TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 24th to 30th of September, 2023
Report No.: TZ-CERT/WRHP/2023/39

1. NETWORK ATTACKS

A total of **46,446** attacks have been recorded compared to last week **45,696** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	218.92.0.92	root	root
2.	139.59.21.27	admin	admin
3.	185.246.128.133	(empty)	1234
4.	193.105.134.95	guest	12345
5.	41.78.73.146	supervisor	password
6.	41.78.75.186	user	123456
7.	41.78.174.124	3comcso	(empty)
8.	14.194.10.253	test	user
9.	183.83.217.240	ubnt	1111
10.	135.125.240.201	Administrator	Daniel12

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of the above listed credentials and default ones. Use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **3,539** malicious software distributed compared to last week in which was **1,755.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	125.116.212.38	trojan.xorddos/ddos	fc4ad4bd76c21eeec817d7c227459fad6fd9f5e9c860242297f28977f775294e
2.	95.154.84.68	miner.	d6834b311280f9074b74d20ba2025e33e27460e197c132729e90c030dd893d18
3.	183.194.96.118	trojan.hajime/genericrxhy	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3

4.	222.243.156.40	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	41.78.174.124	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	41.78.75.186	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
7.	41.78.73.146	trojan.xorddos/ddos	dc2279cbb01ed9d179c6914f1a72ac2c1f9218920d90904b02d1f7781c10736c
8.	41.78.169.54	trojan.	ac80f84043b824c7e0b68dee20412bc51177d3c8db61f5aeea90655969e66507
9.	50.31.21.10	trojan.	8b3048631a205ae64d490f8805708192a200bae303f4d138338247e5a97380e8
10.	125.116.212.38	trojan.multiverze	ce98656dba7fcf84a3c583f23fe936cc5f9d0a8332bb298063322693c4f3cf9e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **6,580** web attacks compared to last week which was **688.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 24th to 30th September, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	3.108.1.218	/
2.	41.78.174.124	/users/sign_in
3.	41.78.169.54	/boaform/admin/formLogin
4.	41.78.73.146	/.env
5.	41.78.75.186	/robots.txt
6.	109.237.96.124	/favicon.ico

7.	109.237.96.251	/index.php
8.	45.156.129.12	/.git/config
9.	85.114.102.58	/Temporary_Listen_Addresses/
10.	139.59.74.136	/%00/

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with most common malware used in the world today. Monitoring of the listed IP address is advised and further to: -

4.1 Note that most of 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 counter act, including monitoring of the IPs in networks. Most likely the same resources might be used for further attacks.

4.2 Discourage usage of listed login resources (usernames and passwords) and consider deploying mechanisms to monitor login attempts.

4.3 Thoroughly check for suspicious files of hashes listed in **Table 2**.

4.4 Deploy Intrusion Detection System (IDS) and configure to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.