TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 23rd of June, 2024 to 29th of June, 2024
Report No.: TZ-CERT/WRHP/2024/27

1. NETWORK ATTACKS

A total of **309,709** attacks have been recorded compared to last week's **288,834** 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	888888
2.	186.69.241.34	Admin	guest
3.	45.165.80.4	mysql	admin123
4.	125.27.179.27	guest	123qwe!@#
5.	183.81.169.238	hikvision	root
6.	185.246.128.133	oracle	password
7.	164.163.98.28	user	abc123
8.	193.105.134.95	ftpuser	(empty)
9.	188.208.218.104	(empty)	P@ssw0rd!
10.	41.78.73.146	postgres	support

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 **59,051** malicious software distributed, compared to last week in which was **18,103.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	117.141.112.242	BASH/Dloader.AAN!tr.dldr	7c2339507fd4fd4eb3a8acbf0a69bd9b781cc17b243610e392f5d0d2fd1a142d
2.	114.189.112.237	trojan.xorddos/ddos	f5685335e0d53d5900783ee6c2bb60071b91030f55b0e92eb2fea7e26d65f9a0
3.	196.219.186.26	ELF/Xorddos.D!tr	38904b38a2bc7279979aaec44afbf42c80e296283a85913cf8fd473baf9df0d8

4.	183.82.118.232	CL.Downloader!gen277	528be0850c47f0d60c4210cc85437817458de3f0ba62c62235c7e762300d5e85
5.	102.22.142.254	Linux/Miner.ABF!tr	9f50ff1eb3f4d67a685791f56e38a9ec1d7368b1f16e42b603857672a3f448cf
6.	89.108.156.18	Adware/Miner	a0a778378af022f34aca2242729b9491aabb24662626226a29ef8e7d5f548bd7
7.	196.219.0.170	Trojan:Linux/Multiverze	c4dde7ac5bba14c079b514d319ad988eeb62405f91889e87321d0d06cea935a0
8.	125.160.86.1	Adware/Miner	a843ac9c087f399fbf8ef10fec872a732c9cf97c2cd249566a6133a2cebdc0c1
9.	91.	RiskTool.Linux.dyj	209acfa3624855145e9dd70fa9262f43cf0ee7d794a7eeec8b18ca691eef10b3
10.	87.225.105.217	Trojan:Linux/CoinMiner	88dc89bf303026c3ea273d879148e308a503cb211538f4cc47b667cf9f43bebb

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,722** web attacks compared to last week which was **2,149.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 23rd of June, 2024 to 29th of June 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.184.125	/
2.	186.233.181.166	/admin/config.php
3.	141.98.83.197	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	66.249.72.105	/recordings/index.php
5.	185.224.128.43	/robots.txt

6.	66.249.72.106	/.env
7.	66.249.64.98	/a2billing/admin/Public/index.php
8.	41.78.73.146	/recordings/index.php
9.	66.249.64.98	/favicon.ico
10.	186.209.106.97	/?XDEBUG_SESSION_START=phpstorm

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,589** ICS attacks compared to last week which was **1,850.**

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 23rd of June, 2024 to 29th of June 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	118.193.56.235	guardian_ast	2404
2.	152.32.225.108	IEC104	1025
3.	172.232.194.194	kamstrup_management_protocol	10001
4.	172.232.206.125	kamstrup_protocol	501
5.	172.232.209.138	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.