TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 15th of June to 21st of June, 2025
Report No.: TZ-CERT/WRHP/2025/24

1. NETWORK ATTACKS

A total of **560,506** attacks have been recorded compared to last week's **100,905** 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.	186.80.45.95	root	123456
2.	181.50.203.88	admin	P@ssw0rd
3.	103.156.74.23	ubuntu	admin
4.	157.230.51.19	user	password
5.	95.182.115.26	oscar	1234
6.	31.3.17.148	(empty)	root
7.	45.144.29.201	hadoop	broadguam1
8.	185.246.128.133	jenkis	ubnt
9.	45.14.245.67	dev	adminHW
10.	193.105.134.95	oracle	Win1doW$

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 **7,412** malicious software distributed, compared to last week in which was **51,655.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	136.144.35.212	downloader.medusa/mirai	16174ef4d82f50ebc62b573c05f71b9db34660b456b9558ef9be06201bfda080
2.	41.78.76.190	Trojan:Script/Multiverze!rfn	16174ef4d82f50ebc62b573c05f71b9db34660b456b9558ef9be06201bfda080
3.	43.230.206.43	BASH/Mirai.AEH!tr.dldr	d9c5bd8dc94485e3d286637b6b97d54a4225cf23a7f2f59a4c6c92e47d16acf4

4.	196.202.1.216	HEUR:Trojan.Linux.Miner.gen	0670da04a700a5e7ec0ca80de285d75985116b669dc02c61cebfc22b5b3edab3
5.	123.176.34.84	trojan.multiverze/genericrxss	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
6.	176.208.33.247	trojan.vsntda24	e3736bd6b87f2cd3a704c19033f904b861e7c720920ced10c16699d0ed01d819
7.	119.92.135.124	HEUR:Trojan.Linux.Miner.gen	40cb80b65c3f0dc8cfa6eaae51a475f79f0b8bf9a1406e3a5eed6b46f6c35a65
8.	41.38.97.177	HEUR:Trojan.Linux.Miner.gen	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c
9.	220.134.145.239	E64/ABMiner.DBNS-21	4578139f892a90ae1e0163e6db400e511170ee81549f8cdd7848da8f74e3f4e5
10.	89.22.175.142	trojan.multiverze/genericrxss	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,278** web attacks compared to last week which was **2,815.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 15th of June to 21st of June, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.185.164	/
2.	23.94.27.122	/admin/config.php
3.	185.218.84.178	/.env
4.	204.76.203.212	/favicon.ico
5.	204.76.203.219	/robots.txt
6.	35.180.79.191	/.git/config

7.	204.76.203.206	/upl.php
8.	5.183.209.244	/1.php
9.	41.242.48.18	/form.html
10.	78.153.140.179	/geoip/

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,727** ICS attacks compared to last week which was **2,207.**

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 15th of June to 21st of June, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	41.59.65.202	kamstrup_protocol	1025
2.	3.131.215.38	guardian_ast	10001
3.	165.154.206.250	IEC104	2404
4.	3.130.96.91	snmp	161
5.	24.199.83.224	kamstrup_management_protocol	50100

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.