TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 2nd of June, 2024 to 8th of June, 2024
Report No.: TZ-CERT/WRHP/2024/23

1. NETWORK ATTACKS

A total of **2,486,240** attacks have been recorded compared to last week's **10,881,686** 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.	186.69.241.34	root	123
2.	198.50.219.188	345gs5662d34	345gs5662d34
3.	45.165.80.4	shcasii	123456
4.	186.67.248.6	jsalt2024	P@ssw0rd2018
5.	193.105.134.95	zhuang	Git123
6.	185.246.128.133	jenkins	root!@#
7.	93.120.240.202	xihang	AAAaaa111
8.	190.57.141.122	szher	Toor123
9.	154.68.39.6	oracle	Covid19@2023
10.	61.7.240.180	digital	M45uys51!

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 **273,406** malicious software distributed, compared to last week in which was **279,797.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
2.	41.59.201.7	trojan.hajime/mirai	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
3.	41.59.196.23	trojan.hajime/mirai	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	41.59.114.20	trojan.	47b268c21591069bfe4099833ad66b8138a53ab2dcb866e040d466aee1f8624c
5.	189.203.180.54	trojan.	6869ce81729acda83597601eb7c89c0bdda23d41bd5fe6900256dfb389a9bf47
6.	41.33.169.57	trojan.r002c0pf524	77ccd5ae0a102102b1c2032ff7f1fa8cc2f1069276f964210e644e1b21d8dd1f
7.	41.59.203.60	trojan.	9123e5c0930c4f86d8844185ad9e7bb3d616581660402ba047527966bdfaab9f
8.	41.59.230.50	miner.ahqvw/r002c0df824	a843ac9c087f399fbf8ef10fec872a732c9cf97c2cd249566a6133a2cebdc0c1
9.	88.215.183.102	miner.r002c0df824/vvhkw	88dc89bf303026c3ea273d879148e308a503cb211538f4cc47b667cf9f43bebb
10.	41.59.128.209	miner.mewnn/r002c0df824	8fc5d13238daba3a4986d674ad885f81850c67000c7f4f57df707f5d810ad241

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,687** web attacks compared to last week which was **12,778.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 2nd of June, 2024 to 8th 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	/users/sign_in
3.	210.207.236.41	/favicon.ico
4.	185.191.126.213	/wp-login.php
5.	185.224.128.43	/admin/config.php
6.	78.153.140.37	/41.59.85.216/.env

7.	169.255.243.12	/.env
8.	41.78.73.146	/robots.txt
9.	165.22.96.132	/cgi-bin/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/.%2e/bin/sh
10.	117.50.187.153	/admin/config.php?password%5B0%5D=ZIZO&username=admin

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,894** ICS attacks compared to last week which was **2,681.**

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 2nd of June, 2024 to 8th of June 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.206.204	amstrup_protocol	1025
2.	35.187.125.4	IEC104	2404
3.	165.154.135.215	guardian_ast	10001
4.	45.79.58.221	kamstrup_management_protocol	50100
5.	35.180.129.176	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.