TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 10th September to 16th of September, 2023
Report No.: TZ-CERT/WRHP/2023/37

1. NETWORK ATTACKS

A total of **41,265** attacks have been recorded compared to last week **84,924** 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	guest	password
4.	193.105.134.95	(empty)	1234
5.	41.78.174.124	user	12345
6.	41.78.75.186	ubnt	adminHW
7.	41.78.73.146	factory	Win1doW$
8.	93.179.90.178	mother	54321
9.	123.190.11.15	supervisor	ubnt
10.	175.178.157.198	3comcso	root

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 **10,714** malicious software distributed compared to last week in which was **21,688.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	61.153.58.90	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
2.	41.226.34.5	ELF/Hajime.A!tr	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	148.113.16.121	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

4.	84.54.51.168	ELF/Xorddos.AB!tr	fc4ad4bd76c21eeec817d7c227459fad6fd9f5e9c860242297f28977f775294e
5.	60.173.93.10	ELF/Xorddos.AB!tr	2f25d1d2f7be1a6e740d47d5d662db56a20582eec9d201431e8cb710bd033aea
6.	41.78.169.54	Trojan:Win32/Ditertag.A	58944a1fbaeec105fa012d0dd6dc2d4982add9bf35c2873be1c188f6cf77d476
7.	208.100.26.231	Riskware/CoinMiner	217a3a1d4bb89fc2df78d0d20f1b42bcf2289fcba7ac5d0fef898b0f57d70c48
8.	50.31.21.5	trojan.linux/malxmr	c88e1dacce96cafa2038f7433fc9e42e7b26714c36e98ed59c483360a4b7cb58
9.	201.80.0.253	Riskware/CoinMiner	f2ee717e515f2033bd511ad741f76f2d829bcaad0aeb7b9d0f9091acf43f2297
10.	152.32.247.130	trojan.linux	eaf9adb4bb80316a3aafceabc0f2ed2aed7c76cf134b9b7c66226fc4f003aa97

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,097** web attacks compared to last week which was **1,606.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 10th September to 16th September, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	158.179.26.107	/
2.	134.255.217.63	/users/sign_in
3.	41.78.73.146	/favicon.ico
4.	41.78.169.54	/robots.txt
5.	41.78.75.186	/.env
6.	183.136.225.32	/boaform/admin/formLogin
7.	41.78.174.124	/DeathShop.php

8.	148.113.16.121	/actuator/gateway/routes
9.	109.237.96.124	/?XDEBUG_SESSION_START=phpstorm
10.	185.100.53.56	/core/img/favicon.ico

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.