TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 26th of January to 01st of February, 2026
Report No.: TZ-CERT/WRHP/2026/03

1. NETWORK ATTACKS

A total of **726,807** attacks have been recorded compared to last week's **802,526** 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.	165.22.163.83	root	123456
2.	178.16.54.6	admin	123
3.	185.11.61.226	user	3245gs5662d34
4.	91.92.241.148	345gs5662d34	345gs5662d34
5.	167.99.209.184	test	password
6.	94.154.35.215	oracle	1234
7.	193.105.134.95	ubuntu	root
8.	185.246.128.133	postgres	12345
9.	104.248.199.47	git	12345678
10.	178.62.232.23	guest	admin

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 **469,852** malicious software distributed, compared to last week in which was **379,045.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	HackTool/Linux.BitCoinMiner.a	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
2.	41.59.211.41	HEUR:Trojan.Linux.Miner.gen	8a37bb2a9e01e8f6f749d8ca2e0c18946fa24f6604262651b8b89f0a6e176615
3.	41.59.201.132	Risktool.Linux.Miner.ck	043675aa01acc869a78590befba137ba77e45a7509926739f7d13b75042d4119

4.	41.59.201.7	Application.Generic.4495641	0bf15aa87b7edf963533962273cd9c622b74dd1e47e770aa910fdf22ce0851df
5.	41.59.26.102	Linux/CoinMiner.ABF	10df86d8a7a3f56d2df33217da626c30e2e6005762f4427ef76c2815b40d8ce8
6.	213.128.187.247	Shell.trojan.multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	123.185.181.52	HackTool/Linux.CoinMiner.a!crit	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
8.	27.112.71.3	Trojan:Script/Wacatac.B!ml	29e2c53ae8f6252284fac2fb74eb0d721923316a320971c2c5bd293bcfd64d1a
9.	187.188.112.132	HEUR:Trojan-Downloader.Shell.Agent.a	9401c933c9f2d1b2100fbe39d46723492c174ecebfa82be8c73f9b4dd9471339
10.	41.59.203.60	Linux.Siggen.10752	2c8200689f018fdf2be10fc32a8a6c7bdf1962881a0253e81ba47c9f72f6f857

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **10,611** web attacks compared to last week which was **13,550.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th of January to 01st of February, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	185.16.39.79	/
2.	95.214.54.147	/logon.htm
3.	204.76.203.212	/favicon.ico
4.	212.86.120.49	/SDK/webLanguage
5.	78.153.140.203	/robots.txt
6.	138.197.65.222	/.env

7.	101.36.104.242	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
8.	193.142.147.209	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
9.	104.219.238.86	/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%%32%65/bin/sh
10.	107.170.64.184	/vendor/phpunit/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 **3,963** ICS attacks compared to last week which was **3,301.**

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 26th of January to 01st of February, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	guardian_ast	10001
2.	3.149.59.26	IEC104	2404
3.	37.19.195.75	kamstrup_protocol	1025
4.	3.137.73.221	kamstrup_management_protocol	50100
5.	34.68.34.78	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.