TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 27th of April to 03rd of May, 2025
Report No.: TZ-CERT/WRHP/2025/17

1. NETWORK ATTACKS

A total of **107,466** attacks have been recorded compared to last week's **60,099** 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.	185.233.247.245	root	123456
2.	45.249.8.86	admin	root
3.	62.149.25.72	user123	password
4.	218.92.0.178	guest	admin
5.	177.190.64.21	user	P@ssw0rd!!
6.	185.246.128.133	ftpuser	Pambazuka08
7.	193.105.134.95	user1	(empty)
8.	193.233.202.219	postgres	user
9.	192.243.100.40	ubnt	support
10.	45.144.29.201	yhtcAdmin	888888

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 **65,749** malicious software distributed, compared to last week in which was **54,134.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.203.56.193	miner.gikam/r002c0dcq25	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf
3.	62.201.218.122	Linux.Siggen.8622	1ef0eb60318495dd0cb100fc828f28237d487b800605c7cc54155cf34582598b

4.	117.156.187.120	miner.pvcyv/r002c0dcv25	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a
5.	196.218.94.218	Riskware.Linux.BitCoinMiner.1!c	7780e72f7dea978946d4615c8db1b239d3e2c742cfc8be2934006b1fd6071110
6.	103.142.108.170	Artemis!Trojan	b6ee8e08f1d4992ca85770e6883c1d2206ebbaf42f99d99aba0e26278de8bffb
7.	79.134.7.175	downloader.bash/miraia	c664663a2343214c23179705cc5499467a2e148fcfb8ea6db01e911ce2aafc2e
8.	14.170.154.14	Possible_BASHDLOD.SMLBAT3	d70ef247ce69731ea5a283125221dcd754b562f6391f4329a024ccabdfbb25e7
9.	79.126.115.32	BASH/Mirai.AEH!tr.dldr	84f228052f0382afe74b823ad694bc91bb0fdad4bbee8cef2658cf7e94426bec
10.	41.43.25.132	Backdoor:Linux/Hajime.A	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,558** web attacks compared to last week which was **2,275.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 27th of April to 03rd of May, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	154.81.156.54	/
2.	173.231.185.164	/admin/config.php
3.	147.182.242.132	/.env
4.	154.81.156.35	/.git/config
5.	45.148.10.97	/favicon.ico
6.	58.211.18.68	/admin/config.php?password%5B0%5D=ZIZO&userna

		me=admin
7.	154.81.156.7	/boaform/admin/formLogin
8.	185.218.86.4	/robots.txt
9.	185.218.84.178	/config.php
10.	207.180.196.165	/core/misc/favicon.ico

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,830** ICS attacks compared to last week which was **781.**

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 27th of April to 03rd of May, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	118.26.104.212	kamstrup_protocol	1025
2.	15.237.40.229	EC104	2404
3.	169.150.196.121	guardian_ast	10001
4.	45.95.147.229	snmp	161
5.	207.90.244.13	Kamstrup_management_protocol	50100

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.