TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 9th of March to 15th of March, 2026
Report No.: TZ-CERT/WRHP/2026/09

1. NETWORK ATTACKS

A total of **1,146,005** attacks have been recorded compared to last week's **1,661,396** 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.	14.225.2.66	root	123456
2.	218.21.0.230	admin	password
3.	161.97.161.123	test	123
4.	94.154.35.215	user	12345678
5.	137.184.226.118	postgres	12345
6.	179.43.139.58	oracle	1234
7.	164.92.151.89	mysql	123456789
8.	178.16.54.226	hadoop	qwerty
9.	213.209.159.159	git	admin
10.	104.248.171.251	backup	111111

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 **1,102,091** malicious software distributed, compared to last week in which was **731,611.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	trojan.multiverze/malxmr	72ce5b00ca4bfa0c18fcdf03a15e5391a85d81300783626598fe7e022e0ec538
2.	41.59.201.132	Trojan:Linux/CoinMiner!MTB	d7f98e379c400c13340781ccb65017c000330824ea26680866b9d3e43d641721
3.	41.59.203.60	Trojan.Linux.Miner.4!c	e948036f1c3b3024a6864fa1c49332c80e1fd28484cf487233a50154ffe104f8

4.	102.208.98.158	Trojan:Linux/Multiverze!rfn	00deea7003eef2f30f2c84d1497a42c1f375d802ddd17bde455d5fde2a63631f
5.	49.151.162.80	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
6.	102.208.164.38	miner.r06ec0dkh25/wlshq	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
7.	41.59.201.7	adware.multiverze/r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
8.	102.208.50.58	Trojan:Linux/Multiverze!rfn	b3a76e7dc7f934a42db6f9b5c9e12a5cc7d121706742b1ff69b881f32ccd5c6d
9.	122.224.42.2	miner.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
10.	81.20.195.202	Trojan:Linux/Multiverze!rfn	0707f0b02b792b14a52de487b55e52edcbc57de46a14527a5fc5ce24274c357d

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **37,736** web attacks compared to last week which was **55,007.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 9th of March to 15th of March, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	15.237.40.229	/
2.	195.26.255.237	/debug/default/view?panel=config
3.	185.16.39.146	/favicon.ico
4.	185.177.72.13	/robots.txt
5.	185.177.72.22	/.env
6.	185.177.72.49	/admin/config.php

7.	98.93.12.125	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
8.	185.177.72.23	/debug/default/view
9.	185.177.72.51	/debug/default/view.html
10.	141.98.10.68	/frontend/web/debug/default/view

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **8,488** ICS attacks compared to last week which was **7,179.**

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 9th of March to 15th of March, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	194.50.16.198	guardian_ast	5900
2.	87.249.133.72	kamstrup_protocol	64294
3.	18.116.101.220	IEC104	443
4.	3.129.187.38	kamstrup_management_protocol	445
5.	87.249.133.69	snmp	1433

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.