TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 12th November to 18th of November, 2023
Report No.: TZ-CERT/WRHP/2023/46

1. NETWORK ATTACKS

A total of **91,448** attacks have been recorded compared to last week **39,914** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	157.90.237.167	root	root
2.	24.199.109.76	admin	12345678
3.	218.92.0.92	guest	@dm1n1$tr@t0r
4.	193.105.134.95	ftpuser	Admin001
5.	185.246.128.133	ubnt	adminHW
6.	143.110.252.11	Administrator	Pass1234
7.	2.56.247.174	postgres	P@ssw0rd!!
8.	41.78.75.186	sa	Qwerty
9.	170.64.191.152	centos	abc@@123
10.	41.78.73.146	wwwroot	Win1doW$

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and password be made to avoid use of the above listed credentials and default ones. Use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **31,007** malicious software distributed compared to last week in which was **31,161.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.249.224.30	trojan.xorddos/ddos	a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6daa3de3
2.	109.98.241.199	ELF/Xorddos.AB!tr	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
3.	122.165.58.59	Trojan:Script/Wacatac.B!ml	020f1fa6072108c79ed6f553f4f8b08e157bf17f9c260a76353300230fed09f0

4.	39.51.212.137	trojan.hajime/genericrxhy	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
5.	196.221.164.236	Trojan:Linux/Downldr.B!MTB	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	31.128.245.114	trojan.mirai/cryp	8127f8c730ffe7f767bec28b083dc7f1acd797399f712a201e991f39b9716b6f
7.	87.255.211.178	trojan.xorddos/ddos	0291de841b47fe19557c2c999ae131cd571eb61782a109b9ef5b4a4944b6e76d
8.	103.247.6.247	Mal/Generic-S	e91b36bc7495acbbeebfda1c6c3b17e8ea4bbcb42e85137f814377f482fa9fc6
9.	14.161.31.247	trojan.hajime/genericrxhy	b23b05b3520a231e7ac2b234bd23bc94852dcdcf14d771c4b5803cb494421c9b
10.	202.165.91.169	GenericRXHU-OQ!5377E8F2EBDB	c9f53c5a7971ce9053edf75583484635154ad09b791cfde914775d49045b1328

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,464** web attacks compared to last week which was **1,261.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 12th November to 18th of November, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	72.251.232.180	/
2.	41.78.75.186	/users/sign_in
3.	109.237.96.124	/admin/config.php
4.	146.190.157.181	/favicon.ico
5.	146.190.250.209	/admin/config.php?password%5B0%5D=ZIZO&username=admin

6.	170.64.194.137	/.env
7.	143.110.177.220	/core/misc/favicon.ico
8.	161.35.213.149	/a2billing/admin/Public/index.php
9.	165.227.45.170	/boaform/admin/formLogin
10.	64.227.174.207	/actuator/gateway/routes

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with 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 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 counter act, 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 to flag detection of attacks associated with list of resources provided especially the IP addresses and the web requests.