TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 02nd of March to 08th of March, 2026
Report No.: TZ-CERT/WRHP/2026/08

1. NETWORK ATTACKS

A total of **1,661,396** attacks have been recorded compared to last week's **1,180,767** 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.	14.225.2.122	admin	password
3.	64.227.140.142	user	123
4.	134.199.159.190	test	12345678
5.	139.59.67.39	ubuntu	1234
6.	46.101.165.248	oracle	12345
7.	161.35.147.28	postgres	qwerty
8.	46.101.169.113	345gs5662d34	123456789
9.	134.209.151.233	guest	admin
10.	170.64.230.102	mysql	P@ssw0rd

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 **731,611** malicious software distributed, compared to last week in which was **753,275.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	194.50.16.198	trojan.multiverze	71a48df7c23c160913e832f5579987e6c40bbab9c3d1a6ed19481d21db1ed49e
2.	204.216.147.144	HEUR:Trojan.Linux.Miner.gen	f01cac66a63b3bfd7409e4bceef30973a813f6ed4e99958313657449b1c7490f
3.	185.55.240.152	Trojan.Linux.Miner.4!c	e948036f1c3b3024a6864fa1c49332c80e1fd28484cf487233a50154ffe104f8

4.	41.93.85.245	Risktool.Linux.Miner.ck	079fef975c5c02792d0fbf7ffb61471ad3ff550b33c0af730f78a9865a4d3f50
5.	41.59.86.238	Trojan:Linux/Sshscan.X	168c689463606a3a6444767e445ffbfda5559926b684526f6d0b59d8be224a05
6.	160.119.76.47	Trojan Horse	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	41.59.86.254	HackTool/Linux.CoinMiner.a!crit	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
8.	41.78.64.60	Artemis!Trojan	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
9.	102.208.186.123	miner.cciiu/mirai	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
10.	196.49.5.50	Trojan:Linux/Multiverze!rfn	0707f0b02b792b14a52de487b55e52edcbc57de46a14527a5fc5ce24274c357d

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **55,007** web attacks compared to last week which was **26,801.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 02nd of March to 08th of March, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.112.139	/
2.	139.87.112.218	/login
3.	152.42.255.97	/login/
4.	152.42.221.249	/assets/webpack/pages.sessions.new.6dbf9c97.chunk.js
5.	185.16.39.146	/news/
6.	89.248.168.239	/assets/webpack/commons~pages.ldap.omniauth_callbacks~pages.omniauth_callbacks~pages.sessions~p

		ages.sessions.new.432e20dc.chunk.js
7.	152.42.164.39	/assets/webpack/runtime.9fcb75d4.bundle.js
8.	204.76.203.206	/assets/webpack/main.a66b6c66.chunk.js
9.	185.177.72.51	/assets/webpack/pages.sessions.new.6dbf9c97.chunk.js.map
10.	185.177.72.52	/assets/webpack/commons~pages.ldap.omniauth_callbacks~pages.omniauth_callbacks~pages.sessions~pages.sessions.new.432e20dc.chunk.js.map

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **7,179** ICS attacks compared to last week which was **8,645.**

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 02nd of March to 08th of March, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	194.50.16.198	guardian_ast	10001
2.	16.58.56.214	kamstrup_protocol	1025
3.	3.131.220.121	kamstrup_management_protocol	50100
4.	87.249.133.69	IEC104	2404
5.	87.249.133.13	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.