TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 12th of May, 2024 to 18th of May, 2024
Report No.: TZ-CERT/WRHP/2024/20

1. NETWORK ATTACKS

A total of **214,078** attacks have been recorded compared to last week's **106,469** 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.	193.105.134.95	root	345gs5662d34
2.	186.224.22.90	admin	3245gs5662d34
3.	52.200.29.169	user	admin
4.	185.246.128.133	test	123456
5.	124.122.58.14	guest	password
6.	64.227.138.66	support	1234
7.	143.244.134.125	345gs5662d34	12345678
8.	110.177.146.38	ubuntu	0000
9.	139.59.12.32	ubnt	root
10.	161.35.235.140	postgres	(empty)

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 **289,038** malicious software distributed, compared to last week in which was **282,735.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	27.73.245.174	trojan.hajime/mirai	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0
2.	176.118.242.31	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	41.59.211.41	trojan.hajime/mirai	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

4.	41.59.196.23	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	41.59.203.60	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	41.59.230.50	trojan.malxmr/usblec24	d16bffbd3ba31504aea1fc01e66e29ad5927830ea5e2cc49369e82a7c68ec5c0
7.	113.28.192.112	miner.	062ba629c7b2b914b289c8da0573c179fe86f2cb1f70a31f9a1400d563c3042a
8.	41.59.194.240	trojan.	77ccd5ae0a102102b1c2032ff7f1fa8cc2f1069276f964210e644e1b21d8dd1f
9.	41.59.37.138	trojan.multiverze/usble924	7c4d16ae0e92dfc65fde6e700929fefaaf4a42f0e4c6cf6996d317940d3859c1
10.	89.147.240.19	Linux/Dldr-VN	6d2a6ff8e81b711a19a938a97391bfdaf33de3d7e4288c8aeebdce1b9ad608df

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **21,071** web attacks compared to last week which was **6,420.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 12th of May, 2024 to 18th of May, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	128.199.137.235	/wp-login.php
2.	185.203.122.206	/xmlrpc.php
3.	195.154.47.99	/
4.	92.25.246.207	/FyEKjr7NHyLNvlws
5.	179.43.188.110	/img/tomcat.png
6.	47.243.24.76	/users/sign_in

7.	92.118.39.120	/bitnami.css
8.	78.153.140.37	/favicon.ico
9.	185.224.128.43	/index.jsp
10.	179.43.188.106	/.env

Table3: Top 10 web attacking IP

4. INDUSTRIAL CONTROL SYSTEMS(ICS) ATTACKS

During the week the sensors recorded a total of **2,229** ICS attacks compared to last week which was **2,295.**

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 12th of May, 2024 to 18th of May, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	13.39.112.85	kamstrup_protocol	10001
2.	165.227.110.45	guardian_ast	1025
3.	164.92.106.15	kamstrup_management_protocol	2404
4.	18.171.242.21	IEC104	50100
5.	147.182.225.86	kamstrup_protocol	16

Table3: 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.