TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 14th of September to 20th of September, 2025
Report No.: TZ-CERT/WRHP/2025/37

1. NETWORK ATTACKS

A total of **569,876** attacks have been recorded compared to last week's **1,343,294** 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.	45.159.112.142	root	123456
2.	185.116.161.213	ubuntu	admin
3.	185.4.30.93	user	password
4.	185.246.130.20	admin	3245gs5662d34
5.	196.251.88.103	(empty)	12345
6.	144.217.113.57	t128	(empty)
7.	196.11.177.98	administrator	P@ssw0rd
8.	103.99.206.83	jenkins	Azerty2025
9.	77.83.207.83	minecraft	Aa112211
10.	204.76.203.83	zabbix	nPSpP4PBW0

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 **503,917** malicious software distributed, compared to last week in which was **584,382.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	HEUR:Trojan.Linux.Miner.gen	0247e170f16fc586cbf818a7f9ef658dfc0d09279ed288de623fdea7ae06bc3d
2.	41.59.201.132	Miner:Linux/CoinMiner.JUO	05d563ca4dd86807cd5e20f4678d30ee71644137ffac807f2f5a6917fa9b78ec
3.	41.59.203.60	Elf.trojan.multiverze	169e1952898276010f212f609c4956a4fd89daa35ce3fa45c31357b44149efaf

4.	41.59.201.7	Trojan:Linux/Multiverze!rfn	17b7944a9b8a4e3edb1b1f2e743ae5d06dae0a8c3a9531e94970aa3261c2cab5
5.	87.118.159.6	Trojan/Linux.CoinMiner.ah	1bd3745a4f9043ead807d7777669b0dbf5b56985e5b3dd9d7cff8384154ea4a8
6.	122.3.116.169	Shell.trojan.multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	14.241.37.174	Miner:Multi/XmrigGo.SY	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
8.	62.171.154.173	Riskware.Linux.BitCoinMiner.1!c	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
9.	147.161.35.198	trojan.jggty/malxmr	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
10.	41.59.211.41	downloader.medusa/shell	7706b4ac0e8f740ff9184bc691dfc5b8d10415618bb21fa69b64d7c9f0dc98b6

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **20,184** web attacks compared to last week which was **24,118.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 14th of September to 20th of September, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	15.237.174.131	/
2.	139.87.112.120	/manager/
3.	195.178.110.201	/favicon.ico
4.	178.128.16.82	/admin/config.php
5.	91.224.92.17	/robots.txt
6.	146.190.110.241	/.env

7.	143.198.82.113	/.git/config
8.	157.230.60.129	/cgi-bin/luci/;stok=/locale
9.	139.87.112.108	/bitnami.css
10.	204.76.203.206	////index.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,445** ICS attacks compared to last week which was **8,306.**

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 14th of September to 20th of September, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	3.130.96.91	guardian_ast	10001
2.	3.131.215.38	kamstrup_protocol	1025
3.	3.137.73.221	IEC104	2404
4.	15.237.174.131	snmp	161
5.	3.143.33.63	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.