TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 9th of February to 15th of February, 2025
Report No.: TZ-CERT/WRHP/2025/07

1. NETWORK ATTACKS

A total of **235,422** attacks have been recorded compared to last week's **225,073** 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.	103.80.117.250	root	123456
2.	131.161.22.242	admin	3245gs5662d34
3.	45.249.8.86	ftuser	1234
4.	5.161.181.1	ubuntu	345gs5662d34
5.	62.171.130.190	server	password
6.	87.98.138.86	debian	Password123!
7.	183.17.230.129	guest	Welcom1
8.	194.0.234.107	user	password
9.	193.105.134.95	345gs5662d34	Welcome123
10.	217.145.79.31	ubnt	root

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 **118,637** malicious software distributed, compared to last week in which was **67,338.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	BASH/Dloader.AAN!tr.dldr	0fd1c384f4f0aaffadd55c41df59a8a559d5faf6ba5eb579cf15d4061f747b9e
2.	122.186.89.30	Trojan:Linux/Multiverze	e15c0783d47589d3a6397311e01af84b87ce78caade6b74baadd4e694cbb2987
3.	196.219.51.130	trojan.multiverze/vsntch24	38ef0580d99fb1524c13f8dc4981fe2757deb290b29f947ebc24b4b359756f63

4.	113.193.214.2	trojan.r002c0dlc24	3bd6d39e64db5e30b9ff6f713248c435cfa6eba7018a3887e5c4400daa04e4aa
5.	185.153.240.151	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	200.75.2.138	trojan.xorddos/ddos	75d031e8faaf3aa0e9cafd5ef0fd7de1a2a80aaa245a9e92bae6433a17f48385
7.	92.154.116.76	ELF/Xorddos.AB!tr	33a6ae6e6b8f2062a7a79fb7e0f4083e3e4fd07752890611c1e8c8f1a091b857
8.	196.202.81.204	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
9.	196.202.91.164	miner.qwxqh/r002c0dbf25	bf88cfc04ac852d82482ab5f57f03709b9db2cf8f25cf4bfa01945ececae2658
10.	103.224.32.105	trojan.fcrcu/r002c0dbf25	88a77aa2602caf98288c7dbcc056394cd3929e6f4ffbc9b83b6e278ea6632c6d

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **5,934** web attacks compared to last week which was **2,358.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 9th of February to 15th of February, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	193.41.206.202	/
2.	170.39.218.109	/admin/config.php
3.	162.217.96.20	/.env
4.	159.203.77.97	/favicon.ico
5.	165.232.186.170	/robots.txt
6.	193.41.206.176	/admin/config.php?password%5B0%5D=ZIZO&userna

		me=admin
7.	83.164.176.174	/_profiler/phpinfo
8.	193.68.89.10	/config/application.yml
9.	45.148.10.90	/admin/assets/js/views/login.js
10.	71.65.113.18	/a2billing/admin/Public/index.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,354** ICS attacks compared to last week which was **2,124.**

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 9th of February to 15th of February, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	138.197.220.168	IEC104	1025
2.	64.227.13.119	kamstrup_protocol	2404
3.	209.97.141.247	guardian_ast	50100
4.	137.184.13.100	kamstrup_management_protocol	10001
5.	194.195.209.117	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.