TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 26th of October to 01st of November, 2025
Report No.: TZ-CERT/WRHP/2025/43

1. NETWORK ATTACKS

A total of **449,772** attacks have been recorded compared to last week's **713,074** 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.	103.99.206.83	root	123456
2.	62.60.131.18	admin	P@ssw0rd
3.	167.250.224.25	ubuntu	admin
4.	91.92.241.148	user	root
5.	185.246.130.20	developer	git
6.	104.248.89.72	postgres	pass123
7.	167.172.43.81	www	qwerty
8.	204.76.203.83	wordpress	password
9.	164.92.156.24	support	12345678
10.	196.251.84.225	deploy	xurros22$

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 **289,453** malicious software distributed, compared to last week in which was **584,271.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Script.Troj.multiverze.v	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.203.60	miner.r002c0dh925/vxoac	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
3.	41.59.201.132	Adware.Linux.GenericKD.7	a972d18300270d54a9ff831af150aa1fb4e7c319dba4fc9dac07b3af756aee05

4.	41.38.70.51	PUA/AVI.CoinMiner.pjtvf	07f79f61869a42c058c7ce0225bbe6bc7cb56ee862dca2b87f4e384150fd69da
5.	117.141.169.156	Trojan.Linux.GenericKD.54429	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
6.	196.41.60.214	CoinMiner.Linux.Agent.Ve20	f6002d4b799bea2f4d563194b8bb6fabc7332c2f2b638c5d358aeb8a8bba0803
7.	196.41.253.22	Tool.Linux.BtcMine.9999	0c7ce0368ae6fa3a1445b52c6d0e9f4a773cf0079601d0b5ece266837473c157
8.	41.59.149.234	Trojan.Linux.GenericKD.54427	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
9.	41.230.216.114	Adware.Linux.GenericKD.8	66c2450f5ee661cdca00d47410b83fa14f94d050a4ee698bfd8344fb8171084d
10.	62.60.131.18	Miner:Multi/XmrigGo.SY	ba1bb8a7ef31a255a52665d459bce74c9e57aec46767f93df1217f20db38fda8

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **47,379** web attacks compared to last week which was **57,469.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th of October to 01st of November, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.112.85	/
2.	139.87.112.75	/login
3.	139.87.112.110	/search/node
4.	139.87.112.83	/user/register
5.	195.178.110.199	/assets/
6.	146.103.38.57	/contact

7.	64.39.98.45	/user/login
8.	64.39.103.120	/user/password
9.	139.87.112.140	/system/timezone/0/-25200/1
10.	64.39.98.155	/robots.txt

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,133** ICS attacks compared to last week which was **4,018.**

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 26th of October to 01st of November, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	34.68.34.92	guardian_ast	10001
2.	77.83.240.70	IEC104	2404
3.	3.132.23.201	kamstrup_protocol	1025
4.	152.32.135.214	kamstrup_management_protocol	50100
5.	3.131.215.38	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.