TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 12th - 18th of January, 2019
Report No. : TZ-CERT/WRHP/2019/02

1. NETWORK ATTACKS

A total of **87,057** attacks have been recorded compared to last week **43,240** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords is as in table below:

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

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 **82,100** distributed malicious software compared to last week which was **21,960**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	46.105.102.30	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb
2.	193.56.29.18	Trojan.Win32.Brambul.bp	d78e79d86b15ed5732c5ddd002f5d38d
3.	110.249.212.46	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
4.	196.41.195.170	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
5.	69.162.110.222	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396

6.	58.218.66.169	Trojan:Win32/Tilken.A!cl	7bbe010f98ae2e350cbfeaa16e58f871
7.	102.165.52.123	Net-Worm.Win32.Agent.pk	e6724f877ecc50d5b07acb52a7aea396
8.	185.53.91.30	Worm.Generic.428092	d78e79d86b15ed5732c5ddd002f5d38d
9.	42.101.79.214	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb
10.	203.202.254.203	Trojan.Win32.Brambul.bp	f273d1283364625f986050bdf7dec8bb

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,267** web attacks compared to last week which was **3,276**.

From the **Table 3** the top 10 web based attacks and their associated requests sent to web servers for the 2nd week of January, 2019 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	132.232.106.156	/www/phpMyAdmin/index.php
2.	125.212.217.214	/wp-content/plugins/portable-phpmyadmin/wp-pma-mod/index.php
3.	51.255.45.209	/boots.php
4.	117.78.40.235	/mysql-admin/index.php
5.	202.166.198.154	/logon.php
6.	80.2.15.35	/index.php
7.	132.232.106.86	/config.php
8.	152.169.154.248	/tomcat.php
9.	134.175.40.34	/claroline/phpMyAdmin/index.php
10.	203.159.249.181	/wp-config.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.