TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 28th of September to 04th of October, 2025
Report No.: TZ-CERT/WRHP/2025/39

1. NETWORK ATTACKS

A total of **720,499** attacks have been recorded compared to last week's **793,190** 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.	46.250.250.74	root	(empty)
2.	187.248.68.142	(empty)	anonymous@
3.	103.99.206.83	exchange	!QAZ2wsx
4.	196.251.88.103	anonymous	r00t
5.	144.217.113.57	Admin	abc123456
6.	41.78.73.146	dba	P@ssw0rd!!
7.	185.246.130.20	service	pass1234
8.	62.60.131.157	appcrypto	1q2w3e4r
9.	196.11.177.98	seekcy	devry
10.	204.76.203.83	support	000000

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 **599,126** malicious software distributed, compared to last week in which was **639,056.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	Malware.LINUX/AVI.Agent.jggty	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
2.	41.59.211.41	HackTool/Linux.BitCoinMiner.a	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
3.	41.231.8.19	Riskware.Linux.BitCoinMiner.1!c	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12

4.	41.59.201.132	Shell.trojan.multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
5.	41.59.201.7	trojan.hajime/mirai	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
6.	103.164.85.26	TrojanDownloader:SH/SAgent.HNAA!MTB	a71aaea82b79b9e8a04c33ce41e4416bc402a5e650aacf2be2ea88ed3e1c8fe9
7.	124.43.19.173	Elf.trojan.multiverze	2ea782041e1edf52de42fdb415c63b4e2d0a24e3801385611d4c668c708a6457
8.	196.1.210.170	HEUR:Trojan.Linux.Miner.gen	2c950af8754cef68298d2e128d11045eed5018c35d30394f5ec087768dc9ae88
9.	118.103.236.181	Adware/Miner	2a71b0288b8b899dfb29e57a35cda39410fa5877e65f0e801f388d10f48eadbe
10.	156.224.139.130	Trojan:Linux/Multiverze!rfn	0f6966bada6e20ae6a8631d066252ca1261f2122d064878e6b4c85e4d4a4e183

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **85,977** web attacks compared to last week which was **21,407.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 28th of September to 04th of October, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	146.103.38.57	/activity
2.	75.119.140.177	/search
3.	195.178.110.108	/
4.	35.180.79.191	/logon.htm
5.	204.76.203.10	/time_entries
6.	37.60.141.156	/user/login

7.	95.214.52.137	/contact
8.	128.199.255.135	/activity.atom
9.	159.223.33.11	/search/node
10.	195.178.110.201	/issues

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **5,979** ICS attacks compared to last week which was **10,096.**

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 28th of September to 04th of October, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	213.136.70.135	kamstrup_ management_protocol	50100
2.	3.130.96.91	guardian_ast	10001
3.	144.91.113.43	kamstrup_protocol	1025
4.	3.131.215.38	IEC104	2404
5.	3.149.59.26	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.