TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 16th of June, 2024 to 22nd of June, 2024
Report No.: TZ-CERT/WRHP/2024/26

1. NETWORK ATTACKS

A total of **288,834** attacks have been recorded compared to last week's **144,533** 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	3245gs5662d34
2.	125.27.179.27	admin	345gs5662d34
3.	45.165.80.4	ADMIN	123456
4.	186.69.241.34	guest	admin
5.	183.81.169.238	hikvision	root
6.	185.246.128.133	wwwroot	password
7.	121.123.29.141	user	xc3511
8.	138.68.71.46	ubnt	(empty)
9.	164.90.213.232	(empty)	hikvision
10.	193.105.134.95	amanda	swsbzkgn

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 **18,103** malicious software distributed, compared to last week in which was **167,904.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	122.165.53.80	ELF/Agent.MKVM!tr	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
2.	202.163.75.19	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
3.	212.154.196.22	ELF/Xorddos.D!tr	98e53e2d11d0aee17be3fe4fa3a0159adef6ea109f01754b345f7567c92ebebb

4.	119.93.243.188	Exploit:Linux/Multiverze	3e6661d8c7c86d181f5f5176b56e241d2de813e8bb53bc66e37479cbe2959327
5.	185.246.128.133	Linux/Miner.ABF!tr	9f50ff1eb3f4d67a685791f56e38a9ec1d7368b1f16e42b603857672a3f448cf
6.	182.253.139.216	Adware/Miner	a0a778378af022f34aca2242729b9491aabb24662626226a29ef8e7d5f548bd7
7.	45.148.10.174	Trojan:Linux/Multiverze	c4dde7ac5bba14c079b514d319ad988eeb62405f91889e87321d0d06cea935a0
8.	141.98.83.197	Adware/Miner	a843ac9c087f399fbf8ef10fec872a732c9cf97c2cd249566a6133a2cebdc0c1
9.	87.98.235.199	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 **2,149** web attacks compared to last week which was **3,687.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th of June, 2024 to 22nd of June 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	173.231.184.125	/
2.	65.0.138.41	/admin/config.php
3.	210.207.236.41	/admin/config.php?password%5B0%5D=ZIZO&username=admin
4.	185.191.126.213	/favicon.ico
5.	185.224.128.43	/.env

6.	78.153.140.37	/robots.txt
7.	169.255.243.12	/a2billing/admin/Public/index.php
8.	41.78.73.146	/recordings/index.php
9.	165.22.96.132	/favicon.ico?1528612569
10.	117.50.187.153	//help/

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **1,850** ICS attacks compared to last week which was **254.**

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 16th of June, 2024 to 22nd of June 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	87.98.235.199	guardian_ast	10001
2.	24.199.80.34	IEC104	2404
3.	147.182.225.86	kamstrup_management_protocol	50100
4.	185.165.191.26	kamstrup_protocol	1025
5.	147.182.202.179	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.