TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 5th of January, 2025 to 11th of January, 2025
Report No.: TZ-CERT/WRHP/2025/02

1. NETWORK ATTACKS

A total of **216,594** attacks have been recorded compared to last week's **381,477** 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	123456
2.	220.134.21.67	admin	123
3.	36.233.75.18	user	1234
4.	122.116.127.90	proftpd	password
5.	122.117.121.70	ttest	admin
6.	125.229.202.174	guest	proftpd
7.	125.230.206.219	vadmin	3245gs5662d34
8.	218.161.83.188	default	P@ssw0rd
9.	118.161.12.16	user	password
10.	77.91.78.95	Administrator	(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 **54,825** malicious software distributed, compared to last week in which was **49,352.**

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	2497ed422b8667ae58fe7fa22acf5761632e433d48504e5083c8b7c95d3420ff
2.	196.151.251.185	Unix.Trojan.Coinminer-10007719-0	2a71b0288b8b899dfb29e57a35cda39410fa5877e65f0e801f388d10f48eadbe
3.	125.160.83.51	HEUR:Trojan.Linux.Miner.gen	3625cfdcd6d434bfa672753ef4b197df8a01388d220bafc9edfa2d0d29c7fcef

4.	196.202.69.4	Unix.Trojan.Coinminer-10007719-0	38ad8fb3bcf873fbe353c552581478884275e801cdd55a3fab81c257c109a28a
5.	196.64.223.202	Trojan:Linux/Multiverz	6189bc78c2cce9b690f17057199410ee91e9827a93a4a33242843bac5b0f9b8e
6.	41.33.190.125	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	41.78.227.2	ELF/Xorddos.AB!tr	03dbf5ef3046a32f095b9ed6037a02c3b8421bdaf8d45cbe9b83e019e89ef2b7
8.	41.33.82.171	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
9.	185.210.157.128	miner.vsntjm24/ysgud	d4635f0f5ab84af5e5194453dbf60eaebf6ec47d3675cb5044e5746fb48bd4b4
10.	41.203.215.119	miner.stlph	992cb5a753697ee2642aa390f09326fcdb7fd59119053d6b1bdd35d47e62f472

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,636** web attacks compared to last week which was **1,875.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 5th of January, 2025 to 11th 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	/admin/assets/js/views/login.js
3.	156.146.36.105	/logon.htm
4.	195.3.223.55	/favicon.ico
5.	154.213.187.122	/robots.txt
6.	141.98.11.119	/.env

7.	103.226.248.206	/cgi-bin/luci/;stok=/locale
8.	193.233.85.23	/.well-known/security.txt
9.	179.43.191.146	/login.rsp
10.	46.19.138.234	/sitemap.xml

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,667** ICS attacks compared to last week which was **2,277.**

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 5th of January, 2025 to 11th of January, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.162.212	kamstrup_protocol	1025
2.	35.180.129.176	IEC104	2404
3.	45.95.147.229	kamstrup_management_protocol	50100
4.	137.184.13.100	guardian_ast	10001
5.	87.98.236.89	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.