TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 20th – 26th of June, 2021
Report No. : TZ-CERT/WRHP/2021/26

1. NETWORK ATTACKS

A total of **1,009,312** attacks have been recorded compared to last week **1,176,134** 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.	5.188.86.236	root	password
2.	45.227.255.206	user	admin
3.	45.227.255.207	user1	12345
4.	5.188.86.210	admin	admin123
5.	5.188.86.178	nproc	passw0rd
6.	5.188.86.221	default	qwerty
7.	5.188.86.165	MikroTik	letmein
8.	5.188.86.207	profile	testing
9.	5.188.87.51	test	000000
10.	5.188.86.167	ubuntu	111111

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 **1,428,588** malicious software distributed compared to last week in which was **1,644,215**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(MD5)
1.	178.237.56.155	HEUR:Trojan.Win32.Miner.b.gen	685bc2af410d86a742b59b96d116a7d9
2.	23.225.70.23	HEUR:Trojan-Downloader.Win32.Generic	02c5f1515bf42798728fac17bfe1e4c1
3.	185.153.228.81	HEUR:Backdoor.Win32.Agent.gen	ca71f8a79f8ed255bf03679504813c6a
4.	50.195.197.105	Trojan-Ransom.Win32.Wanna.m	ae12bb54af31227017feffd9598a6f5e

5.	122.186.76.94	TrojanDownloader:Win32/ZombieBoy.A!bit	70ccd9220cebb56eaa38b9f1bd1a1cd8
6.	103.105.15.178	Ransom.Wannacry	414a3594e4a822cfb97a4326e185f620
7.	172.110.224.27	Trojan.Win32.Reconyc.fuzv	c71eacf3ffaf82787a533eb452bcf3e7
8.	117.110.224.27	Trojan-Ransom.Win32.Wanna.m	996c2b2ca30180129c69352a3a3515e4
9.	185.156.73.60	Trojan:MSIL/Cryptor	0ab2aeda90221832167e5127332dd702
10.	81.243.152.143	TrojanDownloader:Win32/Small	72e284e320ba59a31975d2df4b080558

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,882** web attacks compared to last week which was **2,546**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 20th and 26th of June, 2021 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	34.136.210.101	/TP/public/index.php
2.	191.232.36.117	/TP/public/index.php?s=captcha
3.	192.158.224.205	/TP/public/index.php?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1
4.	154.21.212.202	/users?page=&size=5
5.	157.90.125.213	/manager/html
6.	52.172.233.241	/login
7.	20.98.246.215	/admin-manager/admin.jsp
8.	154.3.215.21	/phpmyadmin/index.php
9.	13.65.95.73	/phpMyAdmin-4.2.1-all-languages/index.php
10.	192.158.239.136	/config/getuser?index=0

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.