TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 13th of October, 2024 to 19th of October, 2024
Report No.: TZ-CERT/WRHP/2024/42

1. NETWORK ATTACKS

A total of **920,327**attacks have been recorded compared to last week's **198,299** 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.	14.241.236.220	root	(empty)
2.	14.241.236.82	admin	toor
3.	198.50.254.181	support	888888
4.	104.236.244.113	superman	password
5.	157.92.160.90	sysadmin	1234admin
6.	190.85.8.138	supervisor	3245gs5662d34
7.	193.105.134.95	user	345gs5662d34
8.	185.246.128.133	enable	P@ssw0rd
9.	117.4.35.61	oracle	12345
10.	41.78.75.186	ubuntu	0000

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 **13,147** malicious software distributed, compared to last week in which was **7,437.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.202.102.18	Backdoor:Win32/Berbew	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
2.	180.245.206.151	Trojan.Linux.Generic.355701	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
3.	117.0.167.126	Trojan.Linux.Generic.355701	12de77bef9500e41c76a2200bc6fa712e7e3fc188dfdd92a764a22c3421b7208

4.	35.180.229.8	Trojan.Linux.Generic.355701	77ccd5ae0a102102b1c2032ff7f1fa8cc2f1069276f964210e644e1b21d8dd1f
5.	113.203.203.229	Trojan:Linux/Multiverze	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
6.	47.93.143.177	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	103.142.210.48	Trojan:Linux/CoinMiner	e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746
8.	112.74.87.57	Trojan:Linux/CoinMiner	7cd48d762a343b483d0ce857e5d2e30fc795d11a20f1827679b9a05d5ab75c3f
9.	116.98.2.23	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 **11,486** web attacks compared to last week which was **2,261.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 13th of October to 19th of October, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	35.180.229.8	/
2.	162.217.96.21	/admin/config.php
3.	93.62.144.194	/admin/assets/js/views/login.js
4.	183.207.45.103	/.env
5.	66.249.64.132	/cgi-bin/luci/;stok=/locale
6.	66.249.64.128	/admin/config.php?password%5B0%5D=ZIZO&userna

		me=admin
7.	66.249.64.129	/login.rsp
8.	41.78.75.186	/command_port.ini
9.	179.43.191.98	/robots.txt
10.	185.224.128.83	/favicon.ico

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **40,950** ICS attacks compared to last week which was **2,059.**

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 13th of October, 2024 to 19th of October, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	196.49.5.50	tls	43
2.	41.78.64.60	ssh	80
3.	160.44.201.156	http	22
4.	35.180.229.8	rdp	993
5.	45.148.10.81	gquic	33

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.