TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 05th of October to 11th of October, 2025
Report No.: TZ-CERT/WRHP/2025/40

1. NETWORK ATTACKS

A total of **720,499** 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.	59.179.31.237	root	123
2.	167.250.224.25	admin	password
3.	196.251.84.225	github	123456
4.	103.99.206.83	kafka	admin
5.	187.248.68.142	ubuntu	(empty)
6.	144.217.113.57	elasticsearch	P@ssw0rd
7.	41.78.73.146	vpn	128tRoutes
8.	185.246.130.20	guest	1234567890
9.	91.92.241.148	sysadmin	12345
10.	204.76.203.83	git	Password123!

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 **528,507** malicious software distributed, compared to last week in which was **599,126.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Miner:Multi/XmrigGo.SY	d6e0eb28cfe1b224f061eff0581091dac985516c78d222f4921587d2ec612010
2.	41.59.203.60	Trojan:Linux/CoinMiner.C12	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
3.	41.59.201.132	HackTool/Linux.BitCoinMiner.a	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8

4.	85.111.32.196	PotentialRisk.PUA/AVI.CoinMiner.vxoac	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
5.	41.231.84.241	Trojan.Win32.Alevaul	94db7ecdcb42293075ae21730582d84e35b82e5a53298b1d134984c1f1c65ea3
6.	81.195.134.218	Script.Troj.multiverze.v	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	196.249.246.66	Generic.Linux.Medusa.C.8AFCBA4D	7706b4ac0e8f740ff9184bc691dfc5b8d10415618bb21fa69b64d7c9f0dc98b6
8.	154.197.141.9	HEUR:Trojan-Downloader.Shell.Agent.p	d6e34e17866dfea45c88188ae9468e7fa519d8ac25e4949d872c3400741cbcec
9.	41.79.199.36	Downloader.Agent/BASH!9.3675A (XSE:egYGnglUN1GfHaqUJi+Ndw)	ab065cdb8262d449f6b64dc3491f38f105509f62212ade27b909614ad91469f5
10.	41.59.149.97	Trojan.Hajime.fdakgq	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **28,395** web attacks compared to last week which was **85,977.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 05th of October to 11th of October, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.113.22	/
2.	64.39.106.5	/assets/
3.	64.39.106.38	/login
4.	64.39.106.49	/admin/config.php
5.	31.220.99.243	/favicon.ico
6.	152.42.218.74	/robots.txt

7.	213.136.70.135	/.env
8.	128.199.255.135	/index.html
9.	172.190.142.176	/explore
10.	64.39.103.49	/mgmt/tm/util/bash

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,998** ICS attacks compared to last week which was **5,979.**

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 05th of October to 11th of October, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	3.131.215.38	kamstrup_protocol	1025
2.	3.132.23.201	guardian_ast	10001
3.	137.184.197.81	IEC104	2404
4.	167.71.115.172	kamstrup_management_protocol	50100
5.	178.128.73.122	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.