TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 5th - 11th of January, 2019
Report No. : TZ-CERT/WRHP/2019/01

1. NETWORKS ATTACKS

A total of **43,240** attacks have been recorded within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are in **Table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	5.188.87.53	server	123456
2.	5.188.87.54	admin	Root
3.	5.188.87.55	Test	password
4.	5.188.87.49	oracle	123
5.	5.188.87.52	User	Password123
6.	5.188.87.51	guest	1234
7.	5.188.86.164	Git	A
8.	5.188.86.196	ubuntu	1
9.	5.188.86.197	nagios	12345
10.	5.188.86.170	postgres	Qwe123

Table 1: 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 **21,960** malicious software distributed across all the sensors.

Below listed are top ten malicious software and their hashes:

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	61.218.135.140	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb
2.	188.76.24.128	Trojan.Win32.Brambul.bp	d78e79d86b15ed5732c5ddd002f5d38d
3.	88.188.82.230	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
4.	188.55.227.21	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
5.	181.229.116.190	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396

6.	88.188.82.230	Trojan:Win32/Tilken.A!cl	7bbe010f98ae2e350cbfeaa16e58f871
7.	87.109.204.178	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
8.	88.188.82.230	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
9.	188.48.238.149	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb
10.	188.50.28.61	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb

Table 2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,276** Web attacks which have been made within the period of the report.

From the **Table3** the top 10 web based attacks and their associated requests sent to web servers for the 1st week of January are detailed. The requests are the payloads.

S/N	ATTACKING IPS	TOP REQUESTS
1.	51.255.45.209	/phpmyadmin/index.php?lang=en
2.	148.70.19.161	/wp-content/plugins/portable-phpmyadmin/wp-pma-mod/index.php
3.	148.255.179.215	/phpMyAdmin__/index.php
4.	179.53.183.162	/phpMyAdmin/index.php
5.	148.255.178.42	/phpMyAdmin/scripts/db___.init.php
6.	118.24.235.50	/mysql/mysqlmanager/index.php
7.	159.65.32.8	/phpmyadmin/index.php?lang=en&pma_username=popa3d&pma_password=popa3d
8.	47.75.100.143	/pwd/index.php
9.	118.25.71.119	/mysql/dbadmin/index.php
10.	132.232.111.238	/shaAdmin/index.php

Table 3: 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 **Table2**

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.