



TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 16th of November to 22nd of November, 2025

Report No.: TZ-CERT/WRHP/2025/46

1. NETWORK ATTACKS

A total of **558,015** attacks have been recorded compared to last week's **838,092** 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.	144.126.224.102	sa	(empty)
2.	91.92.241.148	root	88888888
3.	103.175.180.208	anonymous	1234567890
4.	167.250.224.25	ipbx	12345678
5.	103.99.206.83	middleware	password
6.	41.78.73.146	infocare	admin
7.	77.83.207.82	ansible	123456
8.	204.76.203.83	ec2-user	1234567
9.	41.78.75.186	git	12345
10.	77.83.207.83	asteriskuser	qwerty

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 **295,033** malicious software distributed, compared to last week in which was **503,266**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	5.182.209.68	Script.Troj.multiverze.v	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	196.41.60.214	Adware.Linux.GenericKD.22 (B)	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	176.74.39.142	Riskware.Linux.BitCoinMiner.1!c	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

4.	41.38.51.10	Malware.LINUX/AVI.Agent.cciiu	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
5.	41.196.160.59	Trojan.Linux.MALXMR.US BLKH25	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
6.	41.47.123.20	Trojan:SH/Geninst.JA	55fde333bacf36587fd2d6fb78dafdbf47222f61a2d866b1ead53171b51fcb a0
7.	77.231.138.87	ELF:Mirai-CZH [Trj]	9d8f81732c3ecc13c2e57df3f8b333db142bc594db5cb0ebc599837e5b62434e
8.	88.229.201.121	Backdoor.Linux.Mirai.wan	79e6dad1656ecec96e74145ae5849375fac7c91ff84e282704dece2de39109ed
9.	117.6.128.131	Trojan.SH.TsunamiInstaller	90f42e0bc3b8fa7c18ed5512c0838b99753a7c409d254783f636034a125238fc
10.	5.182.209.68	Backdoor:Linux/Mirai.GS!MTB	f96b42d674954691a01bc5ceafc3302c0e6d8074e329b73f36920a40c210ed17

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **8,496** web attacks compared to last week which was **16,076**.

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th of November to 22nd of November, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	178.128.100.29	/
2.	130.49.178.120	/.env
3.	92.246.87.104	/robots.txt
4.	94.26.88.18	/favicon.ico
5.	3.227.240.138	/cgi-bin/luci;/stok=/locale
6.	15.181.1.164	/logon.htm

7.	44.210.15.221	/.well-known/security.txt
8.	172.190.142.176	/sitemap.xml
9.	20.243.53.228	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
10.	77.83.240.70	/cgi-bin/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/%32%65/bin/sh

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,786** ICS attacks compared to last week which was **6,014**.

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 16th of November to 22nd of November, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	3.130.96.91	kamstrup_management_protocol	50100
3.	3.134.148.59	IEC104	2404
4.	3.149.59.26	kamstrup_protocol	1025
5.	77.83.240.170	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.