TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 9th to 15th of April, 2023
Report No.: TZ-CERT/WRHP/2023/15

1. NETWORK ATTACKS

A total of **221,144** attacks have been recorded compared to last week **250,531** 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.	77.93.239.114	root	admin
2.	104.194.11.254	admin	123456
3.	171.251.27.188	ubuntu	support
4.	193.105.134.95	support	password
5.	195.3.147.52	user	12345
6.	205.185.118.29	PlcmSplp	345gs5662d34
7.	116.110.83.99	guest	3245gs5662d34
8.	116.110.27.106	345gs5662d34	adminHW
9.	116.98.168.139	test	PlcmSplp
10.	171.251.19.213	oracle	RIP000

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 **171,123** malicious software distributed compared to last week in which was **182,858**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan.Gen.NPE	9bcd3a0bc51dbdfc7a0b249912644865c5711f191698d0f6590b6359174a6155
2.	41.72.61.245	Downloader.Trojan	af03cfb63f0c4dbca12eb24d1add9b8f17757309bc3d18a73a16fe1ee576915a
3.	41.59.211.41	Perl.Pircbot	2220783661db230d0808a5750060950688e2618d462ccbe07f54408154c227c1
4.	41.59.86.254	trojan.hajime/linux	a04ac6d98ad9893127

			83d4fe3456c53730b212c79a426fb215708b6c6daa3de3
5.	41.59.196.23	Trojan.GenericKD.50084125	b0984f01570b2b5502b8cfe0ed44f4294216b300c2cda485247588d2b29e55e74568324108
6.	41.93.57.66	trojan.linux	8c5e2b96cb61ebb3750f5be23fc9aca14d7ac97efb7d57afebd85472dcc8e015
7.	41.211.101.78	HEUR:Trojan-DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
8.	94.59.97.156	Trojan.Linux.Generic.246192	e6ce9937266d30a22c6aa5c48d818dba86491b1becf1fe0ca07b3de85d2d88ab
9.	41.226.178.111	Trojan.Win32.Eb.dqb	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946
10.	41.188.104.186	rojan.linux/xorddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,078** web attacks compared to last week which was **2,811**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 9th to 15th of April, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	121.173.126.140	/users/sign_in
3.	122.155.108.140	/adcr.nhn
4.	213.65.160.226	/boaform/admin/formLogin
5.	5.164.23.174	/recordings/

6.	84.187.8.212	//ajax.php?yokyok=ls
7.	109.237.96.124	/.env
8.	152.89.196.54	//rr.php?yokyok=ls
9.	109.237.96.251	/admin//modules/ajax.php
10.	119.29.170.96	/admin//modules/core/ajax.php

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.