TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 22nd of June to 28th of June, 2025
Report No.: TZ-CERT/WRHP/2025/25

1. NETWORK ATTACKS

A total of **198,963** attacks have been recorded compared to last week's **560,506** 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.	45.144.29.201	root	root
2.	103.156.74.23	admin	P@ssw0rd
3.	164.163.98.28	ubuntu	admin
4.	45.14.245.67	administrator	password
5.	173.231.185.164	MANAGER	administrator
6.	195.178.110.160	(empty)	123456
7.	185.246.128.133	rootftp	rootftp@123
8.	164.163.98.29	mohammad	ipc@hs66
9.	193.105.134.95	odoo15	Pass@2023
10.	176.65.151.51	oscar	Marvin123

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 **66,145** malicious software distributed, compared to last week in which was **7,412.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Malware@#2z34o5m8iwnt9	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	41.231.8.19	Miner:Linux/Coinminer.99dbe0da	25b72e5d0b32b3758d8fb1e3ccdd5401a274caf5f56d5ec06da3a77cb16cd09f
3.	121.121.104.189	Linux.Siggen.8622	416b2e3f207bb5a08bc7df29108e054f4dcb912c9cb7c421c96f08864d23b5d3

4.	197.144.26.108	Malware.LINUX/AVI.Agent.nyayh	47b268c21591069bfe4099833ad66b8138a53ab2dcb866e040d466aee1f8624c
5.	200.75.2.138	EXP/ELF.Coinminer.A	48e8ad0a9587c30feea0e800e250ffe96036ca0c201ee90494101012de8579d1
6.	196.179.209.170	HEUR:Trojan.Linux.Miner.gen	1a8cfff75c4f4b4b6cdb982d60647c413cd306b561de716e1b76efea98c68c2a
7.	103.211.37.117	ELF:Agent-CXA [Trj]	40cb80b65c3f0dc8cfa6eaae51a475f79f0b8bf9a1406e3a5eed6b46f6c35a65
8.	152.70.144.244	Exploit.EXP/ELF.Coinminer.A	4578139f892a90ae1e0163e6db400e511170ee81549f8cdd7848da8f74e3f4e5
9.	37.156.146.183	Trojan[downloader]:Linux/Geninst.JM	d9c5bd8dc94485e3d286637b6b97d54a4225cf23a7f2f59a4c6c92e47d16acf4
10.	152.200.241.122	W32.Common.2A157808	88a2a33269c6699da8da7c736965b21a88f4b687d3f739d55258296322d21f15

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **8,313** web attacks compared to last week which was **2,278.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 22nd of June to 28th of June, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	185.177.72.108	/
2.	41.59.65.202	/admin/config.php
3.	173.231.185.164	/.git/HEAD
4.	153.213.12.50	/.env
5.	194.233.76.209	/favicon.ico
6.	45.232.240.13	/.git/config

7.	62.210.88.112	/.env.old
8.	162.216.16.109	/.git/logs/HEAD
9.	204.76.203.219	/.git/info/exclude
10.	185.196.9.254	/robots.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,439** ICS attacks compared to last week which was **3,727.**

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 22nd of June to 28th of June, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	41.59.65.202	kamstrup_protocol	1025
2.	118.193.36.107	IEC104	2404
3.	13.245.164.212	guardian_ast	10001
4.	3.130.96.91	snmp	161
5.	3.132.23.201	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.