TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 26th of January to 1st of February, 2025
Report No.: TZ-CERT/WRHP/2025/05

1. NETWORK ATTACKS

A total of **460,745** attacks have been recorded compared to last week's **662,113** 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.	176.120.74.223	root	Win1doW$
2.	103.170.179.158	admin	r00t
3.	45.249.8.86	postgres	123qwe!@#
4.	5.161.181.1	deploy	abc123456
5.	131.161.22.242	debian	admin
6.	122.116.127.90	telnet	telnetadmin
7.	114.32.150.104	sa	!@#$%^&*
8.	138.68.160.61	ubuntu	P@ssw0rd
9.	125.229.189.58	cron	(empty)
10.	1.34.253.238	oracle	1q2w3e4r

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 **72,643** malicious software distributed, compared to last week in which was **74,363.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan:Linux/Multiverze	043675aa01acc869a78590befba137ba77e45a7509926739f7d13b75042d4119
2.	178.81.29.238	Trojan.Gen.NPE	05107cd7d97c5735f95cf0460ce1da2db4631abbc167c0b21842949bdca6651c
3.	181.189.154.93	HEUR:Trojan.Linux.Miner.gen	217a3a1d4bb89fc2df78d0d20f1b42bcf2289fcba7ac5d0fef898b0f57d70c48

4.	190.95.96.94	Mal/Generic-S	306f0c79ad9ee76e996556f909306fda5704b456d670aa9daeb54760b4b5e4f6
5.	196.202.80.128	Trojan:Linux/Multiverze	3474e95e102353c50c7bc0241a8e9ed6a17fa9eba072a24628c4cbb08b8ff64b
6.	41.226.160.42	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	171.229.10.152	ELF/Xorddos.AB!tr	33a6ae6e6b8f2062a7a79fb7e0f4083e3e4fd07752890611c1e8c8f1a091b857
8.	41.111.198.172	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
9.	203.146.249.79	Trojan:Linux/CoinMiner	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4
10.	41.139.147.225	Backdoor:Linux/Mirai!rfn	992cb5a753697ee2642aa390f09326fcdb7fd59119053d6b1bdd35d47e62f472

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,312** web attacks compared to last week which was **1,962.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th of January to 1st of February, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	167.99.52.233	/
2.	162.217.96.20	/admin/config.php
3.	164.92.71.220	/.env
4.	54.162.184.235	/admin/config.php?password%5B0%5D=ZIZO&username=admin
5.	146.19.24.168	/favicon.ico

6.	193.41.206.98	/.well-known/security.txt
7.	195.3.223.55	/admin/assets/js/views/login.js
8.	185.196.220.253	/robots.txt
9.	41.78.75.186	/a2billing/admin/Public/index.php
10.	109.244.96.94	/libs/js/iframe.js

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,112** ICS attacks compared to last week which was **3,071.**

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 26th of January to 1st of February, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	152.32.170.230	kamstrup_protocol	1025
2.	137.184.13.100	IEC104	2404
3.	207.90.244.13	kamstrup_management_protocol	50100
4.	147.182.225.86	guardian_ast	10001
5.	164.92.106.15	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.