TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 13th of July to 19th of July, 2025
Report No.: TZ-CERT/WRHP/2025/28

1. NETWORK ATTACKS

A total of **152,454** attacks have been recorded compared to last week's **231,522** 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	admin
2.	196.251.88.103	admin	123456
3.	149.28.62.29	345gs5662d34	3245gs5662d34
4.	193.105.134.95	(empty)	345gs5662d34
5.	185.246.128.133	guest	password
6.	179.43.189.98	user	12345678
7.	207.167.66.226	ubuntu	1234567890
8.	59.127.79.125	ubnt	FattMan1234567890
9.	51.161.8.48	admin1	123456789
10.	185.93.89.118	support	(empty)

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 **102,767** malicious software distributed, compared to last week in which was **120,626.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.76.190	miner.okrub/r002c0dgi25	9557bc559f728571b23040b453b896c359b4b914b9aa87db6117866366 9e1e9d
2.	110.49.3.16	Trojan.Linux.GenericKD.52491	f8bbe4d65cb09dc3158a62926b1fda06549770ba1063accf12ed43f97c1ec4c7
3.	101.50.76.8	miner.jlerq/r002c0dg625	0d58ee0cd46d5908f31ba415f2e006c1bb0215b0ecdc27dd2b3afa74799e17bd

4.	62.210.80.69	Riskware.Linux.BitCoinMiner.1!c	b158697f5166889c4793ddca63f099a332ed705e7c62c0ed795a5686e4a1bcef
5.	119.83.15.227	downloader.mirai/bash	e773f7895f142b7e56f2f89a73edca9ae0963168ee8b079b6630944e9cf24010
6.	181.66.181.214	Miner:Multi/XMRig	1bffd7c3966df6d50a91f5b181ba6bb68d0eeff2fc9c7fbb004d74e429999af3
7.	196.202.71.89	downloader.medusa/shell	9a4747fb4ca166cf3ba048b21b377a4a0748d0b0d388a3f183f9b9d14a69c00a
8.	200.93.70.101	miner.snaui/r06ec0dgh25	f4661f6ee571fadbbb0dcd7371bd047d50a4c751dd849836a1290da1348004b2
9.	37.106.132.199	HackTool/Linux.BitCoinMiner.a	ceb8e519abfdba1a6487e10f7994445275e84e6f1c09ddfb44f8f24da99b13b0
10.	103.22.99.242	Miner:Multi/XmrigGo.SY	306c4e975edd4a95ae67c669cac871c233a5a7dd6591afa963b79304decc45ed

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,137** web attacks compared to last week which was **2,975.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 13th of July to 19th of July, 2025, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	157.230.60.129	/
2.	149.50.96.5	/.env
3.	93.123.109.152	/favicon.ico
4.	91.224.92.17	/cgi-bin/luci/;stok=/locale
5.	204.76.203.219	/robots.txt
6.	165.22.99.117	/.git/config

7.	78.153.140.203	/SDK/webLanguage
8.	45.194.66.7	/logon.htm
9.	149.50.96.114	/page/style/index.css
10.	89.42.231.140	/bapply.cgi

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,686** ICS attacks compared to last week which was **1,876.**

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 13th of July to 19th of July, 2025, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.173.74	kamstrup_protocol	1025
2.	161.97.160.103	kamstrup_management_protocol	50100
3.	45.82.78.254	guardian_ast	10001
4.	198.58.109.185	snmp	161
5.	207.90.244.26	IEC104	2404

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.