TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 30th of June, 2024 to 6th of July, 2024
Report No.: TZ-CERT/WRHP/2024/28

1. NETWORK ATTACKS

A total of **199,152** attacks have been recorded compared to last week's **309,709** 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.	162.254.168.226	root	12345678
2.	188.208.218.104	admin	guest
3.	186.69.241.34	mysql	123admin
4.	45.165.80.4	guest	123qwe!@#
5.	192.254.104.68	sa	root
6.	185.246.128.133	ubuntu	password
7.	193.105.134.95	user	abc123
8.	41.78.74.32	ftpuser	(empty)
9.	92.118.39.239	(empty)	P@ssw0rd!
10.	183.178.93.162	useradmin	666666

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 **28,595** malicious software distributed, compared to last week in which was **59,051.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	92.98.175.76	BASH/Dloader.AAN!tr.dldr	7c2339507fd4fd4eb3a8acbf0a69bd9b781cc17b243610e392f5d0d2fd1a142d
2.	196.202.11.60	trojan.xorddos/ddos	f5685335e0d53d5900783ee6c2bb60071b91030f55b0e92eb2fea7e26d65f9a0
3.	176.29.241.170	ELF/Xorddos.D!tr	38904b38a2bc7279979aaec44afbf42c80e296283a85913cf8fd473baf9df0d8

4.	36.77.46.26	CL.Downloader!gen277	528be0850c47f0d60c4210cc85437817458de3f0ba62c62235c7e762300d5e85
5.	196.219.151.219	Linux/Miner.ABF!tr	9f50ff1eb3f4d67a685791f56e38a9ec1d7368b1f16e42b603857672a3f448cf
6.	95.25.53.184	Adware/Miner	a0a778378af022f34aca2242729b9491aabb24662626226a29ef8e7d5f548bd7
7.	141.98.83.197	Trojan:Linux/Multiverze	c4dde7ac5bba14c079b514d319ad988eeb62405f91889e87321d0d06cea935a0
8.	117.211.8.92	Adware/Miner	62ae36274d9e33b704ce1485952cb76dea26dd84a6bf18c870db21ae1c3b7528
9.	5.238.239.239	RiskTool.Linux.dyj	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
10.	202.152.138.8	Trojan:Linux/CoinMiner	f02db168deea23fc07f2410dfe79663b78c9b82e4340535934feaa5d639bc4db

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,003** web attacks compared to last week which was **2,722.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 30th of June, 2024 to 6th of July 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	15.237.40.229	/
2.	173.231.184.125	/admin/config.php
3.	66.249.72.105	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	141.98.83.197	/robots.txt
5.	45.148.10.174	/.env

6.	66.249.72.107	/favicon.ico
7.	66.249.72.106	/logon.htm
8.	41.78.73.146	/a2billing/admin/Public/index.php
9.	41.78.74.32	/recordings/index.php
10.	66.249.64.105	/admin/assets/js/views/login.js

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,640** ICS attacks compared to last week which was **1,589.**

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 30th of June, 2024 to 6th of July 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.227.31.168	guardian_ast	2404
2.	13.38.26.129	IEC104	1025
3.	207.90.244.17	kamstrup_management_protocol	10001
4.	172.232.194.218	kamstrup_protocol	501
5.	172.232.195.184	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.