TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 10th – 16th of January, 2021
Report No. : TZ-CERT/WRHP/2021/03

1. NETWORK ATTACKS

A total of **944,328** attacks have been recorded compared to last week **993,222** 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.	5.188.86.210	nproc	Admin@123
2.	5.188.86.178	admin	123456
3.	5.188.86.207	test	12345678
4.	5.188.86.165	user	123456@
5.	5.188.86.167	default	qwerty
6.	5.188.86.206	MikroTik	password
7.	5.188.86.221	root	test
8.	5.188.86.168	ftpuser	q1w2e3
9.	5.188.86.169	ubuntu	nproc
10.	5.188.86.212	server	admin

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 **382,865** malicious software distributed compared to last week in which was **69,987**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	54.93.99.154	TrojanDownloader:Win32/Small	685bc2af410d86a742b59b96d116a7d9
2.	193.123.67.84	HEUR:Trojan-Downloader.Win32.Generic	02c5f1515bf42798728fac17bfe1e4c1
3.	193.123.70.216	Trojan-Ransom.Win32.W	ae12bb54af31227017feffd9598a6f5e

		anna.m	
4.	54.93.227.51	Trojan:MSIL/Cryptor	0ab2aeda90221832167e5127332dd702
5.	85.76.10.10	Trojan-Ransom.Win32.Wanna.m	6e72ad805b4322612b9c9c7673a45635
6.	3.125.39.123	Trojan.Win32.Swisyn.fsyi	235e9af4c6f5b5de7d30d0589bbcff14
7.	112.78.1.134	Trojan.GenericKD.33730059	4590bad4daf0aea59d603a0e83892d86
8.	2.205.96.4	Ransom:Win32/CVE-2017-0147.A	6b5a9da099c8dd5b63a63c01c0256210
9.	117.53.152.16	Win32:Malware-gen	2c7c29e56a4c443c7f3d572d04d7da5e
10.	1.10.226.189	Win32/Worm.WannaCrypt.W	996c2b2ca30180129c69352a3a3515e4

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week, the sensors recorded a total of **86,201** web attacks compared to last week which was **86,527**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 10th and 16th of January, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	176.9.192.126	/
2.	139.162.186.32	/main.php
3.	180.149.228.182	/phpmyadmin/
4.	95.217.224.252	/phpmyadmin/scripts/setup.php
5.	38.79.90.76	/script
6.	176.9.175.215	/sqlite/main.php
7.	207.32.219.41	/SQLiteManager-1.2.4/main.php
8.	94.102.59.103	/TP/public/index.php?s=captcha
9.	51.81.142.133	/TP/public/index.php?s=index/
10.	5.39.44.147	/boaform/admin/formLogin?username=user&psd=user

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.