TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 24th of November, 2024 to 30th of November, 2024
Report No.: TZ-CERT/WRHP/2024/48

1. NETWORK ATTACKS

A total of **141,767** attacks have been recorded compared to last week's **158,632** 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.	69.30.250.163	root	admin
2.	178.162.215.169	admin	!@#%^&*
3.	147.45.47.117	websrvc	proftpd
4.	185.107.172.71	proftpd	123456
5.	176.122.18.207	test	Win1doW$
6.	103.130.59.7	support	1234qwer
7.	202.159.60.204	debian	system
8.	142.116.38.248	oracle	Password
9.	45.238.64.21	ftpuser	anonymous@
10.	45.33.113.220	ubuntu	(empty)

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 **24,799** malicious software distributed, compared to last week in which was **7,715.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	trojan.shell/bash	337ae3a4fe38c75acad6fac00db69046a8da0341524df34431a8b46f90896022
2.	156.195.196.63	HEUR:Trojan-Downloader.Shell.Agent.bc	be8cbe4f4bfcc27f366d09382cff27ebf1d08c250a90144cf272d854c3beee2f
3.	175.176.23.54	trojan.mirai/shell	e77318536a44e8986f54eab60f8dc6e7e569080b0f89edaebfd2ab20cb3ffc78

4.	196.219.125.58	ELF/Siggen.689!tr	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	41.78.227.2	trojan.r002c0din24	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
6.	36.157.245.74	trojan.multiverze/r002c0djg24	aa85190274311673a61039d434c6b30a0f694ce645a0340f0c11424d0eff8f87
7.	223.83.184.169	Trojan.Linux.GenericKD.7949	b14212857fe74349571dc653447dd59ff5938a768a65f90a3d4d653b669f8c83
8.	27.220.110.16	trojan.r002c0dj624	e150fc20ddf1f2169ab6011ee4af4103d94f80046e64c2c99b2e60f80055724b
9.	49.146.226.104	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
10.	197.207.76.210	miner.mirai/vsntjm24	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,955** web attacks compared to last week which was **3,182.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 24th of November, 2024 to 30th of November, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	162.217.96.21	/
2.	194.50.16.198	/admin/config.php
3.	179.43.163.250	/cgi-bin/luci/;stok=/locale
4.	78.153.140.223	/admin/assets/js/views/login.js
5.	141.98.11.48	/.env
6.	64.23.201.216	/admin/config.php?password%5B0%5D=ZIZO&userna

		me=admin
7.	144.126.159.131	/favicon.ico
8.	47.84.69.78	/robots.txt
9.	41.78.73.146	/logon.htm
10.	78.153.140.224	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,703** ICS attacks compared to last week which was **1,830.**
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 24th of November, 2024 to 30th of November, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	24.199.95.110	IEC104	404
2.	66.228.62.17	guardian_ast	10001
3.	141.98.7.248	kamstrup_management_protocol	50100
4.	13.58.97.162	kamstrup_protocol	1025
5.	164.92.114.247	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.