TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 21st to 27th of May, 2023
Report No.: TZ-CERT/WRHP/2023/21

1. NETWORK ATTACKS

A total of **85,414** attacks have been recorded compared to last week **309,427** 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	admin
2.	195.3.147.52	admin	password
3.	213.109.160.99	guest	123456
4.	171.251.24.238	user	12345
5.	111.198.57.24	ubnt	1234
6.	41.78.174.77	support	root
7.	41.78.75.186	postgres	admin123
8.	5.10.250.122	test	1qaz@WSX
9.	218.92.0.90	pi	user
10.	20.219.149.128	supervisor	ubnt

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 **147,125** malicious software distributed compared to last week in which was **617,039**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.141	Linux.Mirai!g2	818675ba09b4883e57790aff9a79669275dfe088d02dc5f5cf459b16375d17db
2.	41.59.194.240	Trojan.Linux.GenericKD.11272	dffb31311e22e5cf804b010bfab84944de6bdf596f3bdad5e5fd57fde68329ad
3.	185.81.157.31	Trojan:Linux/Multiverze	77a2c317ca9d43acc056cf8217a8c838d23af63965b33dc931877360d5919b8d
4.	41.59.201.132	trojan.linux/hajime	a04ac6d98ad9893127

			83d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	41.59.41.28	Trojan:Linux/Downldr.B!MTB	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	41.65.167.246	trojan.linux	ab31ea17ea415efd30a19fdb7a68b92146692b76584007cbbb94f55b9761b8dc
7.	41.59.200.32	trojan.linux	9ec9a97605509da77411ab9b0267c25fb8074e36e2d96adb50a144d6dcf35620
8.	41.78.64.252	Riskware/CoinMiner	edadd035cac52ae08767a9aea15761678f8a3ebad09f55d3a36e2205387a15bcd
9.	41.59.196.23	HEUR:Trojan-DDoS.Linux.Xarcen.d	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
10.	41.211.106.43	Trojan.Win32.Eb.dqb	4bf044ae7b903ca9edf19180b617abd363bf981d4a22d0b0de13fa72461be4fa

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,070** web attacks compared to last week which was **3,291**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 21st to 27th of May, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	86.14.185.18	/users/sign_in
3.	121.200.50.180	/boaform/admin/formLogin
4.	210.114.17.205	/favicon.ico
5.	222.127.31.237	/.env

6.	109.237.96.251	/robots.txt
7.	84.252.140.133	/.git/config
8.	83.97.73.89	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	109.237.96.124	/manual.txt
10.	41.78.169.54	/1.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.