TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 24th of August to 30th of August, 2025
Report No.: TZ-CERT/WRHP/2025/34

1. NETWORK ATTACKS

A total of **637,679** attacks have been recorded compared to last week's **1,255,003** 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.	103.146.203.60	root	123456
2.	185.233.247.245	admin	admin
3.	38.140.236.91	cloudera	(empty)
4.	103.91.140.28	(empty)	password
5.	1.34.6.225	user	345gs5662d34
6.	196.251.88.103	support	3245gs5662d34
7.	203.166.207.157	developer	P@ssw0rd
8.	66.78.40.221	postgres	cloudera
9.	104.168.169.218	deploy	123456789
10.	45.240.183.14	git	root

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 **589,805** malicious software distributed, compared to last week in which was **866,432.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	Trojan/Linux.CoinMiner.ah	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
2.	41.59.211.41	Trojan.Linux.Generic.413115 (B)	10a1aac9eb7707893306482216b9174dde795c20dd3ea69d8c5730f5f503f33d
3.	41.59.102.74	CoinMiner/Linux.Agent.30304472	17f551e0a1ca78baf32038c6de781452386726293c0c222203e08f3eb08119b2

4.	41.59.149.75	HEUR:Trojan.Linux.Miner.gen	1bbe53c96d4e6238cb542b526fc76e14847cf2cec0ad4c05500bb70b70bfde48
5.	41.59.201.132	Miner:Linux/CoinMiner.99dbe0da	224716b23ba31c2fa60382dd9efb2bd6cbe878e1c827292371053fc664d76abe
6.	41.59.201.7	trojan.multiverze/vsnw01j24	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
7.	213.248.191.157	Trojan.Linux.GenericKD.54430	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
8.	16.79.13.69	Tool.Linux.BtcMine.9999	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8
9.	187.102.48.229	trojan.jggty/malxmr	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
10.	41.59.203.60	Trojan[downloader]:Win/Wacatac.B9nj	5b9210db87cfb74d5a953470ac82b04621cf663632b8f37a000f2aa88f103869

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **86,535** web attacks compared to last week which was **35,919.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 24th of August to 30th of August, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	197.250.227.237	/
2.	64.39.106.28	/wp-login.php
3.	64.39.106.27	/login
4.	64.39.106.107	/wp-login.php?action=lostpassword
5.	64.39.106.89	/login/
6.	64.39.106.126	/news/

7.	185.177.72.144	/favicon.ico
8.	64.39.106.82	/admin/config.php
9.	64.39.106.33	/accounting/control/main
10.	185.177.72.9	/q79w_38jg__.shtml

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **4,774** ICS attacks compared to last week which was **4,469.**

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 24th of August to 30th of August, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	77.83.240.70	kamstrup_protocol	1025
2.	165.154.129.151	guardian_ast	10001
3.	165.154.172.88	snmp	161
4.	3.132.23.201	IEC104	2404
5.	3.143.33.63	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.