TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 24th December to 30th of December, 2023
Report No.: TZ-CERT/WRHP/2023/52

1. NETWORK ATTACKS

A total of **103,359** attacks have been recorded compared to last week **56,331** 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	wwwroot	P@ssw0rd!!
3.	41.78.73.146	ftp	qwerty
4.	165.22.214.17	wordpress	admin123
5.	41.78.75.186	sa	Win1doW$
6.	170.64.202.140	telnet	12345678
7.	138.197.109.23	superadmin	(empty)
8.	170.64.154.138	mysql	abc123456
9.	170.64.210.122	splunk	tomcat
10.	170.64.131.214	ubuntu	anonymous

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 **43,748** malicious software distributed, compared to last week in which was **7,478.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	113.161.218.118	Linux/DDoS-BH	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
2.	183.149.223.124	ELF/Xorddos.AB!tr	57e9955208af9bc1035bd7cd2f7da1db19ea73857bea664375855f693a6280d8
3.	201.248.243.136	Riskware/CoinMiner	2d4af503d71c8d5ebedb020adea78e35bc37c5456dd15611f5e98c90cbb3d095

4.	196.249.224.30	Adware/Miner	3f41466bdd0a5dafbb95d699cc940d7ae37caaa032680f7eb6035aeb14e5618c
5.	196.117.99.242	trojan.xorddos/ddos	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	117.4.60.222	trojan.xorddos/generica	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
7.	196.191.120.250	Downloader	9c0a4a7150ab4d645c85eaab56b992694513c3a8cd5656fc7ca85f898f51c7e6
8.	187.237.166.165	Trojan:Linux/Downldr.AL!MTB	b927f9ff536db3dafbea0ec62c2581b3acc42da18fe6fc932be077e5e9036aaf
9.	27.72.56.50	trojan.generica/xorddos	d2dda52df6dc7681b6bc687732dff93f8292adaa8b1ae95eb1a31c80547240d5
10.	196.202.14.224	ELF/Generic.246192!tr	5d8aab2ce5b8ba8c7b102ddaa3c89ea3ed4426acce68a64f4b1c7711a5d38308

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,371** web attacks compared to last week which was **954.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 24th December to 30th December, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	42.192.53.183	/
2.	41.78.75.186	/users/sign_in
3.	78.153.140.30	/.env
4.	41.78.73.146	/favicon.ico
5.	78.153.140.37	/admin/config.php
6.	39.108.98.55	/robots.txt

7.	51.89.124.57	/boaform/admin/formLogin
8.	102.67.158.23	/?XDEBUG_SESSION_START=phpstorm
9.	185.224.128.191	/actuator/gateway/routes
10.	188.215.235.101	/admin/config.php?password%5B0%5D=ZIZO&username=admin

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.