TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 15th of September, 2024 to 21st of September, 2024
Report No.: TZ-CERT/WRHP/2024/38

1. NETWORK ATTACKS

A total of **78,684** attacks have been recorded compared to last week's **75,578** 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.	185.246.128.133	sysadmin	12345
3.	193.105.134.95	guest	P@ssw0rd
4.	183.81.169.238	centos	(empty)
5.	41.78.75.186	support	password
6.	209.38.17.7	postgres	root
7.	170.64.220.227	username	54321
8.	193.32.162.83	testuser	qwer1234
9.	206.189.179.86	user	ubuntu@2024
10.	212.60.80.58	supervisor	test@123

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 **14,087** malicious software distributed, compared to last week in which was **21,203.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.202.15.15	Trojan.Gen.NPE	20e3f957446527a31ff3fd9d53b48c6046c9858d789ca043a6869cbea254bc20
2.	187.202.22.57	Mal/Generic-S	306f0c79ad9ee76e996556f909306fda5704b456d670aa9daeb54760b4b5e4f6
3.	187.1.181.250	Trojan.Gen.NPE	765289f938cc2bd64c9778dbabe048afa8ac3277a150c940d2730c14d24687b5

4.	13.245.17.35	Trojan.Linux.Generic.355701	9f1c64524e7139b93dea1fa48edb73098fe84ff1a32d93a548a09042c2a03ac7
5.	45.148.10.242	Trojan.Linux.Generic.355701	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	94.23.145.155	Adware/Miner	42efa318e298e6069af565b5d09f30d38fc15d7ab1f1361addc9288e5a4e4d98
7.	115.206.247.122	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	35.233.114.139	HEUR:Trojan-DDoS.Linux.Xorddos.gen	2303e3dc2f0d3723dfb90b557ad4b36c3d98efde2cc8f29b091d8144986dc861
9.	197.186.25.118	Trojan:Linux/CoinMiner	e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746
10.	13.244.75.167	Trojan:Linux/CoinMiner	88a339d0932322a43a5101d7afad05fa3bbcdbabe62cd5e287daa077398fef97

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **5,803** 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 15th of September to 21st of September, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	13.245.17.35	/
2.	217.15.163.40	/logon.htm
3.	45.148.10.242	/admin/assets/js/views/login.js
4.	196.249.100.116	/cgi-bin/luci/;stok=/locale
5.	185.191.126.213	/.env
6.	149.50.103.48	/robots.txt

7.	89.248.171.23	/favicon.ico
8.	197.186.25.118	/nice%20ports%2C/Tri%6Eity.txt%2ebak
9.	66.249.64.132	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
10.	66.249.64.128	/HNAP1

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,500** 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.	197.186.25.118	IEC104	2404
2.	94.23.145.155	guardian_ast	10001
3.	35.233.114.139	kamstrup_management_protocol	50100
4.	152.32.207.179	kamstrup_protocol	1025
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.