TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 5th of February –11th of February, 2023
Report No.: TZ-CERT/WRHP/2023/6

1. NETWORK ATTACKS

A total of **330,505** attacks have been recorded compared to last week 335,910 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.	183.134.6.42	root	admin
2.	171.225.185.9	admin	123456
3.	171.225.184.78	support	password
4.	171.225.185.108	guest	support
5.	193.105.134.95	user	PlcmSplp
6.	195.3.147.52	PlcmSplp	12345
7.	171.225.184.143	huawei	1234
8.	171.225.184.108	test	root
9.	206.189.130.33	ftp	Win1doW$
10.	206.189.130.33	www	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 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 **1,179,167** malicious software distributed compared to last week in which was **964,783**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.86.254	Trojan.Gen.NPE	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946
2.	41.59.211.41	Trojan.Generic.31654391	94dfff36061e989490abf4b5ec7dcb7c70f89af6136fecc632cdfdd3ca39c223
3.	41.78.64.254	TrojWare.Script.TrojanDownloader.Agent.	a1a3af9b10cff6fb4ed4df549b3661657fbb694cf831ce689ff02555d666b627
4.	41.59.203.31	HEUR:Trojan-	405f289c8c9aa46a261

		Downloader.Shell.Agent.p	59af0fa99d29b5cf59feae89ac1bf9dcfec109a94d5e1
5.	196.41.222.98	HEUR:Trojan-Downloader.Shell.Agent.bc	ed902957efb11382546f2cff80e5284832f7f53c4e2b82b9d181c1f3ef65513f
6.	196.41.222.5	Trojan.Linux.Generic.246192	48409bbbe5559ec2eae71fcfd8dcdb5ebe7472ef864eabdcdca427660287e0fc
7.	41.59.201.3	Linux.MiraiTrojan.Linux.GenericKD.40003689	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	41.59.203.192	Trojan.Linux.GenericKD.40003689	a37b519f4146749aef1e3ff0d5a76ef4cf9659927a4a4db527e22309cc988cd0
9.	41.59.201.52	HEUR:Trojan-DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
10.	41.59.41.28	Trojan.Win32.Eb.dqb	c70ca8df777bfc5a77d06eb625a0e6d7afdcd563df02a2d16de95813ae717a31

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **10,454** web attacks compared to last week which was **9,247**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 5th of February, 2023 – 11th of February, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	156.211.122.192	/
2.	183.136.225.32	/users/sign_in
3.	72.251.235.155	/boaform/admin/formLogin
4.	193.32.162.159	/favicon.ico
5.	5.172.190.11	/admin/config.php
6.	109.237.96.124	/robots.txt

7.	103.77.188.30	/admin/config.php?password%5B0%5D=ZIZO&username=admin
8.	109.237.96.124	/.env
9.	193.32.162.159	/.git/config
10.	1.13.8.48	/sitemap.xml

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.