



TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 10th March 2024 to 16th of March, 2024

Report No.: TZ-CERT/WRHP/2024/11

1. NETWORK ATTACKS

A total of **93,791** attacks have been recorded compared to last week's **86,154** 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.	185.246.128.133	root	admin
2.	193.105.134.95	user	p@ssw0rd
3.	121.123.29.141	debian	support
4.	41.78.38.142	supervisor	888888
5.	175.123.253.229	ubuntu	(empty)
6.	43.163.212.159	support	123admin
7.	213.109.202.127	postgres	1234567890
8.	41.78.73.146	admin	root
9.	43.130.246.180	mysql	default
10.	43.135.157.137	zabbix	tomcat

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 **10,514** malicious software distributed, compared to last week in which was **33,226**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	111.68.121.155	TrojanDownloader:Linux/Morila!MTB	acb409c544941061154005b4582cb4d1610ed0c0cf7f57fe02c305a275e1053f
2.	46.40.200.86	Backdoor:Win32/Berbew	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
3.	196.189.185.241	Trojan:Linux/Downldr.B!MTB	cb831b6d75c3e9ca356f2196e36bae3d069f19a8f7d2191e6fe7c43849d916fc

4.	182.48.204.173	Trojan:Linux/Downldr.B!M TB	d5601202dff3017db238 145ff21857415f663031a ca9b3d534bec8991b12 179a
5.	86.106.243.214	Linux/Downloader.p	078688efd30f25ff39d68 7e7a867ed9314cce33e 2fc7b0e8c9c54314a4d8 cf35
6.	59.98.111.98	DoS:Linux/Xorddos!pz	ea40ecec0b30982fbb16 62e67f97f0e9d6f43d2d5 87f2f588525fae683abea 73
7.	1.163.245.119	Trojan:Linux/Multiverze	8a20aea398f7452fdb51 e94661baa3a402da320 1c5d5edf191711c7c5e2 7b382
8.	212.83.8.81	HEUR:Trojan- Downloader.Shell.Agent.p	409e6be60a200711954 b03a747748ea87de175 6b2ad9e81fa6454598bd efb065
9.	103.153.180.171	Trojan:Linux/Multiverze	7901ea3019dcd61d891 3ba4f2cb37a5de33123b 4b58482c7a96d96660c 45a5a1

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,521** web attacks compared to last week which was **7,533**.

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 10th March 2024 to 16th of March, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	41.216.183.12	/
2.	63.251.106.21	/users/sign_in
3.	146.19.24.28	/admin/config.php?password%5B0%5D=ZIZO&userna me=admin
4.	41.78.75.186	/admin/config.php
5.	41.78.38.142	/favicon.ico
6.	41.78.73.146	/etc/passwd
7.	78.153.140.30	/bundle.js
8.	78.153.140.37	/files/

9.	83.97.73.245	/info.php
10.	103.183.121.244	/password.php

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.