TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 18th of May to 24th of May, 2025
Report No.: TZ-CERT/WRHP/2025/20

1. NETWORK ATTACKS

A total of **134,559** attacks have been recorded compared to last week's **152,934** 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.	103.80.117.250	root	root
2.	187.85.152.82	admin	123456
3.	45.144.29.201	ubuntu	P@ssw0rd!!
4.	45.14.245.67	cameras	password
5.	45.249.8.86	(empty)	(empty)
6.	194.0.234.107	Administrator	admin
7.	89.20.53.95	wwwroot	1234567890
8.	185.246.128.133	888888	broadguam1
9.	193.105.134.95	dell	Wind1doW$
10.	185.233.247.245	user	founder88

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 **9,574** malicious software distributed, compared to last week in which was **45,512.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.139.133.163	Miner:Linux/CoinMiner.99dbe0da	0fd4aaed2bfff47c0dbd6e34ba6abd2988493e9cf43038e75526f81bf9e089f6
2.	41.78.76.190	Linux/CoinMiner.ABF	2cc7249e379420271a359492b7cfa182251bc66817014699729a2bb346d94adb
3.	49.249.85.2	HEUR:Trojan.Linux.Miner.gen	3e9b22ca450a78aa2ee279292bc6f73fe6d1a575d8c9035c8fac36740cc28bd3

4.	41.121.91.122	Risktool.Linux.Miner.ck	40cb80b65c3f0dc8cfa6eaae51a475f79f0b8bf9a1406e3a5eed6b46f6c35a65
5.	14.170.154.14	Linux.Siggen.8622	51b052a524af278366fb5527d4a5eee949b63f85168c37d4f97aefe3e73fe66a
6.	202.141.252.141	Shell.trojan.mirai	5504b184a859986ff9a68dbb4f215ee201bb4ac94b0cfb67e10343ad28b0979d
7.	156.199.1.97	A Variant Of Linux/Xorddos.P	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	89.31.58.165	trojan.hajime/mirai	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
9.	180.253.163.216	HackTool.XMRMiner!1.FD0F (CLASSIC)	fc8730fbe87bcbdc093a1ffbcb0028ccb4c24638e55d13fd853b07574f4cbe4a
10.	182.253.57.55	HackTool/Linux.BitCoinMiner.a	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,067** web attacks compared to last week which was **11,021.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 18th of May to 24th of May, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	142.132.250.254	/
2.	173.231.185.164	/admin/config.php
3.	93.123.109.231	/.env
4.	204.76.203.206	/.git/config
5.	204.76.203.219	/favicon.ico
6.	185.92.195.238	/boaform/admin/formLogin

7.	206.189.136.214	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	93.123.109.230	/logon.htm
9.	93.123.109.229	/robots.txt
10.	204.76.203.212	/nice%20ports%2C/Tri%6Eity.txt%2ebak

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,389** ICS attacks compared to last week which was **2,446.**

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 18th of May to 24th of May, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.206.250	IEC104	2404
2.	3.137.73.221	kamstrup_protocol	1025
3.	205.210.31.25	guardian_ast	10001
4.	45.140.17.26	snmp	161
5.	212.83.190.55	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.