TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 20th of April to 26th of April, 2025
Report No.: TZ-CERT/WRHP/2025/16

1. NETWORK ATTACKS

A total of **60,099** attacks have been recorded compared to last week's **226,616** 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.	62.149.25.72	root	admin
2.	45.249.8.86	admin	shell
3.	87.98.138.86	tshell	(empty)
4.	185.246.128.133	guest	123456
5.	170.64.238.153	support	founder88
6.	193.105.134.95	ftpuser	support
7.	173.231.185.164	user	password
8.	174.126.229.244	default	vadmin
9.	203.251.25.226	vadmin	54321
10.	14.50.131.36	administrator	12345678

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 **54,134** malicious software distributed, compared to last week in which was **70,865.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	Trojan.Win32.MULTIVERZE.VSNW01J24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	196.219.75.37	RiskWare[RiskTool]/Linux.BitCoinMiner	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf
3.	190.200.214.231	Trojan:Linux/Coinminer!rfn	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a

4.	196.218.195.122	TROJ_GEN.R002C0DCK25	7780e72f7dea978946d4615c8db1b239d3e2c742cfc8be2934006b1fd6071110
5.	200.84.122.104	Trojan.Linux.GenericKD.45058	b6ee8e08f1d4992ca85770e6883c1d2206ebbaf42f99d99aba0e26278de8bffb
6.	196.203.231.205	Unix.Trojan.Coinminer-10007719-0	b096e257576ea8265b3dde1b2a8bf67606a8ec7994bf41ac4b52b329714df323
7.	196.219.79.196	Linux.Siggen.8622	3ff3a9c848b9a1571f528dd0d2a316a767ac2fdcc0dd3db0a8a8879564a5d759
8.	41.111.171.105	W32.Common.2A157808	88a2a33269c6699da8da7c736965b21a88f4b687d3f739d55258296322d21f15
9.	196.219.0.170	Artemis!Trojan	0390934d3a4f01ce48546c99830547c9c8f46672adf9eb475fa1a03f29664e5b
10.	14.236.253.47	Risktool.Linux.Miner.ck	243407432245afff15e8c3aeb3422eb878c53acd2b0f9468c47d613a4f652abe

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,275** web attacks compared to last week which was **4,171.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th of April to 26th of April, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	154.83.103.106	/
2.	154.81.156.54	/admin/config.php
3.	154.83.103.202	/.env
4.	185.255.122.19	/.git/HEAD
5.	173.231.185.164	/.git/config
6.	83.222.191.34	/favicon.ico

7.	35.180.129.176	/users/sign_in
8.	216.10.250.218	/.aws/credentials
9.	35.195.46.0	/.git/index
10.	37.32.20.198	/.env.production

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **781** ICS attacks compared to last week which was **1,974.**

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 20th of April to 26th of April, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	35.180.129.176	kamstrup_protocol	1025
2.	207.90.244.27	Kamstrup_management_protocol	50100
3.	207.90.244.25	guardian_ast	10001
4.	207.90.244.13	IEC104	2404
5.	107.170.2.114	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.