TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 6th of July to 12th of July, 2025
Report No.: TZ-CERT/WRHP/2025/27

1. NETWORK ATTACKS

A total of **231,522** attacks have been recorded compared to last week's **102,131** 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.	103.156.74.23	root	345gs5662d34
2.	149.28.62.29	admin	3245gs5662d34
3.	141.98.10.162	345gs5662d34	admin
4.	207.167.66.226	(empty)	123456
5.	45.144.29.201	ubuntu	(empty)
6.	185.246.128.133	ts3server	P@ssw0rd
7.	196.251.88.103	odoo15	1234
8.	173.231.185.164	ec2-user	1qaz@WSX
9.	45.14.245.67	jose	sftp_user@123
10.	193.105.134.95	jenkis	changeme

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 **120,626** malicious software distributed, compared to last week in which was **91,576.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	BASH/Mirai.AEH!tr.dldr	0534c5c6d40ecb7b01e6e3844ffdd350cdc374cc8f0b265fe7b524f83c4a62a3
2.	43.230.206.43	HEUR:Trojan-Downloader.Shell.Agent.p	d9c5bd8dc94485e3d286637b6b97d54a4225cf23a7f2f59a4c6c92e47d16acf4
3.	41.73.214.34	miner.jlerq/r002c0dg625	0d58ee0cd46d5908f31ba415f2e006c1bb0215b0ecdc27dd2b3afa74799e17bd

4.	78.186.250.110	miner.jkrjs/r002c0dg125	1bffd7c3966df6d50a91f5b181ba6bb68d0eeff2fc9c7fbb004d74e429999af3
5.	88.250.61.211	Trojan:Linux/CoinMiner.C12	306c4e975edd4a95ae67c669cac871c233a5a7dd6591afa963b79304decc45ed
6.	196.202.92.67	trojan.multiverze/shell	3b15778595cef00d1a51035dd4fd65e6be97e73544cb1899f40aec4aaa0445ae
7.	41.72.210.222	HackTool.XMRMiner!1.FD0F (CLOUD)	801997d5e5967ab874a94ca04e10900e49e6209f1e2fafa7cc95ad67955f8d23
8.	190.120.249.134	Miner:Multi/XmrigGo.SY	306c4e975edd4a95ae67c669cac871c233a5a7dd6591afa963b79304decc45ed
9.	196.221.149.13	downloader.medusa/bash	d9c5bd8dc94485e3d286637b6b97d54a4225cf23a7f2f59a4c6c92e47d16acf4
10.	41.33.34.161	Generic.Linux.Medusa.C.F19D4DF2	d62938e2923e66e52c17e539fbad85e72472229d2575166361c0314d79f03ee0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,975** web attacks compared to last week which was **3,309.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 6th of July to 12th of July, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.185.164	/
2.	159.223.75.62	/admin/config.php
3.	185.177.72.202	/.env
4.	204.76.203.206	/logon.htm
5.	152.42.208.187	/favicon.ico
6.	213.136.84.241	/robots.txt

7.	89.42.231.140	/config.php
8.	141.98.11.152	/.git/config
9.	45.194.66.7	/admin/config.php?password%5B0%5D=ZIZO&username=admin
10.	185.218.84.46	/cgi-bin/luci/;stok=/locale

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,876** ICS attacks compared to last week which was **1,831.**

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 6th of July to 12th of July, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	142.93.246.40	kamstrup_protocol	1025
2.	157.230.8.8	IEC104	2404
3.	13.38.26.129	guardian_ast	10001
4.	3.132.23.201	kamstrup_management_protocol	50100
5.	3.130.96.91	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.