TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 23rd of February to 01st of March, 2026
Report No.: TZ-CERT/WRHP/2026/07

1. NETWORK ATTACKS

A total of **1,180,767** attacks have been recorded compared to last week's **908,185** 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.	209.38.21.90	root	12345678
2.	170.64.138.253	centos	passw0rd
3.	170.64.177.132	debian	P@ssw0rd
4.	129.212.178.128	sol	root
5.	209.38.89.29	backup	123123
6.	209.38.86.230	pi	admin123
7.	94.154.35.215	administrator	654321
8.	170.64.205.89	solana	1q2w3e4r
9.	14.225.2.122	dspace	1234567
10.	38.49.209.144	ftpuser	1234567890

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 **753,275** malicious software distributed, compared to last week in which was **402,386.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	194.50.16.198	Linux.Siggen.10752	106ef2534abd3904912df6c156f8385799c364c5b4fdad54c71509ff51292901
2.	185.55.240.152	trojan.genericrxss/r002c0pjf2	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
3.	204.216.147.144	adware.multiverze/r002c0dkq25	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

4.	41.93.85.245	Gen:Variant.Backdoor.Linux.Tsunami.1	9701ae7249aa394624bf33096e3f5dd2be0bb778debba3364f5277a50874cc31
5.	41.59.86.238	Trojan:Linux/Multiverze!rfn	094d2147548839ba5ed36d884983aaf14bd7ae650095dec96a1cf537d3b23b48
6.	80.94.93.5	HEUR:Trojan.Linux.Miner.gen	b14212857fe74349571dc653447dd59ff5938a768a65f90a3d4d653b669f8c83
7.	102.208.186.123	Application.Generic.4495641	00deea7003eef2f30f2c84d1497a42c1f375d802ddd17bde455d5fde2a63631f
8.	59.120.103.230	Trojan.GenericKD.74212318	32b44db3980a94e1be989a4c5605cb2b3ed2db6cfa208943c70ae2a82d983291
9.	137.64.10.229	downloader.medusa/shell	8b9ea0ab6d318a0bf0e90a2d12c9b2a23d3f242f1b081464e4721fbc12b1ec11
10.	144.172.112.233	Trojan-Downloader.Shell.Miner.cf	dccfd62d350184fc137b18acbdd56fceee07f2c7b7f89eb1071e7c4eb0f01bcd

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **26,801** web attacks compared to last week which was **25,518.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 23rd of February to 01st of March, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	140.82.0.86	/
2.	45.194.92.25	/manager/html
3.	204.76.203.206	/favicon.ico
4.	185.16.39.146	/robots.txt
5.	204.76.203.210	/.env
6.	152.42.221.249	/cgi-

		bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
7.	152.42.204.17	/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/bin/sh
8.	45.153.34.187	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
9.	89.248.168.239	/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
10.	204.76.203.212	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **8,645** ICS attacks compared to last week which was **4,349.**

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 23rd of February to 01st of March, 2026, are detailed.

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	194.50.16.198	guardian_ast	10001
2.	77.83.240.70	kamstrup_protocol	1025
3.	16.58.56.214	IEC104	2404
4.	3.130.168.2	kamstrup_management_protocol	50100
5.	3.129.187.38	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.