TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 22nd of December, 2024 to 28th of December, 2024
Report No.: TZ-CERT/WRHP/2024/52

1. NETWORK ATTACKS

A total of **420,545** attacks have been recorded compared to last week's **907,984** 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.	77.91.78.95	root	123456
2.	116.193.222.195	admin	root
3.	194.169.175.107	guest	admin
4.	51.79.69.86	proftpd	12345
5.	209.38.21.32	default	password
6.	183.91.160.89	Administrator	1234
7.	62.171.130.190	CUAdin	proftpd
8.	220.132.200.72	suoervisor	(empty)
9.	1.170.96.247	CMCCAdmin	P@ssw0rd
10.	1.34.209.215	ubuntu	345gs5662d34

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 **74,956** malicious software distributed, compared to last week in which was **59,095**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	154.0.30.235	downloader.medusa/shell	ce9a5d9b5c25ecfcde1c946901db42efdfa881de812e2a1cab84b1650b057a7a
2.	41.78.76.190	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	113.176.123.40	Unix.Trojan.Coinminer-10007719-0	0165937bc9d7a0a3572826b2cf7bb2471a61dbe910e25b2799dc3481a8d7eb6e

4.	92.46.48.19	Trojan.Gen.NPE	08cf4792f94eb68bef8f9b7b8746fd1a0349937a54b0b746e442ac8ace57b831
5.	103.242.107.98	trojan.dfaxi/r002c0dkc24	0f6966bada6e20ae6a8631d066252ca1261f2122d064878e6b4c85e4d4a4e183
6.	117.5.127.62	trojan.r002c0di924	1ce5ff9824b3b2f5f1e0adc59eb50de5a5ec461f3b35ad10717ede86825bbdc1
7.	85.113.208.43	trojan.r002c0dkj24	1e968044a1a92b613d1d64fd665658ef361982b450c1d3ab90ccc7822f6025ce
8.	78.165.106.58	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
9.	41.111.234.98	ELF/Xorddos.AB!tr	286c3a9c635a607797fef8bd4cb46ff2816dcd6550d61b2b9c525c1e10f28da3
10.	122.129.85.251	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,150** web attacks compared to last week which was **2,155.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 22nd of December, 2024 to 28th of December, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	193.41.206.24	/
2.	95.214.53.205	/login.rsp
3.	141.98.11.155	/.env
4.	154.213.187.122	/admin/assets/js/views/login.js
5.	185.191.126.213	/logon.htm
6.	72.167.55.229	/favicon.ico

7.	41.78.75.186	/robots.txt
8.	66.249.64.105	/cgi-bin/luci/;stok=/locale
9.	45.81.23.5	/.git/config
10.	102.212.216.147	/_profiler/phpinfo

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,629** ICS attacks compared to last week which was **1,694.**
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 22nd of December, 2024 to 28th of December, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	41.78.65.26	kamstrup_protocol	1025
2.	87.98.236.89	kamstrup_management_protocol	10001
3.	165.154.41.213	IEC104	50100
4.	104.234.115.41	guardian_ast	2404
5.	45.95.147.229	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.