



TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 7th of April, 2024 to 13th of April, 2024
Report No.: TZ-CERT/WRHP/2024/15

1. NETWORK ATTACKS

A total of **275,120** attacks have been recorded compared to last week's **227,087** 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.	20.39.192.244	root	123456
2.	218.92.0.124	admin	345gs5662d34
3.	193.105.134.95	345gs5662d34	3245gs5662d34
4.	185.246.128.133	test	admin
5.	183.81.169.238	user	password
6.	103.155.193.186	ubnt	1234
7.	116.110.84.124	guest	12345
8.	170.64.220.63	Admin	root
9.	170.64.238.3	support	(empty)
10.	179.43.180.106	(empty)	0

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 **226,895** malicious software distributed, compared to last week in which was **47,775**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.201.7	downloader.bash/miraib	18e0f574bf11bc5e7de8c95b83c187649b2d87d74651e59d9c2aad53ac7bb7f1
2.	41.59.211.41	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	171.244.188.221	trojan.hajime/mirai	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	31.41.93.54	trojan.hajime/genericrxic	d5601202dff3017db238 145ff21857415f663031a ca9b3d534bec8991b12 179a
5.	41.59.114.92	trojan.	ea40ecec0b30982fbb16 62e67f97f0e9d6f43d2d5 87f2f588525fae683abea 73
6.	41.33.37.19	trojan.	6ef27a778205b4934461 5af4c6983ebe2ac8fe89 738eb44c202fdefb0fb40 cc9
7.	41.59.196.23	trojan.multiverze	72ce5b00ca4bfa0c18fc df03a15e5391a85d8130 0783626598fe7e022e0e c538
8.	186.223.210.72	HEUR:Trojan- Downloader.Shell.Agent.p	409e6be60a200711954 b03a747748ea87de175 6b2ad9e81fa6454598bd efb065
9.	111.61.77.241	Trojan.Linux.GenericKD.7 949	9623c860ea32daf38df7 70d354165d7c7802d33 7c8743c4288e3799ebc c8e0cd
10.	41.59.203.60	Trojan.Linux.GenericKD.4 0003689	a37fced60c901a743ae7 8ab761c0e96673e805b 90af39b76c09279db2c5 7ea5e

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,351** web attacks compared to last week which was **1,462**.

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 7th of April, 2024 to 13th of April, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	3.104.38.100	/
2.	146.19.24.28	/users/sign_in
3.	35.219.159.17	/oauth/token
4.	41.78.38.84	/favicon.ico
5.	50.114.115.247	/.env
6.	78.153.140.30	/robots.txt

7.	103.23.144.10	/1.php
8.	185.224.128.43	/info.php
9.	78.153.140.37	/bundle.js
10.	162.250.127.46	/files/

Table3: Top 10 web attacking IP

4. 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:

-
- 4.1 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.
- 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 it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.