TZ-CERT HONEYPOTS WEEKLY REPORT
**Period : ** 29th of January – 4th of February, 2023
Report No.: TZ-CERT/WRHP/2023/5

1. NETWORK ATTACKS

A total of **335,910** attacks have been recorded compared to last week **231,875** 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.	1.116.139.19	root	admin
2.	171.225.184.208	sa	password
3.	171.225.184.184	support	qwerty123456
4.	193.105.134.95	ubuntu	123456
5.	171.225.184.247	guest	666666
6.	91.121.172.204	user	RIP000
7.	195.3.147.52	ftpuser	default
8.	171.225.184.90	test	Win1doW$
9.	45.87.105.81	Administator	support
10.	171.225.184.112	3comcso	cameras

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 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 **964,783** malicious software distributed compared to last week in which was **122,450**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.203.31	Trojan Horse	c801a195cb85ddc6bfe5b95114a078b9be030d80cedeceba1e4c20d3858418aa
2.	196.41.222.98	Trojan.Generic.31654391	a0035ef408f06db49ada52f30fc42451689a1b1086759a373a05656353a14ead
3.	41.78.64.254	TrojWare.Script.TrojanDownloader.Agent.	c70ca8df777bfc5a77d06eb625a0e6d7afdcd563df02a2d16de95813ae717a31
4.	41.59.211.41	HEUR:Trojan-	db06a40d33db2416bcc

		Downloader.Shell.Agent.p	452736ad5ee7b4035c457b3f7d559b05ec200d6a8c7a5
5.	196.41.222.5	HEUR:Trojan-Downloader.Shell.Agent.bc	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
6.	41.59.86.254	Trojan.Linux.Generic.246192	a37b519f4146749aef1e3ff0d5a76ef4cf9659927a4a4db527e22309cc988cd0
7.	41.59.41.28	Linux.MiraiTrojan.Linux.GenericKD.40003689	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	41.77.26.121	Trojan.Linux.GenericKD.40003689	48409bbbe5559ec2eae71fcfd8dcdb5ebe7472ef864eabdcdca427660287e0fc
9.	118.122.217.142	HEUR:Trojan-DDoS.Linux.Xarcen.d	ed902957efb11382546f2cff80e5284832f7f53c4e2b82b9d181c1f3ef65513f
10.	41.59.203.192	Trojan.Win32.Eb.dqb	cdf16795ec6ea3857851ece799fbe687e0b646a3f555ebd34199a64500b705eb

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **9,247** web attacks compared to last week which was **4,032**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 29th of January – 4th of February, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	192.151.144.58	/
2.	45.148.119.152	//admin/config.php
3.	183.136.225.32	/users/sign_in
4.	72.251.235.155	/boaform/admin/formLogin
5.	179.43.177.242	/favicon.ico
6.	121.173.126.140	/admin/config.php

7.	103.77.188.30	/robots.txt
8.	109.237.96.124	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	193.32.162.159	/.env
10.	1.13.8.48	/adcr.nhn

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.