TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 09th of February to 15th of February, 2026
Report No.: TZ-CERT/WRHP/2026/05

1. NETWORK ATTACKS

A total of **1,148,364** attacks have been recorded compared to last week's **787,376** 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.	198.143.191.202	sa	123456
2.	167.99.47.208	root	password
3.	104.248.196.57	admin	12345678
4.	170.64.146.163	user	123456789
5.	129.212.177.54	dbuser	qwerty
6.	165.245.142.196	anonymous	admin
7.	129.212.186.129	app	(blank)
8.	129.212.189.214	(blank)	!QAZ2wsx
9.	129.212.181.67	test	anonymous@
10.	129.212.187.71	www	root

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 **536,901** malicious software distributed, compared to last week in which was **480,433.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.201.132	trojan.genericrxss/r002c0pjf23	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	41.59.203.60	Trojan:Linux/Multiverze!rfn	82317107f5be9f7f6c73c3bda834a69461f7e94cef83587e72ff6749f7b94498
3.	41.59.211.41	HEUR:Trojan.Linux.Miner.gen	9e5b93d3095f577136717e6aae8b51fea50d66ef9123eedccfc23b8faebf6d6c

4.	41.59.149.194	Trojan.Linux.Generic.355701	0390934d3a4f01ce48546c99830547c9c8f46672adf9eb475fa1a03f29664e5b
5.	82.137.255.8	Elf.trojan.eddci	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
6.	117.140.173.58	Generic.Bash.MiraiA.296477B6	e4374bfdcc87adbb1948c4d94c7a5cd37a4041e0d82a93eb69a0d72b75093bb2
7.	41.13.25.240	Win32.Trojan-Downloader.Agent.Pjgl	19fb02b2b324fd44462efe40714900e450dd9f67bc0d1b0e691def4a429dba1a
8.	102.208.164.38	Trojan.Script.Shell.a!c	f0f0c3f43e8537cb43cb932959534f038ec6ee9405aab2303d7da4d0cb34fb00
9.	41.124.121.19	Trojan:Win32/Kepavll!rfn	6eab89c2c5d517644343626c17077ed5198af9af38a98fa211ed8ee5d8175ded
10.	165.165.141.93	SH/Mirai.D.gen!Camelot	b41eb4fa4b1270f8b9f6a723d57f144f24f3f677e49cd340552aa6a4a457b251

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **22,646** web attacks compared to last week which was **21,296.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 09th of February to 15th of February, 2026, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	84.247.164.62	/
2.	176.120.22.114	/.env
3.	204.76.203.206	/favicon.ico
4.	204.76.203.210	/robots.txt
5.	185.16.39.146	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.php
6.	159.223.54.162	/cgi-

		bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
7.	45.135.193.11	/?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
8.	204.76.203.212	/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.	87.120.191.67	/hello.world?%ADd+allow_url_include%3d1+%ADd+auto_prepend_file%3dphp://input
10.	195.3.221.8	/vendor/phpunit/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 **5,194** ICS attacks compared to last week which was **3,814.**

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 09th of February to 15th 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.	87.249.133.18	kamstrup_management_protocol	50100
4.	18.218.118.203	IEC104	2404
5.	47.84.199.67	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.