TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 21st of September to 27th of September, 2025
Report No.: TZ-CERT/WRHP/2025/38

1. NETWORK ATTACKS

A total of **793,190** attacks have been recorded compared to last week's **569,876** 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.	220.241.56.171	ubuntu	3245gs5662d34
3.	196.251.88.103	admin	password
4.	144.217.113.57	user	345gs5662d34
5.	196.11.177.98	test	admin
6.	185.246.130.20	postgres	nPSpP4PBW0
7.	103.99.206.83	345gs5662d34	P@ssw0rd
8.	213.136.70.135	steam	1234
9.	204.76.203.83	bitnami	Admin123
10.	196.251.84.225	tuan	root

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 **639,056** malicious software distributed, compared to last week in which was **503,917.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	trojan.hajime/mirai	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
2.	41.59.203.60	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
3.	41.59.201.7	miner.r002c0dh925/vxoac	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12

4.	87.118.159.6	miner.wwqhb/r002c0dhc25	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
5.	41.59.201.132	trojan.jggty/malxmr	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
6.	41.59.102.74	Trojan:Linux/CoinMiner.C12	d6e0eb28cfe1b224f061eff0581091dac985516c78d222f4921587d2ec612010
7.	212.233.205.81	Miner:Multi/XmrigGo.SY	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
8.	213.192.237.45	Riskware.Linux.BitCoinMiner.1!c	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
9.	196.203.231.46	trojan.jggty/malxmr	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
10.	125.209.82.205	downloader.medusa/shell	7706b4ac0e8f740ff9184bc691dfc5b8d10415618bb21fa69b64d7c9f0dc98b6

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **21,407** web attacks compared to last week which was **20,184.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 21st of September to 27th of September, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.112.119	/
2.	45.148.10.152	/logon.htm
3.	204.76.203.10	/login
4.	185.93.89.97	/news/
5.	146.190.111.146	/login/
6.	213.136.70.135	/favicon.ico

7.	139.87.112.120	/.env
8.	204.76.203.206	/robots.txt
9.	83.147.54.232	/cgi-bin/luci/;stok=/locale
10.	196.251.92.60	/help/topics/autodevops/index.md

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **10,096** ICS attacks compared to last week which was **3,445.**

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 21st of September to 27th of September, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	213.136.70.135	kamstrup_ management_protocol	50100
2.	3.134.148.59	guardian_ast	10001
3.	3.132.23.201	kamstrup_protocol	1025
4.	3.131.215.38	IEC104	2404
5.	3.137.73.221	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.