TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 22nd of September, 2024 to 28th of September, 2024
Report No.: TZ-CERT/WRHP/2024/39

1. NETWORK ATTACKS

A total of **152,659** attacks have been recorded compared to last week's **78,684** 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	root	3245gs5662d34
2.	104.236.244.113	admin	345gs566d34
3.	14.241.236.220	ubuntu	admin
4.	117.4.35.61	test	password
5.	185.246.128.133	user	root
6.	193.105.134.95	support	root
7.	183.81.169.238	stem	P@ssw0rd
8.	41.78.75.186	deploy	123456
9.	129.226.4.248	postgres	12345
10.	193.106.245.20	sysadmin	test

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 **15,214** malicious software distributed, compared to last week in which was **14,087.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.93.57.66	trojan.hajime/mirai	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
2.	181.64.223.79	trojan.hajime/ltfzr	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	88.247.141.235	Trojan.Linux.Generic.355701	0165937bc9d7a0a3572826b2cf7bb2471a61dbe910e25b2799dc3481a8d7eb6e

4.	41.111.220.41	trojan.r002c0dfi24	069446d39b4d564adf965954119a2e1ffc0bddcfa0142c5db428ebc5731dd973
5.	78.163.171.16	trojan.multiverze/r002c0pfa24	12de77bef9500e41c76a2200bc6fa712e7e3fc188dfdd92a764a22c3421b7208
6.	103.255.235.26	trojan.multiverze/r002c0dg224	1c847d3bd3ef4bf7e21a7091f1479e0e2ca432585ebea996653845b9adfb150e
7.	180.254.244.123	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
8.	183.83.54.139	Trojan:Linux/CoinMiner	e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746
9.	116.103.230.14	miner.r06ec0dic24/sfpmb	88a339d0932322a43a5101d7afad05fa3bbcdbabe62cd5e287daa077398fef97
10.	116.212.142.47	miner.r06ec0dic24/zuzhm	42efa318e298e6069af565b5d09f30d38fc15d7ab1f1361addc9288e5a4e4d98

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,087** web attacks compared to last week which was **2,676.**

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

SN	ATTACKING IPS	TOP URI
1.	45.148.10.242	/
2.	185.191.126.213	/logon.htm
3.	149.50.103.48	/admin/assets/js/views/login.js
4.	66.249.64.132	/cgi-bin/luci/;stok=/locale
5.	185.224.128.83	/webpages/login.html
6.	109.89.80.123	/robots.txt

7.	66.249.64.129	/.env
8.	45.190.160.59	/favicon.ico
9.	66.249.64.128	/nice%20ports%2C/Tri%6Eity.txt%2ebak
10.	185.16.39.118	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,557** ICS attacks compared to last week which was **2,500.**

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 September, 2024 to 28th of September, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	197.186.25.118	kamstrup_protocol	1025
2.	94.23.145.155	IEC104	2404
3.	35.233.114.139	kamstrup_management_protocol	50100
4.	152.32.207.179	guardian_ast	10001
5.	147.182.241.81	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.