TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 08th of June to 14th of June, 2025
Report No.: TZ-CERT/WRHP/2025/23

1. NETWORK ATTACKS

A total of **100,905** attacks have been recorded compared to last week's **110,261** 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	345gs5662d34	root
4.	157.230.51.19	guest	admin
5.	95.182.115.26	user	password
6.	31.3.17.148	test	adminHW
7.	45.144.29.201	jenkins	1234
8.	185.246.128.133	e8ehomeasb	345gs5662d34
9.	45.14.245.67	hadoop	broadguam1
10.	193.105.134.95	(empty)	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 **51,655** malicious software distributed, compared to last week in which was **52,209.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	136.144.35.212	BASH/Mirai.AEH!tr.dldr	d9c5bd8dc94485e3d286637b6b97d54a4225cf23a7f2f59a4c6c92e47d16acf4
2.	41.78.76.190	downloader.medusa/bash	02595a4edb6df490bf23b37dfbe425019b84eae9b27639a76058d8fc1aed0aea
3.	196.202.1.216	HEUR:Trojan.Linux.Miner.gen	12097f9321ae6226dc089829d626fb9df46f34a8ba941988d1fd5f6c89d2d125

4.	123.176.34.84	Unix.Trojan.Coinminer-10007719-0	8accc4d8494bcca13f8de9772eea26f75a759f2815696bafd63a605c507de75c
5.	196.202.19.121	trojan.multiverze/genericrxss	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
6.	41.59.201.7	trojan.vsntda24	e3736bd6b87f2cd3a704c19033f904b861e7c720920ced10c16699d0ed01d819
7.	103.165.42.185	HEUR:Trojan.Linux.Miner.gen	40cb80b65c3f0dc8cfa6eaae51a475f79f0b8bf9a1406e3a5eed6b46f6c35a65
8.	106.222.224.153	Adware/Miner	3e9b22ca450a78aa2ee279292bc6f73fe6d1a575d8c9035c8fac36740cc28bd3
9.	176.208.33.247	E64/ABMiner.DBNS-21	2cc7249e379420271a359492b7cfa182251bc66817014699729a2bb346d94adb
10.	201.116.12.105	LINUX/AVI.Agent.gikam	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,815** web attacks compared to last week which was **1,923.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 08th of June to 14th of June, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	143.198.207.228	/
2.	173.231.185.164	/admin/config.php
3.	204.76.203.219	/.env
4.	24.199.89.244	/robots.txt
5.	204.76.203.206	/favicon.ico
6.	204.76.203.212	/.git/config

7.	93.123.109.231	/196.49.5.50/.env
8.	89.42.231.140	/config.php
9.	45.135.193.100	/1.php
10.	67.205.191.215	/boaform/admin/formLogin

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,207** ICS attacks compared to last week which was **1,919.**

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 08th of June to 14th of June, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	152.32.148.140	kamstrup_protocol	1025
2.	3.130.96.91	guardian_ast	10001
3.	45.140.17.26	IEC104	2404
4.	3.132.23.201	snmp	161
5.	35.203.210.215	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.