TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 12th of January to 18th of January, 2026
Report No.: TZ-CERT/WRHP/2026/01

1. NETWORK ATTACKS

A total of **70,044** attacks have been recorded compared to the previous week's **818,737** 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.	78.111.67.73	root	123456
2.	45.179.216.18	admin	password
3.	185.11.61.226	user	admin
4.	91.92.241.148	postgres	P@ssw0rd
5.	185.11.61.151	test	p@ssw0rd
6.	204.76.203.83	oracle	12345
7.	193.105.134.95	ubuntu	123456789
8.	185.246.128.133	guest	12345678
9.	157.245.66.5	mysql	1234
10.	176.65.132.95	git	123

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 **923** malicious software distributed, compared to previous week in which was **406,178.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.221.165.53	Trojan:Linux/Multiverze!rfn	d0b25d94a4ce13959db8529e67fa22ae4c60a923e7dfc5a96954f971c80f9760
2.	154.126.208.190	downloader.gen2/mirai	00c9c6183c973b3f487ba67d953788025099f9b1f0e2b341d1a1267fdc900434
3.	223.205.219.80	Trojan:Script/Wacatac.B!ml	927ded80ff4459c92b4ef59e1ec081738139462a4abe1ceb95e1052870107a63

4.	87.222.142.140	HEUR:Backdoor.Linux.Mirai.gen	ec12b5ee023ece253d4dbb0fd7fb45f8f5b21918ec7a550a203300265d3adfe1
5.	129.0.182.246	Trojan:Win32/Egairtigado!rfn	51f8f0550b5383eee78778f392e2df67b3893dbe490bb257436222c36a9d6769
6.	196.219.0.170	Adware.Linux.GenericKD.22	3625d068896953595e75df328676a08bc071977ac1ff95d44b74bbcb7018c6f
7.	180.242.78.43	Malware.LINUX/AVI.Agent.cciiu	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
8.	196.218.39.134	BASH/Mirai.AEH!tr.dldr	a4937335be62e9843f12854b43ea2ac007e27863aeb3d36c418cc09d63b49642
9.	196.218.39.131	HTML.ExploitKit	40bec1ee86a5ba5ed620bbe546b09d072481d71356ba2025974c08a0e3f3fb0c
10.	36.77.227.45	Trojan:JS/Berbew	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **21,616** 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 12th of January to 18th of January, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	213.209.159.151	/
2.	185.196.10.2	/favicon.ico
3.	195.26.240.95	/robots.txt
4.	5.104.86.151	/SDK/webLanguage
5.	70.23.81.129	/.well-known/security.txt
6.	82.180.145.120	/sitemap.xml

7.	78.153.140.203	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
8.	204.76.203.18	/core/misc/favicon.ico
9.	157.230.105.206	/user/login
10.	192.159.99.95	/login

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,078** 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 12th of January to 18th of January, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	147.182.247.10	kamstrup_management_protocol	50100
2.	134.122.46.85	guardian_ast	10001
3.	185.93.89.172	IEC104	2404
4.	207.90.244.26	snmp	161
5.	207.90.244.3	kamstrup_protocol	1025

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.