TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 28th of July, 2024 to 3rd of August, 2024
Report No.: TZ-CERT/WRHP/2024/32

1. NETWORK ATTACKS

A total of **700,018** attacks have been recorded compared to last week's **741,888** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	78.154.174.174	root	admin1234
2.	149.28.203.19	centos	changeme
3.	76.16.229.249	administrator	qwerty
4.	125.212.204.18	postgres	abc123
5.	162.254.168.226	ftpuser	P@ssw0rd
6.	218.92.0.97	ubuntu	Password1
7.	52.200.29.169	jenkins	1q2w3e4r
8.	197.149.95.74	docker	pass
9.	183.81.169.238	test	123456789
10.	218.92.0.24	mysql	M1n3cr4ft123

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and passwords be made to avoid use of the above listed credentials and default ones. The use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **228,343** malicious software distributed, compared to last week in which was **195,120.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.32.1.92	HEUR:Trojan-Downloader.Shell.Agent.dh	093a6470fe8bde8a7ef9cf3f21c169f41e19f88f9165b1782b7ede6f45d2e782
2.	205.209.166.133	BASH/Dloader.AAN!tr.dldr	61e01dd195cffd031765c0cfe190a3fa90b22beb02d65eccdfd437a0fc2c341f
3.	117.236.99.117	Trojan.Gen.NPE	27463e58f56397edbd9f329378d71bda4e2b7b89fca12cfc68c6e91cd44f656d

4.	154.177.200.189	trojan.xorddos/ddos	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
5.	116.105.224.103	Trojan:Linux/CoinMiner	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	122.185.155.182	miner.r002c0dgm24/xmrig	28dc11bfe01f303a15c73150a9a7cdfda39828722c8ecb698147f78c500140a6
7.	41.220.30.134	miner.gafin/r002c0dga24	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
8.	89.36.67.207	Application.Linux.Generic.24172	66354c8878ca935f0fc6e3623e190e8a400318ded4c8d3d7baa85873059bc179
9.	86.57.138.171	miner.qbumq/r002c0dgm24	929efd52db47fe4723fb8532104b612f82414bc2c48639cfbf1dac69378f76fd
10.	115.187.30.27	miner.r002c0dga24/ulxhm	836545ce7bb472c89b272e295ae92fd9fcdf6142a9f0bc5cfceedfeaa7dd6c9e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,268** web attacks compared to last week which was **4,537.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 28th of July, 2024 to 3rd of August, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.184.125	/
2.	185.191.126.213	/admin/config.php
3.	149.50.103.48	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	213.35.98.119	/favicon.ico
5.	213.37.156.66	/logon.htm

6.	77.240.99.157	/robots.txt
7.	100.42.185.220	/recordings/index.php
8.	185.224.128.43	/a2billing/admin/Public/index.php
9.	185.224.128.74	/.env
10.	92.249.48.202	/.well-known/security.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,132** ICS attacks compared to last week which was **3,059.**

From the table below these are the top 5 ICS attacks and their associated attacking IP, exploited protocols and exploited ports as detailed for the period between 28th of July, 2024 to 3rd of August, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	123.58.207.140	IEC104	2404
2.	45.79.132.227	kamstrup_protocol	1025
3.	13.245.17.35	guardian_ast	10001
4.	207.90.244.10	snmp	161
5.	193.177.182.119	kamstrup_management_protocol	50100

Table4: Top 5 ICS attacking IP

5. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with the most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

5.1 Note that most of the 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 counteract, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

5.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

5.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

5.4 Deploy Intrusion Detection System (IDS) and configure it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.