TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 22nd – 28th June, 2019
Report No. : TZ-CERT/WRHP/2019/25

1. NETWORK ATTACKS

A total of **47,256** attacks have been recorded compared to last week **52,874** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in **table 1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	183.59.151.35	wordpress	root
2.	216.144.240.138	admin	admin
3.	115.231.233.208	root	qwert123
4.	102.165.50.210	student	test
5.	45.14.151.10	tracy	tracy
6.	5.188.210.139	angel	angel123
7.	162.243.144.152	adm	123456
8.	185.209.0.26	webmaster	Pas
9.	36.231.105.203	cumulus	Cumul
10.	120.237.142.236	cesar	cesar12

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 **32,316** malicious software distributed compared to last week in which was **122,850**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	216.83.53.207	Trojan.Win32. Brambul. bp	06bba7b7dfb4728110477d23caf5af06
2.	212.83.145.12	Trojan.GenericKD.4484531	786ab616239814616642ba4438df78a9
3.	77.247.110.168	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
4.	209.50.60.252	Gen:Win32.SMTP-Mailer.dqW@aqb@WXmG	065172e07a125623ea0a0fbcdaaa6dee
5.	189.211.142.184	Trojan:Win32/Occamy.C	c99e235fd91a121bbf193c471229d07b

6.	194.28.112.49	Trojan:Win32/Tilken.A!c l	7bbe010f98ae2e350cbfeaa1 6e58f871
7.	158.69.240.189	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52 a7aea396
8.	180.244.129.243	Worm.Generic.428092	d78e79d86b15ed5732c5ddd 002f5d38d
9.	216.144.240.138	Backdoor.Win32.Agent.rqr	7867de13bf22a7f3e3559044053e33 e7
10.	185.40.4.67	Trojan.Win32. Brambul. Bp	f273d1283364625f986050bd f7dec8bb

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,458** web attacks compared to last week which was **1,528**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the 4th week of June, 2019 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	122.121.52.153	/agendax/ConnectComputer/view/indexFrame.shtml
2.	185.176.27.74	/templates/ovcgi/view/snitz_forums_.mdb
3.	183.2.202.42	/phpMyAdmin/setup.php
4.	102.165.50.210	/surveys/big.php?pathtotemplate=
5.	89.248.174.201	/gnu/log/comments
6.	185.176.27.90	/contrib/yabbse/hp/device/search/admin.php
7.	158.69.240.189	/cgi-bin/comments
8.	193.32.161.48	/phpmyadmin/setup.php
9.	65.118.71.158	/contrib/yabbse/Activex/ds.py
10.	185.176.27.66	/gnu/log/comments

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.