TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 2nd of February to 8th of February, 2026
Report No.: TZ-CERT/WRHP/2026/04

1. NETWORK ATTACKS

A total of **787,376** attacks have been recorded compared to last week's **726,807** 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.	141.105.71.30	root	123456
2.	94.154.35.215	admin	123
3.	171.6.185.49	user	password
4.	178.16.54.6	test	1234
5.	91.92.241.148	postgres	12345678
6.	167.99.32.200	ubuntu	3245gs5662d34
7.	152.42.136.105	oracle	345gs5662d34
8.	64.227.67.214	guest	12345
9.	146.190.232.99	345gs5662d34	admin
10.	185.246.128.133	mysql	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 **480,433** malicious software distributed, compared to last week in which was **469,852**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	141.105.71.30	HEUR:Trojan-Downloader.Shell.Agent.p	ed8a62a9ab02182d0d1f806af9a21d785801c0aaf7c8e265e077682f053c6b67
2.	94.154.35.215	downloader.gen2/mirai	5865dc23a2bc5fbae7f2963e98d4c39daf1391dd8821415d21ac66ee7a5a320e
3.	171.6.185.49	trojan.genericrxss/r002c0pjf23	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

4.	178.16.54.6	trojan.r002c0dli24	0165937bc9d7a0a3572826b2cf7bb2471a61dbe910e25b2799dc3481a8d7eb6e
5.	91.92.241.148	Trojan:Linux/Multiverze!rfn	1ae7b00337c85270ab8c44dac3b35ce988e6aa5a92ac17ea9b3310b15e802e80
6.	167.99.32.200	Trojan:Linux/Multiverze	29948c2e322b68dabbfafaac2593fa252c7d65b66b0d139a2397f327ad73d14e
7.	152.42.136.105	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
8.	64.227.67.214	Trojan:Linux/CoinMiner.C12	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
9.	146.190.232.99	Trojan.Linux.GenericKD.65861	0f414ee10329eda51be819f29d5895d0a78eccb668eda2189a32ed12f951229e
10.	185.246.128.133	adware.multiverze/r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **645** web attacks compared to last week which was **10,611.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 2nd of February to 8th of February, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	41.93.85.245	/
2.	41.59.86.238	/.env
3.	41.78.64.60	/favicon.ico
4.	77.83.240.70	/robots.txt
5.	194.50.16.73	/assets/webpack
6.	187.108.1.130	/help

7.	187.191.2.214	/help/user/&lt
8.	193.46.255.113	/users/sign_in?redirect_to_referer=yes&redirect_to_referer=yes
9.	41.59.203.60	/assets/webpack/e.action?e.action:this.defaultAction,this.target&e.action:this.defaultAction,this.target
10.	89.188.113.58	/explore/groups?sort=created_asc&sort=created_asc

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,814** ICS attacks compared to last week which was **3,963.**

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 2nd of February to 8th of February, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	87.249.133.84	kamstrup_protocol	1025
3.	89.188.113.58	IEC104	2404
4.	152.32.134.156	kamstrup_management_protocol	50100
5.	3.137.73.221	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.