TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 15th of December, 2024 to 21st of December, 2024
Report No.: TZ-CERT/WRHP/2024/51

1. NETWORK ATTACKS

A total of **907,984** attacks have been recorded compared to last week's **178,153** 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.	178.162.215.169	root	666666
2.	147.45.47.117	admin	root
3.	113.163.216.230	(empty)	admin
4.	69.30.250.163	centos	1234
5.	176.122.18.207	default	password
6.	45.238.64.21	ubuntu	12345
7.	103.130.59.7	guest	[Service]
8.	202.159.60.204	vadmin	1111
9.	146.190.152.73	CUAdmin	P@ssw0rd
10.	186.28.56.169	superadmin	(empty)

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 **59,095** malicious software distributed, compared to last week in which was **178,153**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan Horse	8b19f9f4ebe05047321d306bc3e5485b38fadd28b9dc5a78a522f2c80db7d17c
2.	78.173.47.163	HEUR:Trojan.Linux.Miner.gen	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
3.	41.40.230.140	Trojan:Linux/Hajime!MSR	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	196.179.79.250	Trojan.Gen.NPE	12ec720d3ac0892d4e8dd3981350ac3b9fabc5631814d2c2bc7b441dfc3f96b3
5.	201.211.4.191	Adware/Miner	2b32bfcb42ea3283cf430c918e73730667fb434a4a2713283e63f44ebcadce36
6.	117.4.74.77	DDoS:Linux/Xarcen.A!MTB	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	41.205.148.9	Linux/XorDDos.b	b927f9ff536db3dafbea0ec62c2581b3acc42da18fe6fc932be077e5e9036aaf
8.	202.83.170.133	DoS:Linux/Xorddos!pz	ba76ffe8c2f466442077c70ed874b2459d677cece7d36cc71e2a8542c27f8c2b
9.	41.111.234.98	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
10.	41.99.66.242	Trojan:Linux/CoinMiner	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,155** web attacks compared to last week which was **1,735.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 15th of December, 2024 to 21st of December, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	203.190.10.123	/
2.	162.217.96.21	/admin/config.php
3.	66.249.64.107	/logon.htm
4.	66.249.64.105	/cgi-bin/luci/;stok=/locale
5.	94.156.248.28	/login.rsp
6.	95.214.53.205	/.env

7.	66.249.64.106	/admin/assets/js/views/login.js
8.	185.191.126.213	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	154.213.187.122	/robots.txt
10.	47.237.94.12	/22919811.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,694** ICS attacks compared to last week which was **2,076.**
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 15th of December, 2024 to 21st of December, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	198.235.24.159	IEC104	2404
2.	45.95.147.229	kamstrup_management_protocol	50100
3.	206.168.32.48	guardian_ast	10001
4.	123.58.203.194	kamstrup_protocol	1025
5.	207.90.244.10	snmp	16

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.