TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 7th of July, 2024 to 13th of July, 2024
Report No.: TZ-CERT/WRHP/2024/29

1. NETWORK ATTACKS

A total of **369,105** attacks have been recorded compared to last week's **199,152** 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.	135.181.96.118	root	345gs5662d34
2.	162.254.168.226	345gs5662d34	123456
3.	188.208.218.104	admin	admin
4.	45.165.80.4	ubuntu	(empty)
5.	183.178.93.162	user	1234
6.	192.254.104.68	test	password
7.	186.69.241.34	deploy	ubnt
8.	183.81.169.238	postgres	eve
9.	170.64.234.21	git	12345
10.	216.238.81.205	(empty)	12345678

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 **181,055** malicious software distributed, compared to last week in which was **28,595.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.93.63.66	downloader.medusa/shell	ea72b85f6413ab7c99c3a35f7f5d7d65707204c5910b2d9a7dd65a7b44ee272d
2.	196.202.11.60	trojan.hajime/mirai	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
3.	116.98.253.15	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

4.	95.65.217.72	Trojan.Linux.GenericKD.7949	298fbd37bd095c2fb15cf2eb742be22ba2679027f692e8bf25e392273844259c
5.	41.139.135.161	Trojan.Linux.GenericKD.7949	3e6661d8c7c86d181f5f5176b56e241d2de813e8bb53bc66e37479cbe2959327
6.	78.189.205.197	trojan.genericrxss/r002c0pjf23	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00
7.	88.248.28.178	trojan.r002c0pfh24	aa85190274311673a61039d434c6b30a0f694ce645a0340f0c11424d0eff8f87
8.	41.203.56.193	Trojan.Linux.GenericKD.7949	b14212857fe74349571dc653447dd59ff5938a768a65f90a3d4d653b669f8c83
9.	187.56.248.5	miner.r002c0dga24/woltr	1e6cf26fcd119c9fc97766370f2748f9122ad35b7d8d2ebcf7b8295930411a94
10.	41.33.89.58	miner.gafin/r002c0dga24	56571760676fa0d8a1807f9fee66c71f2eb1b71556aa3785ff327274f4c99464

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **10,518** web attacks compared to last week which was **4,003.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 7th of July, 2024 to 13th of July, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	35.180.229.8	/
2.	173.231.184.125	/admin/config.php
3.	157.173.195.59	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	141.98.83.197	/favicon.ico
5.	92.249.48.202	/.env

6.	157.245.206.84	/recordings/index.php
7.	185.191.126.213	/a2billing/admin/Public/index.php
8.	45.15.18.72	/robots.txt
9.	111.7.96.156	/logon.htm
10.	45.148.10.174	/.git/config

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,909** ICS attacks compared to last week which was **1,640.**

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 7th of July, 2024 to 13th of July, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	152.32.151.128	IEC104	2404
2.	165.154.118.9	kamstrup_management_protocol	1025
3.	101.36.108.134	kamstrup_protocol	10001
4.	165.154.41.232	guardian_ast	501
5.	137.184.30.28	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.