TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 13th August to 19th of August, 2023
Report No.: TZ-CERT/WRHP/2023/33

1. NETWORK ATTACKS

A total of **83,906** attacks have been recorded compared to last week **81,880** 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.	193.105.134.95	root	1qaz@wsx
2.	185.246.128.133	admin	postgres
3.	45.142.182.120	guest	root123
4.	104.236.245.68	ftpuser	Win1doW$
5.	170.64.131.96	sftp	admin123
6.	170.64.137.108	centos	P@ssw0rd
7.	170.64.153.50	hadoop	123456
8.	170.64.153.3	jenkins	888888
9.	170.64.153.16	oracle	dbadmin
10.	15.204.76.69	postgres	Aa123456

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 **176,698** malicious software distributed compared to last week in which was **89,587.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Trojan:Script/Wacatac.B!ml	eeec1c5486101eb5855846e11738b31e3178c92a8dcb181cee8a766d4547ad95
2.	41.59.194.240	Linux.Xorddos	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
3.	196.190.222.242	ELF/Hajime.A!tr	95cb198454a5ec16e297a5f4c4f7c424e23ddb8ce2432bbe07e81e723279e242

4.	41.59.201.132	Downloader.Trojan	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
5.	196.41.210.118	HEUR:Trojan-Downloader.Shell.Agent.a	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	196.41.206.22	Linux/DDoS-CIF	0b00e66a921aad0f036c20a7c5f3fcd1fb44b5db77248f6d6aa5cd37730a0ec4
7.	41.59.196.23	Trojan Horse	6b6c1bd77604a85b0abcd98103eb738ca94cc1fbf74043f62ed95ec5561e507f
8.	196.127.23.179	trojan.linux/malxmr	c88e1dacce96cafa2038f7433fc9e42e7b26714c36e98ed59c483360a4b7cb58
9.	200.84.45.132	Riskware/CoinMiner	f2ee717e515f2033bd511ad741f76f2d829bcaad0aeb7b9d0f9091acf43f2297
10.	116.107.52.26	trojan.linux	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,176** web attacks compared to last week which was **1,096.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 13th August to 19th of August, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	103.110.84.47	/
2.	122.155.108.140	/users/sign_in
3.	148.113.16.121	/favicon.ico
4.	60.217.75.70	/robots.txt
5.	109.237.96.251	/sitemap.xml
6.	109.237.96.124	/assets/webpack/main.a66b6c66.chunk.js

7.	41.78.169.54	/aaa9
8.	41.78.174.124	aab8
9.	43.158.217.52	/.well-known/security.txt
10.	41.78.75.186	/assets/built/screen.css?v=8cfc086fe8

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.