TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 1st of September, 2024 to 7th of September, 2024
Report No.: TZ-CERT/WRHP/2024/37

1. NETWORK ATTACKS

A total of **140,252** attacks have been recorded compared to last week's **1,297,294** 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.	14.161.253.60	root	123123123
2.	117.247.227.45	guest	admin
3.	62.12.114.109	admin	ABCabc123
4.	167.99.198.183	test	root
5.	104.236.244.113	ftpuser	Win1doW$
6.	193.105.134.95	oracle	qwertyuiop123
7.	212.80.7.238	cameras	password
8.	185.246.128.133	sysadmin	Abc!@#123
9.	41.78.75.186	oracle	cameras
10.	113.13.221.71	sa	1234qwer

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 **25,945** malicious software distributed, compared to last week in which was **58,892.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.189.255.252	Trojan Horse	168c689463606a3a6444767e445ffbfda5559926b684526f6d0b59d8be224a05
2.	196.224.230.190	Trojan.Gen.NPE	1fdd1176933a786be5aec4814c143f4a192a32284a015bf3a28d96e6df66a3d9
3.	95.181.238.98	Trojan.Gen.NPE	47b268c21591069bfe4099833ad66b8138a53ab2dcb866e040d466aee1f8624c

4.	190.90.6.22	Trojan:Linux/Multiverze	86853a0c9272afe15734577c5a7a14a5f98632b89aa986945e3bed3aa0c39b72
5.	190.221.56.220	Trojan.Gen.NPE	87b1421c4c09aaec626ac12b4763c1dbff5d667ec3ea87d9982d5fe5fde0feaf
6.	181.124.23.52	Trojan.GenericKD.74003008 (B)	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	45.189.56.11	CL.Downloader!gen277	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	14.98.190.250	Trojan.Gen.NPE	e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746
9.	103.89.234.5	CL.Downloader!gen277	88a339d0932322a43a5101d7afad05fa3bbcdbabe62cd5e287daa077398fef97
10.	93.51.213.106	Backdoor.Berbew.F	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,850** web attacks compared to last week which was **4,396.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 1st of September, 2024 to 7th of September, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	45.148.10.242	/
2.	45.148.10.251	/logon.htm
3.	45.148.10.247	/cgi-bin/luci/;stok=/locale
4.	185.191.126.213	/admin/assets/js/views/login.js
5.	149.50.103.48	/.env
6.	66.249.64.132	/robots.txt

7.	179.43.133.242	/favicon.ico
8.	66.249.64.128	/solr/admin/cores?action=STATUS&wt=json
9.	41.78.75.186	/cgi-bin/authLogin.cgi
10.	66.249.64.129	/v2/_catalog

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,463** ICS attacks compared to last week which was **2,843.**

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 1st of September, 2024 to 7th of September, 2024, are detailed

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