TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 8th of September, 2024 to 14th of September, 2024
Report No.: TZ-CERT/WRHP/2024/37

1. NETWORK ATTACKS

A total of **75,578** attacks have been recorded compared to last week's **140,252** 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.	104.236.244.113	root	admin
2.	62.12.114.109	admin	1234
3.	167.99.198.183	guest	123456
4.	185.246.128.133	ubnt	(empty)
5.	193.105.134.95	support	password
6.	41.78.75.186	postgres	root
7.	193.32.162.79	supervisor	54321
8.	183.81.169.238	3comcso	1234admin
9.	209.38.16.137	user	12345
10.	186.96.145.241	oracle	Win1doW$

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 **21,203** malicious software distributed, compared to last week in which was **25,945.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	45.189.56.11	HEUR:Trojan.Linux.Miner.gen	168c689463606a3a6444767e445ffbfda5559926b684526f6d0b59d8be224a05
2.	112.27.178.171	Trojan.Linux.GenericKD.21294	87b1421c4c09aaec626ac12b4763c1dbff5d667ec3ea87d9982d5fe5fde0feaf
3.	14.98.190.250	Trojan.Linux.Generic.355701	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

4.	45.148.10.242	Trojan.Linux.Generic.355701	9f892306ebe85654e7cccbbc5b7bcd11be8553576001251e0d3fd32b86c3bc4f
5.	190.221.56.220	Trojan.Linux.Generic.355701	cfd7ad5fd929fbdef0af698ee1f7f1624ed46109a50125f7ab39b14bd84dfcac
6.	171.7.114.76	Trojan.GenericKD.74003008 (B)	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	102.182.51.128	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	141.255.160.234	HEUR:Trojan-DDoS.Linux.Xorddos.gen	2303e3dc2f0d3723dfb90b557ad4b36c3d98efde2cc8f29b091d8144986dc861
9.	115.75.74.230	Trojan:Linux/CoinMiner	e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746
10.	221.207.184.120	Trojan:Linux/CoinMiner	88a339d0932322a43a5101d7afad05fa3bbcdbabe62cd5e287daa077398fef97

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,676** web attacks compared to last week which was **2,850.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 8th of September, 2024 to 14th 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	/cgi-bin/luci/;stok=/locale
4.	78.153.140.151	/admin/assets/js/views/login.js
5.	185.224.128.47	/.env
6.	41.78.75.186	/favicon.ico

7.	66.249.64.128	/robots.txt
8.	66.249.64.132	/nice%20ports%2C/Tri%6Eity.txt%2ebak
9.	66.249.64.129	/actuator/gateway/routes
10.	45.190.160.59	/static/css/633.030ebb42.chunk.css

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,488** ICS attacks compared to last week which was **1,463.**

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 8th of September, 2024 to 14th of September, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	94.23.145.155	IEC104	2404
2.	13.244.75.167	guardian_ast	10001
3.	207.90.244.17	kamstrup_management_protocol	50100
4.	164.92.106.15	kamstrup_protocol	1025
5.	159.89.124.112	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.