TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 4th February 2024 to 10th of February, 2024
Report No.: TZ-CERT/WRHP/2024/6

1. NETWORK ATTACKS

A total of **329,255** attacks have been recorded compared to last week's **235,290** 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	admin	user
3.	41.78.73.146	user	root
4.	45.90.12.212	ubnt	123456
5.	41.78.38.139	guest	(empty)
6.	218.92.0.93	default	1234
7.	62.210.66.53	support	123
8.	89.208.103.89	supervisor	12345
9.	111.231.19.61	test	ubnt
10.	142.171.30.130	uucp	1234567890

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 **495,403** malicious software distributed, compared to last week in which was **191,098.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	52.81.102.75	downloader.medusa/shell	100dde1bf937d211792774860145be271f9ec3c36e9d2d2ecde3ab781308404d
2.	41.78.64.250	HEUR:Trojan-DDoS.Linux.Xorddos.gen	a8f555d9e3c6919b3fa2809614fe60c235ea7fa435143865e68d501da63b1a21
3.	41.59.194.240	Trojan:Win32/Ditertag.A	ed6592ba14cd29f887196338a98a63560978d240bd9d89d7689a985fe92f7413

4.	41.93.57.66	Trojan.Gen.NPE	765289f938cc2bd64c9778dbabe048afa8ac3277a150c940d2730c14d24687b5
5.	138.122.92.14	Riskware/CoinMiner	c5cbbc98b9b0916ea3fb8360651e698fd4f56d97421d7bcb1839d12a77fa3784
6.	195.154.200.116	CL.Downloader!gen277	8a20aea398f7452fdb51e94661baa3a402da3201c5d5edf191711c7c5e27b382
7.	131.129.136.223	trojan.generica/r002c0pee21	aa4ae40d671a033f63cdd8e8f650c848eb91ddb46e3d9146a972555f40f2215b
8.	196.218.64.138	trojan.malxmr/uselvkh23	27d205dc183ea2fad0e55e10b206404be20908e39a74569ff99182d7326ed9c0
9.	1.53.161.204	trojan.multiverze/uselvk123	306f0c79ad9ee76e996556f909306fda5704b456d670aa9daeb54760b4b5e4f6
10.	41.93.63.66	trojan.genericrxss/r002c0pjf23	58944a1fbaeec105fa012d0dd6dc2d4982add9bf35c2873be1c188f6cf77d476

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **7,293** web attacks compared to last week which was **2,018.**

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

SN	ATTACKING IPS	TOP URI
1.	64.225.6.114	/
2.	146.19.24.23	/users/sign_in
3.	41.78.73.146	/.env
4.	63.251.106.21	/favicon.ico
5.	141.98.10.76	/boaform/admin/formLogin
6.	41.78.38.139	/admin/config.php

7.	175.132.151.230	/robots.txt
8.	78.153.140.37	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	93.123.39.227	/a2billing/admin/Public/index.php
10.	14.103.20.212	/?XDEBUG_SESSION_START=phpstorm

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.