TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 19th of May, 2024 to 25th of May, 2024
Report No.: TZ-CERT/WRHP/2024/21

1. NETWORK ATTACKS

A total of **4,757,465** attacks have been recorded compared to last week's **214,078** 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.	52.200.29.169	345gs5662d34	3245gs5662d34
3.	45.165.80.4	git	345gs5662d34
4.	186.67.248.6	oracle	123456
5.	143.255.140.129	shcasii	Git123
6.	93.120.240.202	xihang	Covid19@2023
7.	190.181.4.12	lixinyu	P@ssw0rd2018
8.	201.81.240.66	es	root!@#
9.	72.206.88.130	zhuang	Administrator
10.	61.83.148.111	digital	jsalt2024

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 **348,280** malicious software distributed, compared to last week in which was **289,038.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	41.59.230.50	ELF/Xorddos.AB!tr	05ed208e50db849510bf9c89b770a0b7b9097ea5b48c8a7ee7ee0c18af6f3385
3.	41.59.203.60	ELF/Xorddos.D!tr	ba76ffe8c2f466442077c70ed874b2459d677cece7d36cc71e2a8542c27f8c2b

4.	41.59.196.23	Trojan:Linux/Multiverze	00deea7003eef2f30f2c84d1497a42c1f375d802ddd17bde455d5fde2a63631f
5.	186.24.11.163	Trojan:Linux/Multiverze	3974a1757c786c61c5cec40d6f3af66aec799459cc51af15dca88ac3c927115d
6.	103.231.163.21	Linux/Miner.ABF!tr	3c2f023d4ae1ca8aa6719d66ae1310914a74b5cf552e9f59883673ba24f067cd
7.	193.107.25.30	Adware/Miner	562b46ab24e657a837f5bdf84cbe91190aac46722c2463183e6d680b836a03f0
8.	122.247.242.33	Trojan:Linux/Multiverze	6168f5d053f4c3d413327947c37b927a759b316d68ac341908695879edcda246
9.	41.59.37.37	Adware/Miner	6f922abf3efc96d286a432e6bfdef73a44a6f4257bc9f36f460a57959180e49a
10.	41.32.181.34	Trojan:Linux/CoinMiner	a728692cf481ed612a35421967a9a499bf1b74f5771059002dfa42c413dda6c7

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **15,057** web attacks compared to last week which was **21,071.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th of May, 2024 to 25th of May, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	128.199.137.235	/wp-login.php
2.	83.147.52.42	/xmlrpc.php
3.	146.70.238.52	/
4.	83.147.52.37	/users/sign_in
5.	78.153.140.30	/favicon.ico
6.	185.224.128.43	/.env/
7.	78.153.140.37	/robots.txt

8.	185.191.126.213	/sitemap.xml
9.	51.89.51.67	/well-known.security.txt
10.	94.156.65.165	/admin/config.php

Table3: Top 10 web attacking IP

4. ICS (INDUSTRIAL CONTROL SYSTEMS) ATTACKS

During the week the sensors recorded a total of **2,681** ICS attacks compared to last week which was **2,229.**

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 19th of May, 2024 to 25th of May, 2024, are detailed

SN	ATTACKING IPS	TOP PROTOCOLS	TOP PORTS
1.	165.154.11.247	guardian_ast	10001
2.	167.248.133.50	IEC104	2404
3.	170.130.204.90	kamstrup_management_protocol	50100
4.	13.38.26.129	kamstrup_protocol	1025
5.	13.39.112.85	snmp	161

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.