/2023/4

1. NETWORK ATTACKS

A total of **231,875** 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	P@ssw0rd
3.	195.3.147.52	support	Aa123456
4.	41.78.174.77	ubuntu	1234567890
5.	101.204.27.20	guest	345gs5662d34
6.	171.225.185.113	user	RIP000
7.	45.249.100.22	supervisor	default
8.	41.78.73.121	test	Win1doW$
9.	171.225.184.145	postgres	support
10.	41.78.174.124	mysql	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 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 **122,450** malicious software distributed compared to last week in which was **469,019**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan Horse	c801a195cb85ddc6bfe5b95114a078b9be030d80cedeceba1e4c20d3858418aa
2.	195.135.213.241	Trojan.Generic.31654391	a0035ef408f06db49ada52f30fc42451689a1b1086759a373a05656353a14ead
3.	196.221.165.184	TrojWare.Script.TrojanDownloader.Agent.	c70ca8df777bfc5a77d06eb625a0e6d7afdcd563df02a2d16de95813ae717a31
4.	69.197.181.58	HEUR:Trojan-	db06a40d33db2416bcc

		Downloader.Shell.Agent.p	452736ad5ee7b4035c457b3f7d559b05ec200d6a8c7a5
5.	196.41.222.98	HEUR:Trojan-Downloader.Shell.Agent.bc	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
6.	41.93.47.66	Trojan.Linux.Generic.246192	bc5964d46a872260b429717a7263ccbece8592b34b84869563d6092c868a253a
7.	78.187.174.241	Linux.MiraiTrojan.Linux.GenericKD.40003689	e056263435f622034d4bc2375b2f60619e9e7dd0cabaaa34f8ade90649d8e213
8.	109.199.253.21	Trojan.Linux.GenericKD.40003689	8536b4ebc530e81acce899611c92f66b944bc9bae57d5bf299719df66ab7bebf
9.	196.219.110.131	HEUR:Trojan-DDoS.Linux.Xarcen.d	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
10.	219.79.221.202	Trojan.Win32.Eb.dqb	f4ac4f735b9ff260a275734d86610dccb8558d1a54c6d6a78a94c33b6aaf6e39

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,032** 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 15th of January – 21st of January, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	183.136.225.32	/
2.	54.212.184.101	/users/sign_in
3.	54.202.241.125	/favicon.ico
4.	20.24.49.95	/boaform/admin/formLogin
5.	72.251.235.155	/robots.txt
6.	125.229.108.134	/admin/config.php

7.	188.166.96.85	/.env
8.	64.223.173.182	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	82.65.53.67	/core/img/favicon.ico
10.	91.89.26.29	/debug/default/view?panel=config

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.