TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 6th of October, 2024 to 12th of October, 2024
Report No.: TZ-CERT/WRHP/2024/41

1. NETWORK ATTACKS

A total of **198,299** attacks have been recorded compared to last week's **320,370** 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	pass
2.	198.50.254.181	admin	cameras
3.	157.92.160.90	support	Win1doW$
4.	14.241.236.82	sa	password
5.	104.236.244.113	ftp	1234admin
6.	185.246.128.133	cameras	666666
7.	193.105.134.95	user	qwertyuiop123
8.	41.78.75.186	admin	P@ssw0rd
9.	193.32.162.38	oracle	12345
10.	183.81.169.238	guest	1234567890

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 **7,437** malicious software distributed, compared to last week in which was **62,427.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.219.181.107	trojan.multiverze/r002c0pfa24	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
2.	187.235.168.129	Trojan:Linux/Multiverze	12ea9ed292055b13e0c4a832c7d2ad583e8f25b7dc0b34d9437593ceb02562f9
3.	101.255.21.75	ELF:Miner-KI [Trj]	17b7944a9b8a4e3edb1b1f2e743ae5d06dae0a8c3a9531e94970aa3261c2cab5

4.	196.202.8.105	Trojan.Linux.GenericKD.7949	38ef0580d99fb1524c13f8dc4981fe2757deb290b29f947ebc24b4b359756f63
5.	118.68.105.145	Not-a-virus:HEUR:RiskTool.Linux.BitCoinMiner.n	629db57b96d6e965401d866f895d86c542efe344b3d489630a6ec09d643add76
6.	35.180.203.18	trojan.multiverze/r002c0dg224	67db999e9ab18659c1d595c9112ac9b22065cf05328c156585bda8589d10cb70
7.	34.38.220.243	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
8.	41.226.172.112	Trojan:Linux/CoinMiner	c1aad34e379fb2f7658756025dee4c6e3d7abe7ed6b46834d03cec155776dc42
9.	171.7.40.120	Trojan.Gen.NPE	e86081329173be1acc1486a47cee17c9c7b78c50928e7bb9e05a86f1c040a746
10.	196.202.71.139	Generic Reputation PUA (PUA)	88a339d0932322a43a5101d7afad05fa3bbcdbabe62cd5e287daa077398fef97

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,261** web attacks compared to last week which was **3,503.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 6th of October to 12th of October, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	141.98.11.79	/
2.	162.217.96.21	/logon.htm
3.	141.98.11.15	/admin/config.php
4.	149.50.103.48	/cgi-bin/luci/;stok=/locale
5.	185.191.126.213	/admin/assets/js/views/login.js
6.	41.78.75.186	/admin/config.phhp?password%5B0%5D=ZIZO&usern

		ame=admin
7.	66.249.64.128	/.env
8.	66.249.64.129	/favicon.ico
9.	78.153.140.179	/a2billing/admin/Public/index.php
10.	58.52.200.53	/recordings/index.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,059** ICS attacks compared to last week which was **2,223.**

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 6th of October, 2024 to 12th of October, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	123.58.213.20	kamstrup_management_protocol	50100
2.	89.190.156.56	kamstrup_protocol	1025
3.	34.38.220.243	IEC104	2404
4.	35.180.203.18	guardian_ast	10001
5.	94.23.145.155	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.