	TZ-CERT HONEYPOTS WEEKLY REPORT **Period:** 07th of September to 13th of September, 2025 **Report No.:** TZ-CERT/WRHP/2025/36

1. NETWORK ATTACKS

A total of **1,343,294** attacks have been recorded compared to last week's **1,336,070** 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.	103.219.204.122	Ubuntu	admin
2.	185.4.30.93	root	(empty)
3.	45.159.112.17	user	123456
4.	185.116.161.213	admin	password
5.	45.159.112.142	linuxadmin	12345
6.	49.249.61.249	system	1234
7.	37.111.53.110	oracle	P@ssw0rd
8.	103.119.82.242	tomcat	password
9.	148.72.158.192	bigdata	123456789
10.	119.30.85.122	redis	Admin@123

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 **584,382** malicious software distributed, compared to last week in which was **447,986.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.60	Script.Troj.multiverze.v	d46555af1173d22f07c37ef9c1e0e74fd68db022f2b6fb3ab5388d2c5bc6a98e
2.	41.59.201.7	Trojan.Linux.Generic.DD49E	229496b55d0668a40fe3d969ba4e942dc2c2fd7452b3d6f79c6beb0db631dc12
3.	41.59.201.132	Tool.Linux.BtcMine.9999	89782d8142297907c9962eebdae29c28df86805a99f38a683ab55c8fa1596dd8

4.	41.59.211.41	HackTool/Linux.BitCoinMiner.a	ee7a31fb0d3c29ca435f08fd147a434c6db921b69d32c8894539a8199b0b15c0
5.	41.59.149.87	Trojan.Linux.GenericKD.54426	d6e0eb28cfe1b224f061eff0581091dac985516c78d222f4921587d2ec612010
6.	41.59.149.141	HEUR:Trojan-Downloader.Shell.Agent.p	6ecab5745b1c9be448cb2689e230d898b4886361160215596474050d0298be43
7.	195.175.200.238	Trojan[downloader]:Linux/Agent.p	88ad168cd9ba2d85e85504a20f569a81ea0d207cd5ca22bc926d416392f19486
8.	118.70.182.169	Linux/TrojanDownloader.SH.ASX	275a76f97d7a64f36bc6d8c62052d9b1ab9b94f5b4263f2c4f6636468f51a0c7
9.	41.47.78.7	TrojanDownloader/Linux.Shell.ad	88ad168cd9ba2d85e85504a20f569a81ea0d207cd5ca22bc926d416392f19486
10.	190.75.46.229	Shell.trojan.shell	6ecab5745b1c9be448cb2689e230d898b4886361160215596474050d0298be43

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **24,118** web attacks compared to last week which was **70,915.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 07th of September to 13th of September, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	139.87.112.115	/
2.	139.87.113.246	/manager/
3.	152.42.193.69	/.git/config
4.	139.87.112.100	/login
5.	91.224.92.17	/admin/config.php
6.	173.231.185.164	/favicon.ico

7.	45.148.10.243	/sysmgmt/2015/bmc/info
8.	159.223.70.170	/robots.txt
9.	213.136.70.135	/.env
10.	4.225.223.48	/boaform/admin/formLogin

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **8,306** ICS attacks compared to last week which was **3,728.**

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 07th of September to 13th of September, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	213.136.70.135	kamstrup_ management_protocol	50100
2.	77.83.240.70	guardian_ast	10001
3.	165.154.135.215	kamstrup_protocol	1025
4.	3.131.215.38	IEC104	2404
5.	3.130.96.91	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.