TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 23rd July to 29th of July, 2023
Report No.: TZ-CERT/WRHP/2023/30

1. NETWORK ATTACKS

A total of **75,026** attacks have been recorded compared to last week **39,815** 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.	193.105.134.95	root	P@ssw0rd
2.	195.3.147.52	admin	admin1
3.	170.64.191.240	guest	oracle
4.	218.92.0.125	ftpuser	admin1234
5.	59.173.31.105	ubnt	12345678
6.	35.230.148.14	support	1qaz@wsx
7.	218.92.0.123	telnet	password123
8.	174.87.71.7	administrator	Win1doW$
9.	51.158.240.138	azureuser	cameras
10.	43.142.109.64	postgres	ubuntu

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 **221,577** malicious software distributed compared to last week in which was **45,504.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Trojan:Script/Wacatac.B!ml	eeec1c5486101eb5855846e11738b31e3178c92a8dcb181cee8a766d4547ad95
2.	41.59.201.7	Linux.Xorddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
3.	31.47.1.30	trojan.hajime/linux	66e0f3674a66647d5a9e23f47f889d4e3ad9b4a66db8f3def48d4675374d12f7

4.	41.64.170.173	Downloader.Trojan	ad14c1c5e519cbe4b45697eebd2b8de306d67b74cd3e04cd282b6f96d9e47cb9
5.	196.41.210.118	HEUR:Trojan-Downloader.Shell.Agent.a	5dd9965275a82e4e20f917c8fc28613f63196f9d8608359889128589b84b1117
6.	198.37.105.226	Linux/DDoS-CIF	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
7.	41.59.194.240	trojan.linux/hajime	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
8.	1.170.132.113	trojan.linux/malxmr	17f551e0a1ca78baf32038c6de781452386726293c0c222203e08f3eb08119b2
9.	190.78.16.187	trojan.linux/uselvk422	c29dc96f96e7d23e18b4cb242dc404a22b5bfc39dd4489a24c30b942ef52742a
10.	196.218.167.234	trojan.linux	f9dd7e02a76377e7e61e1283ac8acc44afc39ffcd71fac362654649e1f524831

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,296** web attacks compared to last week which was **767.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 23rd July to 29th of July, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	54.234.44.21	/
2.	109.237.96.124	/users/sign_in
3.	3.227.252.118	/favicon.ico
4.	109.237.96.251	/robots.txt
5.	213.109.202.66	/.env
6.	41.78.75.186	/boaform/admin/formLogin

7.	41.78.169.54	/sitemap.xml
8.	41.78.174.124	/core/img/favicon.ico
9.	183.136.225.48	/geoip/
10.	41.78.174.77	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

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.