TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 28th of April, 2024 to 4th of May, 2024
Report No.: TZ-CERT/WRHP/2024/18

1. NETWORK ATTACKS

A total of **129,163** attacks have been recorded compared to last week's **162,652** 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.	103.7.72.237	root	WindoW$
2.	193.105.134.95	administrator	P@ssw0rd!
3.	185.246.128.133	mysql	Zte521
4.	159.65.129.69	ftpuser	adminHW
5.	41.59.204.164	nginx	password
6.	139.59.44.183	flask	abc123456
7.	183.81.169.238	git	666666
8.	170.64.185.147	postgres	r00t
9.	41.78.73.146	unix	qwerty
10.	170.64.213.59	hadoop	admin

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 **343,722** malicious software distributed, compared to last week in which was **49,626.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.211.41	downloader.bash/miraib	abd882efdb9f24ef844af635472b6ecb2266a38604485271ce85a251b390ee31
2.	41.59.203.31	trojan.hajime/genericrxic	d68d85af59c7cfdf08f957b801888957bcc046ff258973c94e6337f719d9bf02
3.	41.59.211.144	Trojan:Linux/Downldr.B!MTB	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	196.202.26.79	HEUR:Trojan-Downloader.Shell.Agent.p	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
5.	41.79.199.36	Linux/XorDDos.c	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	41.59.196.23	trojan.	6ef27a778205b49344615af4c6983ebe2ac8fe89738eb44c202fdefb0fb40cc9
7.	41.59.114.100	trojan.multiverze	72ce5b00ca4bfa0c18fcdf03a15e5391a85d81300783626598fe7e022e0ec538
8.	41.59.203.60	HEUR:Trojan-Downloader.Shell.Agent.p	409e6be60a200711954b03a747748ea87de1756b2ad9e81fa6454598bdefb065
9.	41.59.106.47	Trojan.Gen.NPE	9623c860ea32daf38df770d354165d7c7802d337c8743c4288e3799ebcc8e0cd
10.	41.59.194.240	Linux/Dldr-VN	3d6af6bd2250678f3ba2fcf3d78087e9bba0f71986914c3cc5d497171f303311

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,658** web attacks compared to last week which was **1,315.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 28th of April, 2024 to 4th of May, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	162.244.210.85	/
2.	78.153.140.37	/users/sign_in
3.	185.117.225.252	/favicon.ico
4.	185.224.128.43	/.env
5.	203.55.81.13	/1.php
6.	78.153.140.30	/bundle.js

7.	159.223.65.82	/info.php
8.	146.19.24.28	/cgi-bin/orospucoc.cgi?user=messagebus&passwd=&cmd=15&system=dW5hbWUJLW0=
9.	191.243.12.201	/files/
10.	135.125.164.195	/form.html

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.