TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 8th of December, 2024 to 14th of December, 2024
Report No.: TZ-CERT/WRHP/2024/50

1. NETWORK ATTACKS

A total of **178,153** attacks have been recorded compared to last week's **161,830** 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.	69.30.250.163	root	123456
2.	178.162.215.169	admin	root
3.	147.45.47.117	345gs5662d34	admin
4.	185.107.172.71	proftpd	345gs5662d34
5.	176.122.18.207	default	password
6.	103.130.59.7	user	12345
7.	202.159.60.204	guest	proftpd
8.	142.116.38.248	supervisor	user
9.	45.238.64.21	support	P@ssw0rd
10.	45.33.113.220	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 **178,153** malicious software distributed, compared to last week in which was **102,667.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	178.162.215.169	trojan.shell/bash	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	71.66.180.6	miner.mirai/vsntjm24	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4
3.	176.122.18.207	miner.stlph	992cb5a753697ee2642aa390f09326fcdb7fd59119053d6b1bdd35d47e62f472

4.	45.238.64.21	miner.r002c0dk424/uvzxy	69dc9dd8065692ea262850b617c621e6c1361e9095a90b653b26e3901597f586
5.	149.54.22.132	miner.royos	29f8524562c2436f42019e0fc473bd88584234c57979c7375c1ace3648784e4b
6.	81.16.116.176	ELF/Siggen.689!tr	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
7.	195.178.110.34	trojan.r002c0din24	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
8.	146.190.152.73	trojan.mirai/shell	e77318536a44e8986f54eab60f8dc6e7e569080b0f89edaebfd2ab20cb3ffc78
9.	85.105.35.252	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
10.	202.159.60.204	Trojan:Linux/Multiverze	337ae3a4fe38c75acad6fac00db69046a8da0341524df34431a8b46f90896022

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,735** web attacks compared to last week which was **1,955.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 8th of December, 2024 to 14th of December, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	162.217.96.21	/
2.	141.98.11.35	/admin/config.php
3.	103.152.100.73	/admin/assets/js/views/login.js
4.	77.105.133.212	/.env
5.	95.214.53.205	/admin/config.php?password%5B0%5D=ZIZO&username=admin

6.	45.81.23.28	/favicon.ico
7.	130.162.43.54	/logon.htm
8.	83.143.112.244	/robots.txt
9.	64.23.201.216	/recordings/index.php
10.	185.191.126.248	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,879** 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 8th of December, 2024 to 14th of December, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.120.223	kamstrup_protocol	1025
2.	165.154.41.6	IEC104	2404
3.	13.244.75.167	guardian_ast	10001
4.	161.35.114.100	kamstrup_management_protocol	50100
5.	50.116.21.189	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.