TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 27th of July to 02nd of August, 2025
Report No.: TZ-CERT/WRHP/2025/30

1. NETWORK ATTACKS

A total of **148,260** attacks have been recorded compared to last week's **107,067** 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	Csgo@123
2.	94.156.177.243	admin	password
3.	196.251.88.103	(empty)	(empty)
4.	173.231.185.164	csgo	admin
5.	179.43.189.98	kamailio	345gs5662d34
6.	185.246.128.133	supervisor	123456
7.	134.199.153.38	postgres	root
8.	193.105.134.95	administrator	1qaz@WSX
9.	61.78.62.85	anonymous	123456789
10.	196.251.72.87	opensips	111111

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 **120,642** malicious software distributed, compared to last week in which was **127,249.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Miner:Linux/CoinMiner.99dbe0da	09501e8ffdec1bb8bab3a7bd4198452b6f183cd4e5523844bc4d1fdb83fd021f
2.	43.246.143.6	Trojan:Linux/Sshscan.X	3f97d465f56417e08438bad7dc3c562293526826ae76d551267286b91d42822a
3.	190.171.166.237	Unix.Trojan.Miner-9993889-0	66f8f315000fe6a2a2e09fba08a867c60f4d330099ab2e94f7bdcb0f0c869377

4.	41.33.177.133	Trojan:Linux/Multiverze	77ccd5ae0a102102b1c2032ff7f1fa8cc2f1069276f964210e644e1b21d8dd1f
5.	89.232.65.2	Trojan.Linux.Generic.413115	83331aee3703d73f8b6218b0537a3d95012c70bfaa2747bf8fdd1798500df41f
6.	5.63.71.102	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	5.248.157.177	trojan.jdobu/vsntgl25	c577132e0175fc3d6ed6fb880b0ddae6b60266db1f19d3b5974237d867ff7484
8.	185.243.5.66	Trojan:Linux/CoinMiner.C12	a5f837cd3b474a3ba5c81f4e9ae86888938b9dd6b9cf802e3e019d30de1df49d
9.	182.73.110.241	miner.jkrjv/r002c0dgs25	a79c55976c27bc471f3599e781d4f355645390705ea3f3e9c6fd504eb4957fc6
10.	41.78.81.250	Trojan.Linux.GenericKD.53615	d3978bf8ba2e285588ea5c7473dac39a25b72fc28664d3e78ffdbdaf85b98f57

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,787** web attacks compared to last week which was **2,646.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 27th of July to 02nd of August, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	178.128.61.13	/
2.	213.136.84.241	/admin/config.php
3.	173.231.185.164	/.env
4.	143.198.85.154	/cgi-bin/luci/;stok=/locale
5.	185.177.72.3	/robots.txt
6.	91.224.92.17	/favicon.ico

7.	35.243.254.66	/config.php
8.	38.211.193.130	/.git/config
9.	149.50.96.114	/admin/assets/js/views/login.js
10.	149.50.96.5	/admin/config.php?password%5B0%5D=ZIZO&username=admin

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,651** ICS attacks compared to last week which was **2,407.**

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 27th of July to 02nd of August, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	152.32.212.41	kamstrup_protocol	1025
2.	3.131.215.38	guardian_ast	10001
3.	3.130.96.91	IEC104	2404
4.	204.76.203.193	kamstrup_management_protocol	50100
5.	3.132.23.201	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.