TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 3rd December to 9th of December, 2023
Report No.: TZ-CERT/WRHP/2023/49

1. NETWORK ATTACKS

A total of **70,129** attacks have been recorded compared to last week **140,817** 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.	218.92.0.124	root	user
2.	112.117.102.95	admin	admin
3.	193.105.134.95	user	root
4.	185.246.128.133	(empty)	123456
5.	170.64.204.103	guest	$V$RFV4rfv
6.	41.78.75.186	ubnt	1234
7.	41.78.73.146	administrator	password
8.	170.64.181.245	oracle	(empty)
9.	207.154.219.102	GET/HTTP/1.1	adminHW
10.	95.181.239.7	supervisor	12345

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 **18,514** malicious software distributed, compared to last week in which was **269,083.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.189.111.195	trojan.bash/miraib	1276e2b8c6b6eaa3b894dc0dc5d537c19b1d8a0e9a82943b364e1c2605e38ed8
2.	113.180.232.96	trojan.mirai/febn	a72ff45b5d33ae5cf878a0ee3e5a88c8780ced70c63307f4f4d3be968adaa3b3
3.	89.19.115.142	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
4.	112.12.0.110	trojan.xorddos/ddos	56e9e3c33348fc6068ed003a37ead4dc87248dc82c151b7fc35435f3f6faec95

5.	178.210.132.114	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
6.	185.253.224.60	trojan.xorddos/generica	0d5ba3cf3aa65d74cb6f4e90f107d2f43af373481b1a981b4f28605ef9c4c689
7.	130.211.54.158	trojan.xorddos/ddos	cc42731bf94ff321ee0d9c9085dde80e2ee5268d571b98594eafc5c799113cd5
8.	196.203.218.202	trojan.malxmr/uselvie23	0094c9465c7e996fad0b14db7e2b23132e8f1e114b22c98e0e265122a7507822
9.	183.62.9.254	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
10.	212.129.17.6	trojan.multiverze/uselvg223	9ac3924fa98c4788086eec79aad88a6e23d222f72cdf3a55d477cd87e9cb6402

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,107** web attacks compared to last week which was **4,221.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 3rd December to 9th of December, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	196.216.218.9	/
2.	72.251.232.180	/users/sign_in
3.	13.234.38.226	/admin/config.php
4.	206.189.86.47	/favicon.ico
5.	41.78.75.186	/boaform/admin/formLogin
6.	41.78.73.146	/admin/config.php?password%5B0%5D=ZIZO&username=admin
7.	47.106.35.122	/index.php/heartbeat
8.	8.140.201.183	/systembc/password.php
9.	31.7.58.42	/recordings/index.php
10.	117.132.188.20	/a2billing/admin/Public/index.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.