TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 25th of May to 31st of May, 2025
Report No.: TZ-CERT/WRHP/2025/21

1. NETWORK ATTACKS

A total of **105,696** attacks have been recorded compared to last week's **134,559** 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.	181.50.203.89	root	123456
2.	89.20.53.95	admin	root
3.	115.247.46.121	(empty)	P@ssw0rd!!
4.	181.50.203.90	ubnt	password
5.	216.238.84.195	uucp	1234
6.	193.105.134.95	345gs5662d34	123
7.	185.246.128.133	oracle	(empty)
8.	152.53.249.114	postgres	Broadguam1
9.	138.197.96.181	tshell	345gs5662d34
10.	173.231.185.164	user123	adminHW

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 **58,981** malicious software distributed, compared to last week in which was **9,574.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	103.121.123.3	Adware/Miner	0670da04a700a5e7ec0ca80de285d75985116b669dc02c61cebfc22b5b3edab3
2.	41.78.76.190	Trojan:Linux/Multiverze	4578139f892a90ae1e0163e6db400e511170ee81549f8cdd7848da8f74e3f4e5
3.	117.3.1.58	trojan.r002c0dbc25	6b6c1bd77604a85b0abcd98103eb738ca94cc1fbf74043f62ed95ec5561e507f

4.	89.31.58.165	HEUR:Trojan.Linux.Miner.gen	72ce5b00ca4bfa0c18fcdf03a15e5391a85d81300783626598fe7e022e0ec538
5.	41.78.219.71	Unix.Trojan.Coinminer-10007719-0	76f4cff23b97b5cc222d0183a9ece353a5a36cfad2e722c6a7e00f47bf3137f0
6.	156.198.230.36	Linux.Siggen.8622	51b052a524af278366fb5527d4a5eee949b63f85168c37d4f97aefe3e73fe66a
7.	196.218.162.53	Risktool.Linux.Miner.ck	40cb80b65c3f0dc8cfa6eaae51a475f79f0b8bf9a1406e3a5eed6b46f6c35a65
8.	197.14.1.181	HEUR:Trojan.Linux.Miner.gen	3e9b22ca450a78aa2ee279292bc6f73fe6d1a575d8c9035c8fac36740cc28bd3
9.	45.221.72.34	Linux/CoinMiner.ABF	2cc7249e379420271a359492b7cfa182251bc66817014699729a2bb346d94adb
10.	45.240.34.74	HackTool/Linux.BitCoinMiner.a	2ef6bb55a79d81fbda6d574456a8c187f610c5ae2ddca38e32cf7cc50912b0bf

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,935** web attacks compared to last week which was **4,067.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 25th of May to 31st of May, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	194.160.194.67	/
2.	217.160.35.149	/.env
3.	51.210.223.51	/admin/config.php
4.	173.231.185.164	/favicon.ico
5.	204.76.203.212	/.git/config
6.	204.76.203.206	/goform/set_LimitClient_cfg

7.	204.76.203.219	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	143.198.207.228	/1.php
9.	185.218.84.7	/form.html
10.	176.65.149.188	/geoip/

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,658** ICS attacks compared to last week which was **2,389.**

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 25th of May to 31st of May, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	3.137.73.221	IEC104	1025
2.	101.36.97.74	kamstrup_protocol	2404
3.	35.180.79.191	guardian_ast	10001
4.	3.132.23.201	snmp	50100
5.	45.95.147.229	Kamstrup_management_protocol	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.