TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 20th of July to 26th of July, 2025
Report No.: TZ-CERT/WRHP/2025/29

1. NETWORK ATTACKS

A total of **107,067** attacks have been recorded compared to last week's **152,454** 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.	45.144.29.201	(empty)	111111
4.	185.246.128.133	user	adminHW
5.	193.105.134.95	guest	(empty)
6.	183.241.252.64	ftpuser	admin123
7.	179.43.189.98	pi	password
8.	196.251.88.103	git	eve
9.	41.78.73.146	solana	1234
10.	170.64.185.177	ubuntu	12345

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 **127,249** malicious software distributed, compared to last week in which was **102,767.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	trojan.jdobu/vsntgl25	c577132e0175fc3d6ed6fb880b0ddae6b60266db1f19d3b5974237d867ff7484
2.	101.50.76.8	miner.okrub/r002c0dgi25	9557bc559f728571b23040b453b896c359b4b914b9aa87db61178663669e1e9d
3.	196.202.22.211	miner.jkrjv	a79c55976c27bc471f3599e781d4f355645390705ea3f3e9c6fd504eb4957fc6

4.	41.111.234.130	HackTool/Linux.BitCoinMiner.a	b158697f5166889c4793ddca63f099a332ed705e7c62c0ed795a5686e4a1bcef
5.	196.203.207.238	miner.oferj/r002c0dgm25	c14567815527c56614ce826efb5c062a620af7733dec486d331b2e4b471c7b3c
6.	41.38.23.74	miner.snaui/r06ec0dgh25	f4661f6ee571fadbbb0dcd7371bd047d50a4c751dd849836a1290da1348004b2
7.	41.169.97.195	trojan.ajkwl/r002c0dgn25	62b3d8920605106b3c793bceedd7bf5e35a61d8c01f0cac6b8496e033cd6792a
8.	41.160.241.84	Trojan:Linux/CoinMiner!rfn	a87ffe7c1c6be9d22ab8cc96b83fc52ebed8b8d4f424ff46cb366fda9ba269d2
9.	41.203.215.119	trojan.alevaul/shell	783adb7ad6b16fe9818f3e6d48b937c3ca1994ef24e50865282eeedeab7e0d59
10.	202.124.150.21	trojan.mirai/gafgyt	d98f7aaa9e2aa30f86d5f7c88bc2e895bee6adeebc6d87a904bd28e6f9e01810

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,646** web attacks compared to last week which was **3,137.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th of July to 26th of July, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	167.71.208.126	/
2.	185.177.72.210	/.env
3.	13.39.112.85	/cgi-bin/luci/;stok=/locale
4.	141.98.11.152	/admin/config.php
5.	91.224.92.17	/favicon.ico
6.	149.50.96.114	/.git/config

7.	185.177.72.204	/logon.htm
8.	204.76.203.219	/robots.txt
9.	149.50.96.5	/boaform/admin/formLogin
10.	173.231.185.164	/_profiler/phpinfo

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,407** ICS attacks compared to last week which was **1,686.**

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 20th of July to 26th of July, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	118.193.36.63	kamstrup_protocol	1025
2.	165.154.43.179	guardian_ast	10001
3.	147.182.169.193	IEC104	2404
4.	167.71.147.245	kamstrup_management_protocol	50100
5.	13.39.112.85	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.