TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 3rd September to 9th of September, 2023
Report No.: TZ-CERT/WRHP/2023/36

1. NETWORK ATTACKS

A total of **84,924** attacks have been recorded compared to last week **39,100** 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.	109.115.248.87	root	admin
2.	218.92.0.92	admin	123456
3.	185.246.128.133	postgres	password
4.	193.105.134.95	user	default
5.	41.78.174.124	anonymous	Win1doW$
6.	41.78.75.186	guest	Admin1234
7.	41.78.73.146	support	P@ssw0rd!!
8.	93.179.90.178	supervisor	Welcom123!
9.	123.190.11.15	centos	abc123$$
10.	175.178.157.198	dbadmin	qwerty123456

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 **21,688** malicious software distributed compared to last week in which was **5,029.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	103.94.113.90	trojan.mirai/xxjvd	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
2.	196.219.246.26	ELF/Hajime.A!tr	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	124.8.181.211	trojan.hajime/genericrxhy	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

4.	154.247.102.111	trojan.hajime/genericrxhy	fc4ad4bd76c21eeec817d7c227459fad6fd9f5e9c860242297f28977f775294e
5.	180.188.255.234	trojan.hajime/genericrxhy	70b02aa3b699608da57c13b052fa05f7ab3d023adc3b212430126482dd363fcf
6.	196.41.206.22	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	41.138.171.53	trojan.xorddos/ddos	320b50faf5bcabf75f9547829ee288e09f654db2e8af4d1f2be555ae23a6e85b
8.	148.113.16.121	trojan.linux/malxmr	c88e1dacce96cafa2038f7433fc9e42e7b26714c36e98ed59c483360a4b7cb58
9.	201.80.0.253	Riskware/CoinMiner	f2ee717e515f2033bd511ad741f76f2d829bcaad0aeb7b9d0f9091acf43f2297
10.	41.78.64.252	trojan.linux	eaf9adb4bb80316a3aafceabc0f2ed2aed7c76cf134b9b7c66226fc4f003aa97

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,606** web attacks compared to last week which was **1,371.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 3rd September to 9th September, 2023 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	103.255.241.98	/
2.	154.49.246.226	/users/sign_in
3.	161.35.109.35	//admin/config.php
4.	203.177.89.27	/boaform/admin/formLogin
5.	47.240.21.19	/.env
6.	103.110.84.228	/favicon.ico

7.	20.68.171.79	/db/dbweb/index.php?lang=en
8.	41.78.174.124	/administrator/pma/index.php?lang=en
9.	41.78.169.54	/phpMyAdmin-5.1.1/index.php?lang=en
10.	109.237.96.251	/phpMyAdmin/index.php?lang=en

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.