TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 12th of January, 2025 to 18th of January, 2025
Report No.: TZ-CERT/WRHP/2025/03

1. NETWORK ATTACKS

A total of **416,474** attacks have been recorded compared to last week's **216,594** 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.	45.7.234.101	root	Win1doW$
2.	103.170.179.158	admin	r00t
3.	61.76.136.25	hadoop	123qwe!@#
4.	45.79.24.65	proftpd	abc123456
5.	218.92.0.179	ftpuser	admin
6.	49.213.232.247	guest	proftpd
7.	220.132.17.49	sa	3245gs5662d34
8.	211.23.95.130	ubuntu	P@ssw0rd
9.	220.133.23.52	user	1qaz2wsx
10.	220.133.58.167	oracle	(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 **78,062** malicious software distributed, compared to last week in which was **54,825.**

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	02ba9b3ee805baa59b6d9a2a5ae689040565877b5c996bfe4002c95cbfdcc13e
2.	114.27.158.133	Trojan.Gen.NPE	0bf15aa87b7edf963533962273cd9c622b74dd1e47e770aa910fdf22ce0851df
3.	196.203.192.145	HEUR:Trojan.Linux.Miner.gen	12de77bef9500e41c76a2200bc6fa712e7e3fc188dfdd92a764a22c3421b7208

4.	116.99.253.11	Mal/Generic-S	5d9d3c86055f6f72bf0c9a862a186d4d3a5b4103db4f6a4099306058058d2390
5.	203.202.248.77	Trojan:Linux/Multiverze	629db57b96d6e965401d866f895d86c542efe344b3d489630a6ec09d643add76
6.	41.38.14.52	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	196.221.217.159	ELF/Xorddos.AB!tr	03dbf5ef3046a32f095b9ed6037a02c3b8421bdaf8d45cbe9b83e019e89ef2b7
8.	62.33.34.131	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
9.	105.33.209.168	Trojan:Linux/CoinMiner	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4
10.	41.203.215.119	Backdoor:Linux/Mirai!rfn	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,784** web attacks compared to last week which was **1,636.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 12th of January, 2025 to 18th of January, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	95.214.55.226	/
2.	154.12.254.8	/admin/assets/js/views/login.js
3.	41.78.75.186	/.env
4.	46.19.138.234	/robots.txt
5.	103.226.248.206	/favicon.ico
6.	122.138.218.254	/logon.htm

7.	41.78.73.146	/admin/config.php
8.	58.242.157.86	/cgi-bin/luci/;stok=/locale?form=country&operation=read
9.	41.78.74.39	/sitemap.xml
10.	193.34.212.75	/.well-known/security.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,739** ICS attacks compared to last week which was **1,667.**

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 12th of January, 2025 to 18th of January, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	118.193.64.15	kamstrup_protocol	1025
2.	137.184.13.100	IEC104	2404
3.	147.182.225.86	kamstrup_management_protocol	50100
4.	147.182.202.179	guardian_ast	10001
5.	35.180.203.18	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.