TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 16th of February to 22nd of February, 2026
Report No.: TZ-CERT/WRHP/2026/06

1. NETWORK ATTACKS

A total of **908,185** attacks have been recorded compared to last week's **1,148,364** 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.	176.241.83.187	root	123456
2.	165.245.134.199	admin	password
3.	165.245.138.205	user	123
4.	129.212.182.142	test	1234
5.	134.199.206.92	ubuntu	12345678
6.	165.245.129.165	oracle	admin
7.	165.245.140.19	postgres	12345
8.	94.154.35.215	guest	qwerty
9.	178.128.226.179	git	123456789
10.	91.92.241.148	mysql	111111

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 **402,386** malicious software distributed, compared to last week in which was **536,901.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	194.50.16.198	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	137.64.10.229	Riskware.Linux.BitCoinMiner.1!c	3625d068896953595e75df328676a08bc071977ac1ff95d44b745bbcb7018c6f
3.	204.216.147.144	Trojan:Linux/Multiverze!rfn	dbb7ebb960dc0d5a480f97ddde3a227a2d83fcaca7d37ae672e6a0a6785631e9

4.	41.93.85.245	Trojan.Linux.Generic.D106EB	17f65f15d3f2af0470a2b4c1baf57227fc6f596e1e1781c2ecd7caef9a0e198a
5.	41.78.64.60	Adware.Linux.GenericKD.21	048e374baac36d8cf68dd32e48313ef8eb517d647548b1bf5f26d2d0e2e3cdc7
6.	102.208.186.123	Linux.Siggen.10752	cae61337a4c92281fb5ba2ae0401e98ed1683bb41fdd833c25ea172bb15f459e
7.	185.55.240.152	Trojan:Win32/Egairtigado!rfn	f1c0e109640d154246d27ff05074365740e994f142ef9846634bec7b18e3b715
8.	144.24.88.37	Malware.LINUX/AVI.Agent.osqhr	59c29436755b0778e968d49feeae20ed65f5fa5e35f9f7965b8ed93420db91e5
9.	77.83.240.70	Trojan.Linux.Mirai	3705ef166838d7ac0290b2bf0eb5cbf6151e61959977abf0ef51213cb6809919
10.	187.191.2.214	BASH/Mirai.AEH!tr.dldr	fb51cc30f5ac43a9cc4ee8e036da03135fdfdb5c285d651682e96d42541fd678

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **25,518** web attacks compared to last week which was **22,646.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th of February to 22nd of February, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	95.111.231.235	/
2.	93.185.165.232	/script
3.	204.76.203.206	/admin/config.php
4.	185.16.39.146	/.env
5.	45.194.92.25	/favicon.ico
6.	165.245.188.128	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php

7.	162.217.98.180	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
8.	87.106.166.65	/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
9.	45.190.112.54	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
10.	207.180.231.68	/hello.world?%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 **4,349** ICS attacks compared to last week which was **5,194.**

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 16th of February to 22nd of February, 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.	18.116.101.220	IEC104	2404
4.	18.218.118.203	kamstrup_management_protocol	50100
5.	45.82.78.106	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.