TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 21st January 2024 to 27th of January, 2024
Report No.: TZ-CERT/WRHP/2024/4

1. NETWORK ATTACKS

A total of **77,766** attacks have been recorded compared to last week **19,092** 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.	199.192.24.235	(empty)	root
4.	170.64.155.31	user	123456
5.	41.78.38.139	guest	1234
6.	41.78.73.146	ubnt	(empty)
7.	111.43.19.99	supervisor	password
8.	170.64.210.198	Admin	adminHW
9.	170.64.206.27	vadmin	Xpon@Olt9417#
10.	167.71.61.117	oracle	SUGAR2AO41

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 **76,971** malicious software distributed, compared to last week in which was **18,548.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	52.81.102.75	ELF/Xorddos.D!tr	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	105.160.63.80	ELF/Xorddos.AB!tr	a8f555d9e3c6919b3fa2809614fe60c235ea7fa435143865e68d501da63b1a21
3.	41.59.194.240	Trojan:Win32/Ditertag.A	ed6592ba14cd29f887196338a98a63560978d240bd9d89d7689a985fe92f7413
4.	88.250.222.125	Trojan.Gen.NPE	765289f938cc2bd64c97

			78dbabe048afa8ac3277a150c940d2730c14d24687b5
5.	213.14.231.106	Riskware/CoinMiner	c5cbbc98b9b0916ea3fb8360651e698fd4f56d97421d7bcb1839d12a77fa3784
6.	41.59.114.244	trojan.xorddos/ddos	8a20aea398f7452fdb51e94661baa3a402da3201c5d5edf191711c7c5e27b382
7.	117.4.120.186	trojan.generica/r002c0pee21	aa4ae40d671a033f63cdd8e8f650c848eb91ddb46e3d9146a972555f40f2215b
8.	189.254.74.74	trojan.malxmr/uselvkh23	27d205dc183ea2fad0e55e10b206404be20908e39a74569ff99182d7326ed9c0
9.	168.187.12.125	trojan.multiverze/uselvk123	306f0c79ad9ee76e996556f909306fda5704b456d670aa9daeb54760b4b5e4f6
10.	201.216.219.169	trojan.genericrxss/r002c0pjf23	3f9a4dc3e6bcc060d5f7693b58df0bf300d74ae86afb1507eef130f7b17cd9ee

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,101** web attacks compared to last week which was **247.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 21st January 2024 to 27th of January, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	146.19.24.23	/
2.	41.78.38.139	/.env
3.	41.78.73.146	/users/sign_in
4.	36.99.136..136	/favicon.ico
5.	78.153.140.30	/boaform/admin/formLogin
6.	85.208.51.177	/robots.txt

7.	18.171.160.197	/actuator/gateway/routes
8.	41.78.73.146	/index.php?title=Special:CreateAccount&returnto=Main%20Page&returntoquery=printable%3Dyes
9.	18.171.184.9	/?XDEBUG_SESSION_START=phpstorm
10.	41.78.38.139	/+CSCOE+/logon.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.