TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 6th August to 12th of August, 2023
Report No.: TZ-CERT/WRHP/2023/32

1. NETWORK ATTACKS

A total of **81,880** attacks have been recorded compared to last week **64,231** 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.	113.74.181.39	root	1qaz@wsx
2.	193.105.134.95	admin	postgres
3.	185.246.128.133	guest	root123
4.	170.64.137.108	ftpuser	Win1soW$
5.	195.181.87.1	dbadmin	admin123
6.	151.245.36.251	support	P@ssw0rd
7.	45.95.147.201	tomcat	123456
8.	45.95.147.207	jenkins	prometheus
9.	104.236.245.68	oracle	dbadmin
10.	103.108.60.16	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 **89,587** malicious software distributed compared to last week in which was **164,841**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.41.210.118	Trojan:Script/Wacatac.B!ml	141e2d75c8ee93b8440b203491d1310db4e69a3ff1c76397583833f77cbd4927
2.	41.59.194.240	Linux.Xorddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
3.	196.188.125.85	ELF/Hajime.A!tr	ad14c1c5e519cbe4b45697eebd2b8de306d67b74cd3e04cd282b6f96d9e47cb9

4.	196.201.233.99	Downloader.Trojan	ad14c1c5e519cbe4b45697eebd2b8de306d67b74cd3e04cd282b6f96d9e47cb9
5.	101.255.158.119	HEUR:Trojan-Downloader.Shell.Agent.a	46ff9f7c0e437df7dd6e1c69790c8fc94e65091e9f3cf1f3243c808f1a1e8621
6.	179.189.22.210	Linux/DDoS-CIF	b4450587b34bf630f24ec1a735e9b2d6c64d7c0050cdf1f807ec95feed7211d4
7.	200.84.165.199	trojan.linux/hajime	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	92.249.236.223	trojan.linux/malxmr	bbb06ba693b01a90afa8f0552a33991a800ee051b667eafe5afdb1caa4c8861e
9.	5.25.174.87	trojan.linux/uselvk422	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
10.	186.223.124.190	trojan.linux	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,096** web attacks compared to last week which was **1,018.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 6th August to 12th of August, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	178.212.32.4	/
2.	185.230.55.9	/users/sign_in
3.	77.91.87.196	/assets/favicon-7901bd695fb93edb07975966062049829afb56cf11511236e61bcf425070e36e.png
4.	109.237.96.251	/robots.txt
5.	70.38.10.158	/assets/webpack/commons~pages.ldap.omniauth_callbacks~pages.omniauth_callbacks~pages.sessions~pa

		ges.sessions.new.432e20dc.chunk.js
6.	57.128.37.150	/assets/webpack/main.a66b6c66.chunk.js
7.	70.38.10.151	/assets/webpack/pages.sessions.new.6dbf9c97.chunk.js
8.	192.175.111.239	/assets/webpack/runtime.9fcb75d4.bundle.js
9.	109.237.96.124	/favicon.ico
10.	192.175.111.254	/.env

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.