TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 11th of August, 2024 to 17th of August, 2024
Report No.: TZ-CERT/WRHP/2024/34

1. NETWORK ATTACKS

A total of **335,038** attacks have been recorded compared to last week's **593,519** 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.	86.109.115.67	root	admin1234
2.	162.254.168.226	debian	changeme
3.	157.245.241.17	admin	qwerty
4.	14.161.253.60	postgres	abc123
5.	125.212.204.18	ftpadmin	P@ssw0rd
6.	14.241.236.82	ubuntu	!@#qwerASDF
7.	149.28.203.19	sa	1q2w3e4r
8.	45.5.110.242	docker	cisco@12321
9.	117.247.227.45	tester	123456789xd
10.	14.161.49.219	mysql	123456

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 **43,901**malicious software distributed, compared to last week in which was **153,382.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	105.103.64.208	HEUR:Trojan.Linux.Miner.gen	0098cfff9e6056e6cf9e1e34a798110a2b6b42fca27652eeabc5bbcbe11b6be2
2.	41.232.106.110	HEUR:Trojan.Linux.Miner.gen	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
3.	103.139.47.162	Trojan:Win32/Mirai!ml	59f7ddd5211671eed5b8c378e228a24d849fe0a1c043941dfd4602029c66f216

4.	103.114.221.11	PossibleThreat	629db57b96d6e965401d866f895d86c542efe344b3d489630a6ec09d643add76
5.	41.38.195.170	HEUR:Trojan.Linux.Miner.gen	67db999e9ab18659c1d595c9112ac9b22065cf05328c156585bda8589d10cb70
6.	41.98.239.207	HEUR:Trojan-DDoS.Linux.Xarcen.d	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	41.131.216.2	HEUR:Trojan-DDoS.Linux.Xorddos.gen	57b0ede720a32dc5a2f80f4c9befbd1d6c2c6f88146ff64ea4fac600276546ea
8.	41.33.164.91	HEUR:Trojan-DDoS.Linux.Xorddos.gen	8869cf20032ac6bcf7fc15332f2f1aa5f3162666cc712294e2c9c0b1c1b7a91a
9.	171.242.79.4	HEUR:DoS.Linux.Agent.eb	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
10.	103.110.237.142	Not-a-virus:HEUR:RiskTool.Linux.BitCoinMine	2480312d23e1d009b3ea04d722c8c671b0dc4c57bbd75fc3a2eaa4a135ad647a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,382** web attacks compared to last week which was **7,428.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 11th of August, 2024 to 17th of August, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	66.249.64.105	/
2.	173.231.184.125	/admin/config.php
3.	185.191.126.213	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	66.249.64.106	/favicon.ico
5.	66.249.64.107	/.env

6.	149.50.103.48	/logon.htm
7.	181.196.136.94	/robots.txt
8.	187.157.242.248	/1.php
9.	41.93.32.139	/_profiler/phpinfo
10.	186.209.106.84	/form.html

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,557** ICS attacks compared to last week which was **3,545.**

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 11th of August, 2024 to 17th of August, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	172.104.210.244	IEC104	2404
2.	45.33.33.230	kamstrup_protocol	1025
3.	165.22.92.131	kamstrup_management_protocol	50100
4.	209.38.37.211	guardian_ast	10001
5.	146.190.87.141	snmp	161

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.