TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 20th of October, 2024 to 26th of October, 2024
Report No.: TZ-CERT/WRHP/2024/43

1. NETWORK ATTACKS

A total of **573,925** attacks have been recorded compared to last week's **920,327** 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.	14.241.236.82	guest	Win1doW$
2.	14.241.236.220	postgres	root
3.	190.85.8.138	Administrator	888888
4.	198.50.254.181	superadmin	password
5.	134.119.214.204	sa	asdASD123@
6.	157.92.160.90	dba	123qwe!@#
7.	104.236.244.113	user	proftpd
8.	185.246.128.133	default	P@ssw0rd
9.	41.78.75.186	telnetadmin	12345
10.	193.105.134.95	ftp	666666

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 **23,697** malicious software distributed, compared to last week in which was **13,147.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.202.71.12	Backdoor:Win32/Berbew	952468f5685c1568b87e77bfd6498df3f95dd0df7ed69180d662605903f00e7f
2.	79.129.1.79	Trojan:Linux/Hajime!MSR	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
3.	169.255.114.114	Mal/Generic-S	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a

4.	101.99.12.248	HEUR:Trojan.Linux.Miner.gen	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
5.	221.4.38.61	Trojan:Linux/Multiverze	00deea7003eef2f30f2c84d1497a42c1f375d802ddd17bde455d5fde2a63631f
6.	218.92.134.23	Adware/Miner	130b71d63afd3eb728ff89a80ab09a23c9f4e6c0c17854c045f196925f4ac8e5
7.	114.4.234.194	Trojan:Linux/CoinMiner	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
8.	110.232.87.79	Trojan:Linux/CoinMiner	7cd48d762a343b483d0ce857e5d2e30fc795d11a20f1827679b9a05d5ab75c3f
9.	191.31.164.9	Not-a-virus:HEUR:RiskTool.Linux.BitCoinMi	c1aad34e379fb2f7658756025dee4c6e3d7abe7ed6b46834d03cec155776dc42
10.	196.202.102.18	Generic Reputation PUA (PUA)	d41149c44b023b6eeaeb03c1e8fb42014092cec84019de6a04c7571f9d71240e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,993** web attacks compared to last week which was **11,486.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th of October to 26th of October, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	162.217.96.21	/
2.	204.101.161.19	/admin/config.php
3.	5.14.176.84	/login.rsp
4.	93.62.144.194	/cgi-bin/luci/;stok=/locale
5.	179.43.191.98	/admin/assets/js/views/login.js
6.	179.43.168.146	/.env

7.	89.117.72.99	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	185.191.126.248	/robots.txt
9.	41.78.75.186	/favicon.ico
10.	41.78.73.146	/command_port.ini

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,867** ICS attacks compared to last week which was **40,950.**

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 20th of October, 2024 to 26th of October, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	137.184.199.54	kamstrup_management_protocol	50100
2.	167.94.146.48	kamstrup_protocol	1025
3.	157.230.59.205	IEC104	2404
4.	45.33.119.146	guardian_ast	10001
5.	45.79.73.75	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.