TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 19th to 25th of March, 2023
Report No.: TZ-CERT/WRHP/2023/12

1. NETWORK ATTACKS

A total of **95,892** attacks have been recorded compared to last week **190,857** 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.	116.98.161.159	root	admin
2.	193.105.134.95	admin	support
3.	195.3.147.52	support	123456
4.	116.98.164.61	PlcmSplp	admin1234
5.	116.110.28.95	guest	password
6.	171.251.19.177	user	PlcmSplp
7.	116.98.172.112	test	1234
8.	41.78.174.77	default	root
9.	47.242.173.58	pi	12345
10.	41.78.75.186	ubnt	(empty)

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 **99,387** malicious software distributed compared to last week in which was **152,551**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan:Linux/Multiverze	169e1952898276010f212f609c4956a4fd89daa35ce3fa45c31357b44149efaf
2.	41.59.86.254	Trojan.Gen.NPE	4bf044ae7b903ca9edf19180b617abd363bf981d4a22d0b0de13fa72461be4fa
3.	85.105.1.47	trojan.linux/hajime	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09

			f0
4.	41.59.211.41	UDS:Backdoor.Linux.Mirai	dadd035cac52ae08767a9aea15761678f8a3ebad09f55d3a36e2205387a15bcd
5.	41.59.203.192	trojan.linux/hajime	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	197.26.59.0	trojan.linux	ab31ea17ea415efd30a19fdb7a68b92146692b76584007cbbb94f55b9761b8dc
7.	60.189.35.80	trojan.linux	8c5e2b96cb61ebb3750f5be23fc9aca14d7ac97efb7d57afebd85472dcc8e015
8.	177.9.40.160	Trojan.Linux.Generic.246192	e6ce9937266d30a22c6aa5c48d818dba86491b1becf1fe0ca07b3de85d2d88ab
9.	91.192.47.240	HEUR:Trojan-DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
10.	201.148.254.181	Trojan.Win32.Eb.dqb	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,011** web attacks compared to last week which was **5,544**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th to 25th of March, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URL
1.	122.168.198.123	/
2.	154.118.226.222	/users/sign_in
3.	34.69.252.51	/boaform/admin/formLogin
4.	189.156.117.17	/favicon.ico
5.	193.42.33.177	/.env

6.	197.250.198.39	/recordings/
7.	41.78.174.77	/.git/config
8.	15.207.205.251	//ajax.php?yokyok=ls
9.	193.32.162.159	/robots.txt
10.	41.78.75.186	/index.php/heartbeat

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.