TZ-CERT HONEYPOTS WEEKLY REPORT

Period: 7th January 2024 to 13th of January, 2024
Report No.: TZ-CERT/WRHP/2024/2

1. NETWORK ATTACKS

A total of **78,164** attacks have been recorded compared to last week **2,636** 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.	218.92.0.124	root	user
2.	185.246.128.133	admin	admin
3.	193.105.134.95	user	root
4.	89.208.103.89	(empty)	123456
5.	139.59.75.17	guest	1234
6.	41.78.73.146	ubnt	12345
7.	139.59.62.69	ubuntu	(empty)
8.	41.78.75.186	dev	password
9.	206.189.136.170	supervisor	ubnt
10.	46.19.139.138	uucp	AdminHW

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 **43,887** malicious software distributed, compared to last week in which was **4,351.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.194.240	downloader.medusa/shell	fef1d976e94d87fc8ebcacd50f46ce5061a380d9f59ccb69093c860bf509bf52
2.	41.59.201.7	trojan.mirai/sejyy	7f5ab956e704bd0787b9ad2ea47c60cf43c02c5c2c18b72edb467ed35281679f
3.	196.221.148.220	trojan.shell/bashdlod	3f9a4dc3e6bcc060d5f7693b58df0bf300d74ae86afb1507eef130f7b17cd9ee

4.	41.33.37.19	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
5.	196.229.23.19	trojan.xorddos/generica	87e0a05bc63eae251277053c7891e4d51ab3a257587b750076183c76a9472357
6.	212.46.20.90	trojan.xorddos/ddos	8a20aea398f7452fdb51e94661baa3a402da3201c5d5edf191711c7c5e27b382
7.	41.59.114.215	trojan.generica/r002c0pee21	aa4ae40d671a033f63cdd8e8f650c848eb91ddb46e3d9146a972555f40f2215b
8.	129.205.100.126	trojan.malxmr/uselvkh23	27d205dc183ea2fad0e55e10b206404be20908e39a74569ff99182d7326ed9c0
9.	103.78.12.160	trojan.multiverze/uselvk123	306f0c79ad9ee76e996556f909306fda5704b456d670aa9daeb54760b4b5e4f6
10.	196.188.51.244	trojan.genericrxss/r002c0pjf23	e89e1234fa7d5bbe565feabcaf5665ef3efccec50db7232da1eba6387a984877

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,255** web attacks compared to last week which was **1,309.**

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

SN	ATTACKING IPS	TOP URI
1.	112.74.15.7	/
2.	144.126.209.232	/users/sign_in
3.	82.66.148.35	/.env
4.	59.49.77.211	/boaform/admin/formLogin
5.	172.10.166.60	/favicon.ico
6.	182.233.39.14	/robots.txt

7.	212.253.79.136	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	103.190.29.157	/.git/config
9.	83.97.73.245	/?XDEBUG_SESSION_START=phpstorm
10.	112.74.15.7	/vendor/phpunit/phpunit/src/Util/PHP/eval-stdin.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.