TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 12th of October to 18th of October, 2025
Report No.: TZ-CERT/WRHP/2025/41

1. NETWORK ATTACKS

A total of **956,132** attacks have been recorded compared to last week's **849,601** 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.	123.5.132.9	root	123456
2.	196.251.84.225	admin	123
3.	103.99.206.83	ubuntu	123@@@
4.	144.217.113.57	nagios	admin
5.	206.81.107.154	postgres	(empty)
6.	45.236.188.4	oracle	Password@2025
7.	196.251.88.103	steam	345gs5662d34
8.	203.78.147.68	jenkins	Qaz123qaz
9.	187.248.68.142	minecraft	P@ssw0rd
10.	167.250.224.25	user	QWE123!@#qwe

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 **544,800** malicious software distributed, compared to last week in which was **528,507.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Trojan[Miner]/Linux.BitCoinMiner.n	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
2.	41.59.203.60	Riskware.ElfArm64.CoinMiner.lacugy	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
3.	196.41.60.214	Trojan:Linux/CoinMiner.C12	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12

4.	41.59.201.132	Trojan:Unknow/Multiverze.Gen	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
5.	182.9.39.212	Trojan.Script.Agent.4!c	94db7ecdcb42293075ae21730582d84e35b82e5a53298b1d134984c1f1c65ea3
6.	31.14.188.69	Trojan:Linux/Multiverze!rfn	00a99866c7a6525cee1a3ca03c4f6362c5c94af5e52494a95f27beb2523fc6e1
7.	41.79.199.36	Trojan[Backdoor]/Linux.Hajime.c	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
8.	189.50.92.142	Trojan:Linux/Sshscan.X	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
9.	49.229.50.34	trojan.hajime/mirai	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
10.	41.59.211.41	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **21,363** web attacks compared to last week which was **28,395.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 12th of October to 18th of October, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	64.39.106.9	/
2.	64.39.106.45	/login/
3.	64.39.103.124	/assets/
4.	65.108.96.96	/news/
5.	195.178.110.201	/xmlrpc.php
6.	89.117.150.149	/robots.txt

7.	217.154.1.15	/admin/config.php
8.	196.249.102.149	/.env
9.	204.76.203.30	/favicon.ico
10.	64.39.106.58	/core/img/favicon.ico

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,279** ICS attacks compared to last week which was **3,998.**

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 12th of October to 18th of October, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	3.131.215.38	guardian_ast	10001
2.	45.95.147.229	kamstrup_protocol	1025
3.	3.134.148.59	IEC104	2404
4.	77.83.240.70	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.