TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 30th of November, 2024 to 7th of December, 2024
Report No.: TZ-CERT/WRHP/2024/49

1. NETWORK ATTACKS

A total of **161,830** attacks have been recorded compared to last week's **141,767** 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	proftpd
3.	147.45.47.117	proftpd	(empty)
4.	185.107.172.71	administrator	admin
5.	176.122.18.207	user	[install]
6.	103.130.59.7	guest	password
7.	202.159.60.204	supervisor	[Service]
8.	142.116.38.248	ftpuser	12345678
9.	45.238.64.21	kafka	1234
10.	45.33.113.220	ubnt	J256

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 **102,667** malicious software distributed, compared to last week in which was **24,799.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan:Linux/Multiverze	12ec720d3ac0892d4e8dd3981350ac3b9fabc5631814d2c2bc7b441dfc3f96b3
2.	80.93.119.11	Trojan:Linux/Multiverze	66ddd92e5d3e803fc3a357a17bf78d43674db8e6916530d24c97accb699a4be5
3.	196.202.26.245	trojan.multiverze/genericrxss	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

4.	196.202.11.188	Linux/CoinMiner.ABF	9f6fa0544c67bd2d3c59f031c2d9ba107312772aaa7852ddb6cb6d9e94bbeb2a
5.	125.166.204.162	trojan.r002c0din24	c671c9bfc3554c4deac3b66fc68719e99a6341bcc3e72d62852874e02983cd83
6.	196.29.194.98	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	196.188.51.241	miner.stlph	992cb5a753697ee2642aa390f09326fcdb7fd59119053d6b1bdd35d47e62f472
8.	41.78.227.2	Trojan:Linux/CoinMiner	69dc9dd8065692ea262850b617c621e6c1361e9095a90b653b26e3901597f586
9.	196.65.251.104	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
10.	41.38.210.152	miner.mirai/vsntjm24	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,613** 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 30th of November, 2024 to 07th of December, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	197.186.1.68	/
2.	105.234.160.24	/admin/config.php
3.	162.217.96.21	/index.php?title=Special:UserLogin&returnto=Main%20Page
4.	95.214.53.211	/login.asp
5.	194.50.16.198	/.env

6.	78.153.140.177	/admin/assets/js/views/login.js
7.	141.98.11.35	/favicon.ico
8.	87.120.116.155	/logon.htm
9.	185.191.126.248	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
10.	66.249.64.105	/robots.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,076** ICS attacks compared to last week which was **1,703.**
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 30th of November, 2024 to 07th of December, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	178.128.78.248	kamstrup_protocol	1025
2.	192.155.89.131	IEC104	2404
3.	35.180.203.18	guardian_ast	10001
4.	217.138.219.220	kamstrup_management_protocol	50100
5.	41.78.65.26	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.