TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 12th to 18th of March, 2023
Report No.: TZ-CERT/WRHP/2023/11

1. NETWORK ATTACKS

A total of **190,857** attacks have been recorded compared to last week **206,900** 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.	143.198.98.252	root	admin
2.	164.163.98.28	admin	support
3.	116.98.175.245	support	123456
4.	116.110.124.135	postgres	admin1234
5.	195.3.147.52	guest	password
6.	193.105.134.95	ansible	PlcmSplp
7.	171.251.19.118	support	root
8.	1.117.140.148	ftpuser	1111111
9.	171.251.17.185	mysql	(empty)
10.	116.105.218.96	test	1234qwer

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 **152,551** malicious software distributed compared to last week in which was **475,897**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.31	trojan.linux/mirai	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	41.59.211.41	trojan.miraib/bash	d4d8cbf1a0b4a7617b6f3a7ced737c123ed3a3da20192862a84c1f6f7dc75edf
3.	41.59.86.254	trojan.linux/hajime	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
4.	196.219.22.123	trojan.linux/xorddos	ea40ecec0b30982fbb1

			662e67f97f0e9d6f43d2d587f2f588525fae683abea73
5.	91.202.181.130	trojan.linux/hajime	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	41.78.64.254	trojan.linux	ab31ea17ea415efd30a19fdb7a68b92146692b76584007cbbb94f55b9761b8dc
7.	41.254.42.74	trojan.linux	8c5e2b96cb61ebb3750f5be23fc9aca14d7ac97efb7d57afebd85472dcc8e015
8.	85.96.191.210	Trojan.Linux.Generic.246192	e6ce9937266d30a22c6aa5c48d818dba86491b1becf1fe0ca07b3de85d2d88ab
9.	196.202.44.183	HEUR:Trojan-DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
10.	105.246.56.90	Trojan.Win32.Eb.dqb	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **5,544** web attacks compared to last week which was **5,708**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 12th to 18th of March, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	23.175.48.202	/
2.	122.168.198.123	//admin/config.php
3.	45.93.16.73	/users/sign_in
4.	46.19.51.104	/cgi-bin/snapshot.cgi?channel=0
5.	5.196.64.124	/favicon.ico
6.	212.192.2.145	/cgi-bin/snapshot.cgi?channel=1

7.	139.255.35.181	/boaform/admin/formLogin
8.	196.43.199.70	/recordings/
9.	41.78.174.77	/.env
10.	193.32.162.159	/cgi-bin/snapshot.cgi?channel=2

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.