TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 3rd of August to 9th of August, 2025
Report No.: TZ-CERT/WRHP/2025/31

1. NETWORK ATTACKS

A total of **634,455** attacks have been recorded compared to last week's **148,260** 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.	103.156.74.23	root	123456
2.	94.156.177.243	admin	admin
3.	196.251.88.103	(empty)	password
4.	173.231.185.164	hadoop	Abc123
5.	179.43.189.98	ubuntu	(empty)
6.	185.246.128.133	www	Admin@123
7.	134.199.153.38	postgres	root
8.	193.105.134.95	administrator	1qazXSW@
9.	61.78.62.85	adolphinscheduler	broadguam1
10.	196.251.72.87	elasticsearch	3245gs5662d34

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 **517,775** malicious software distributed, compared to last week in which was **120,642.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	MW32.Common.00000000	99eb12f2ab3c4866a353e098ffa3cb7a967e617c49b98480394ec5d8ea92b094
2.	43.246.143.6	HEUR:Trojan.Linux.Miner.gen	15d2ae90c82b2c36cceb01286222414f9f0e4eccbae21b981fa72c9accb39b52
3.	190.171.166.237	trojan.nutax/r002c0dkp24	3168306188b22044cc4b5ecf7bc7259df69e0dfbc568445e30ee0c22211a129a

4.	41.33.177.133	miner.r002c0dbe25	3c5ffe548ea93622d11b67eead48d50f9ee39b09e1e813747883d1528569ffd1
5.	89.232.65.2	ELF:Agent-CXA [Trj]	51b052a524af278366fb5527d4a5eee949b63f85168c37d4f97aefe3e73fe66a
6.	5.63.71.102	Trojan:Script/Multiverze	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	5.248.157.177	trojan.r002c0dgu25/xqfnl	a5f837cd3b474a3ba5c81f4e9ae86888938b9dd6b9cf802e3e019d30de1df49d
8.	185.243.5.66	Trojan:Linux/CoinMiner.C12	a5f837cd3b474a3ba5c81f4e9ae86888938b9dd6b9cf802e3e019d30de1df49d
9.	182.73.110.241	miner.jkrjv/r002c0dgs25	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
10.	41.78.81.250	Trojan.Linux.GenericKD.53615	d3978bf8ba2e285588ea5c7473dac39a25b72fc28664d3e78ffdbdaf85b98f57

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **25,621** web attacks compared to last week which was **4,787.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 3rd of August to 9th of August, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	178.128.61.13	/
2.	213.136.84.241	/admin/config.php
3.	173.231.185.164	/favicon.ico
4.	143.198.85.154	/sysmgmt/2015/bmc/info
5.	185.177.72.3	/users/sign_in
6.	91.224.92.17	/admin/assets/js/views/login.js

7.	35.243.254.66	/CGI/Java/Serviceability?adapter=device.statistics.device
8.	38.211.193.130	/.git/config
9.	149.50.96.114	/q79w_38jg__.shtml
10.	149.50.96.5	/.env

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **14,860** ICS attacks compared to last week which was **1,651.**

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 3rd of August to 9th of August, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	13.57.185.66	kamstrup_management_protocol	50100
2.	8.52.235.60	snmp	2404
3.	152.32.134.166	IEC104	161
4.	40.160.19.170	kamstrup_protocol	1025
5.	40.160.12.59	guardian_ast	10001

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.