TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 9th July to 15th of July, 2023
Report No.: TZ-CERT/WRHP/2023/28

1. NETWORK ATTACKS

A total of **55,533** attacks have been recorded compared to last week **50,286** 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.	195.3.147.52	root	123456
2.	193.105.134.95	admin	admin
3.	41.78.75.186	user	(empty)
4.	41.78.174.124	(empty)	password
5.	41.78.174.77	oracle	root
6.	111.6.24.12	guest	1234
7.	117.239.76.153	postgres	user
8.	14.116.193.108	mysql	ubnt
9.	36.56.10.154	ubnt	12345
10.	43.245.85.164	jenkins	postgres

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 **110,584** malicious software distributed compared to last week in which was **84,509**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.190.222.128	trojan.linux/mirai	e157ed8de3ca37e9be1f6f48f1b78cab567a0c84648425b5d6d307fd0af602f6
2.	196.41.206.22	trojan.mirai/linux	bc90c376f7710916d0dbbfa15646af0268c73c272f884d2abdc44a16eba9bbb7
3.	124.107.139.69	trojan.linux/hajime	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	196.41.10.182	trojan.linux/hajime	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	41.59.201.7	trojan.linux/hajime	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
6.	196.221.69.223	trojan.linux/hajime	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
7.	196.188.0.172	ELF/Agent.MKVM!tr	0aa4b85087c0bb27544d908682f7df7ba5d6987206cf317263b7b018f6bcda2e
8.	196.201.233.33	trojan.linux/uselvf623	c9f53c5a7971ce9053edf75583484635154ad09b791cfde914775d49045b1328
9.	196.202.54.142	trojan.linux/uselvk422	c29dc96f96e7d23e18b4cb242dc404a22b5bfc39dd4489a24c30b942ef52742a
10.	196.203.231.205	trojan.linux	f9dd7e02a76377e7e61e1283ac8acc44afc39ffcd71fac362654649e1f524831

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,542** web attacks compared to last week which was **2,021.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 9th July to 15th of July, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	20.254.98.165	/
2.	122.168.198.123	//admin/config.php
3.	185.224.128.213	/users/sign_in
4.	213.109.202.66	/admin/config.php
5.	109.237.96.124	/favicon.ico

6.	41.78.174.124	/.env
7.	109.237.96.251	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
8.	41.78.174.77	/boaform/admin/formLogin
9.	41.78.75.186	/robots.txt
10.	41.78.169.54	/aab8

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.