TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 02nd - 08th of February, 2019
Report No. : TZ-CERT/WRHP/2019/05

1. NETWORK ATTACKS

A total of **99,890** attacks have been recorded compared to last week **82,107** 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.	5.188.86.194	user	user
2.	5.188.86.207	admin	admin
3.	5.188.87.51	root	root
4.	5.188.87.52	student	test
5.	5.188.87.49	tracy	tracy
6.	5.188.87.54	angel	angel12345
7.	5.188.86.197	adm	123456
8.	5.188.86.164	webmaster	pas
9.	5.188.86.198	cumulus	cumul
10.	5.188.86.196	cesar	Cesar12

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus it's advised to review usernames and passwords in use as well consider enforcing use of password policies.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded a total of **45,607** distributed malicious software compared to last week which was **41,842**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	185.53.88.69	Trojan.Win32.Brambul.bp	06bba7b7dfb4728110477d23caf5af06
2.	175.146.23.185	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
3.	185.53.88.63	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
4.	46.105.102.30	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
5.	185.217.69.173	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396

6.	185.156.177.24	Trojan:Win32/Tilken.A!cl	7bbe010f98ae2e350cbfeaa16e58f871
7.	147.135.79.2	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
8.	210.64.134.133	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
9.	102.165.48.8	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb
10.	192.67.159.13	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **4,764** web attacks compared to last week which was **7,012**.

From the **Table 3** the top 10 web based attacks and their associated requests sent to web servers for the 1st week of February, 2019 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	203.214.80.79	/phpmy/index.php
2.	114.116.13.163	/phpMyAdmin1/index.php
3.	123.207.140.22	/admin/mysql2/index.php
4.	82.159.30.250	/phpmyadmin/index.php?lang=en&pma_username=root&pma_password=2015
5.	111.230.29.39	/pwd/index.php
6.	192.144.184.227	/tomcat.php
7.	148.70.54.2	/
8.	169.236.198.12	/system.php
9.	79.202.107.135	/mysql/admin/index.php?lang=en
10.	111.2.28.153	/confg.php

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 in future.

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.