TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 20th August to 26th of August, 2023
Report No.: TZ-CERT/WRHP/2023/34

1. NETWORK ATTACKS

A total of **53,365** attacks have been recorded compared to last week **83,906** 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.	218.92.0.92	root	admin
2.	210.113.102.171	admin	123456
3.	193.105.134.95	(empty)	12345
4.	185.246.128.133	user	1234
5.	104.236.245.68	ubnt	password
6.	113.57.92.188	guest	123
7.	170.64.131.135	support	ubnt
8.	41.78.75.186	supervisor	support
9.	41.78.174.124	Accept:*/*	1234567890
10.	45.95.146.78	Cameras	(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 **21,923** malicious software distributed compared to last week in which was **176,698.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.252	trojan.mirai/xxjvd	93308cc75fe66f4a9a658082a27f024a9d47265549845a81c9073b451ec5eea0
2.	41.59.211.41	trojan.hajime/siggen	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
3.	139.255.109.154	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
4.	182.255.48.138	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a4

			26fb215708b6c6daa3de3
5.	179.6.39.94	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
6.	47.110.74.113	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	176.109.14.126	trojan.xorddos/ddos	320b50faf5bcabf75f9547829ee288e09f654db2e8af4d1f2be555ae23a6e85b
8.	41.59.201.7	trojan.linux/malxmr	c88e1dacce96cafa2038f7433fc9e42e7b26714c36e98ed59c483360a4b7cb58
9.	189.8.19.186	Riskware/CoinMiner	f2ee717e515f2033bd511ad741f76f2d829bcaad0aeb7b9d0f9091acf43f2297
10.	41.78.64.252	trojan.linux	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,066** web attacks compared to last week which was **2,176.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th August to 26th of August, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	147.124.221.247	/
2.	164.90.176.224	/users/sign_in
3.	54.255.166.167	/41.78.64.60/.env
4.	41.78.174.124	/favicon.ico
5.	143.42.50.168	/.env
6.	41.78.169.54	/robots.txt
7.	41.78.75.186	/boaform/admin/formLogin
8.	109.237.96.251	/1.php
9.	109.237.96.124	/?XDEBUG_SESSION_START=phpstorm
10.	148.113.16.121	/aaa9

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.