TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 09th of November to 15th of November, 2025
Report No.: TZ-CERT/WRHP/2025/45

1. NETWORK ATTACKS

A total of **838,092** attacks have been recorded compared to last week's **607,328** 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.	145.239.255.60	root	123456
2.	103.76.111.110	admin	password
3.	178.214.77.7	test	admin
4.	60.163.139.198	orangepi	qwerty
5.	91.92.241.148	(empty)	Aa112233
6.	167.250.224.25	marek	orangepi
7.	187.248.68.142	newuser	nPSpP4PBW0
8.	41.78.73.146	supervisor	P@ssw0rd
9.	103.175.180.208	jenkins	Pi123321
10.	196.251.84.225	administrator	123456789

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 **503,266** malicious software distributed, compared to last week in which was **428,522.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	Trojan:Linux/Multiverze!rfn	0534c5c6d40ecb7b01e6e3844ffdd350cdc374cc8f0b265fe7b524f83c4a62a3
2.	196.41.60.214	Trojan.Linux.Agent.adc	12de77bef9500e41c76a2200bc6fa712e7e3fc188dfdd92a764a22c3421b7208
3.	41.59.203.60	EXP/ELF.Coinminer.A	1388fbdd71a44e3726852c002e2abfabc114575d951d7e702db3bd8fbae61a05

4.	5.189.153.250	HEUR:Trojan.Linux.Miner.gen	14c782bb55f60937521000fde2b95aeafafc822b791e4911e8f042fbcc211deb
5.	122.252.176.22	CoinMiner/Linux.Agent.30304472	1e968044a1a92b613d1d64fd665658ef361982b450c1d3ab90ccc7822f6025ce
6.	41.33.89.62	Trojan.Script.Multiverze.4!c	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	41.111.188.15	PUA/AVI.CoinMiner.pjtvf	07f79f61869a42c058c7ce0225bbe6bc7cb56ee862dca2b87f4e384150fd69da
8.	41.111.172.44	Risktool.Linux.Miner.nf	be8f32a15a3077ab8f5d25236d6e7b491cd216028f77d27bed5df333ff7c56c0
9.	41.139.177.151	Tool.Linux.BtcMine.9999	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
10.	41.59.211.41	Adware.Linux.GenericKD.13	0c7ce0368ae6fa3a1445b52c6d0e9f4a773cf0079601d0b5ece266837473c157

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **16,076** web attacks compared to last week which was **23,760.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 09th of November to 15th of November, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	13.245.108.156	/
2.	195.178.110.199	/robots.txt
3.	20.196.107.56	/cgi-bin/luci/;stok=/locale
4.	77.83.240.70	/.env
5.	13.74.149.244	/admin/config.php
6.	83.150.218.91	/favicon.ico

7.	45.95.147.229	/api/.env
8.	20.222.232.51	/sitemap.xml
9.	193.142.147.209	/.well-known/security.txt
10.	20.37.96.143	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **6,014** ICS attacks compared to last week which was **3,334.**

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 09th of November to 15th of November, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	45.95.147.229	kamstrup_management_protocol	50100
3.	13.245.108.156	IEC104	2404
4.	3.131.215.38	kamstrup_protocol	1025
5.	3.130.96.91	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.