TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 19th of January to 25th of January, 2026
Report No.: TZ-CERT/WRHP/2026/02

1. NETWORK ATTACKS

A total of **802,526** attacks have been recorded compared to last week's **70,044** 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.	94.56.40.180	root	123123
2.	138.197.141.65	admin	root
3.	194.163.164.129	ftpuser	1q2w3e4r
4.	134.122.33.72	pi	654321
5.	185.11.61.151	centos	1234567
6.	91.92.241.148	backup	password1
7.	178.16.54.6	hadoop	1234567890
8.	134.209.207.137	administrator	vyos
9.	188.166.2.202	seki	(empty)
10.	134.199.192.131	nginx	admin123

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 **379,045** malicious software distributed, compared to last week in which was **923.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	TROJ_GEN.R002C0DIA25	0534c5c6d40ecb7b01e6e3844ffdd350cdc374cc8f0b265fe7b524f83c4a62a3
2.	41.59.211.41	HEUR:Trojan.Linux.Miner.gen	09501e8ffdec1bb8bab3a7bd4198452b6f183cd4e5523844bc4d1fdb83fd021f
3.	113.28.71.9	Trojan:Linux/Multiverze!rfn	289fd4a7a10aaf8aa313ab80cc170018fc662d0a7d034a3b92b9d3d3945b0736

4.	62.122.139.65	Application.Generic.4495641	36e70b9c5271aefeb3e4b4bc0eff8e81683f0ddfea4deed55dbc4cc0567ca179
5.	41.13.9.47	Static AI - Malicious ELF	3f711f010ee63dd3a089cff847c5443a0bdd5d63c49e956e4d3bc5cb922f9462
6.	60.187.197.135	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	41.111.178.28	Riskware.Linux.BitCoinMiner.1!c	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
8.	200.75.2.138	Adware/Miner	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9
9.	41.111.173.218	Adware.Linux.GenericKD.21	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
10.	41.59.203.60	Linux.Siggen.10752	32163237c78802ec6f0c1e734f120cc562f394c87d2a5b35bc5788fe9bb1653e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **13,550** web attacks compared to last week which was **21,616.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th of January to 25th of January, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	18.196.3.237	/
2.	34.207.235.82	/logon.htm
3.	185.16.39.79	/favicon.ico
4.	212.86.120.49	/robots.txt
5.	78.153.140.179	/SDK/webLanguage
6.	78.153.140.203	/.env

7.	149.50.97.166	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
8.	204.76.203.125	/geoserver/wfs?request=ListStoredQueries&service=wfs&version=2.0.0
9.	204.76.203.212	/login
10.	171.236.215.9	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **3,301** ICS attacks compared to last week which was **4,078.**

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 19th of January to 25th of January, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	45.95.147.229	guardian_ast	10001
2.	77.83.240.70	IEC104	2404
3.	3.137.73.221	kamstrup_management_protocol	50100
4.	3.132.23.201	kamstrup_protocol	1025
5.	34.19.116.48	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.