TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 02nd - 08th of September, 2019
Report No. : TZ-CERT/WRHP/2019/31

1. NETWORK ATTACKS

A total of **522,139** attacks have been recorded compared to last week **70,205** 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.	134.19.187.75	wordpress	root
2.	185.220.221.206	admin	admin
3.	134.19.187.78	root	qwert123
4.	88.214.26.97	student	test
5.	153.36.242.114	tracy	tracy
6.	185.220.221.207	angel	angel123
7.	194.113.106.161	adm	123456
8.	119.196.83.6	webmaster	Pas
9.	141.98.81.138	cumulus	Cumul
10.	5.188.86.195	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 **296,797** malicious software distributed compared to last week in which was **67,914**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	179.126.34.218	HEUR:Backdoor.Win32.Agent.gen.	ca71f8a79f8ed255bf03679504813c6a
2.	216.245.213.134	RDN/Generic Downloader.x	8831cfc4b15416f07eb34d944641e179
3.	200.70.37.80	Trojan-Ransom.Win32.W	0ab2aeda90221832167e5127332dd702

		anna.m	
4.	37.49.225.226	Trojan-Ransom.Win32.Wanna.m	996c2b2ca30180129c69352a3a3515e4
5.	195.154.177.142	Net-Worm.Win32.Kido.ih	fbd8778d87c08492ef10a95ac7c30612
6.	62.4.22.64	HEUR:Trojan.Win32.Webdown.gen	0129086ae5fa2269d1037ff0ac0fca48
7.	185.254.122.37	BehavesLike.Win32.RansomWannaCry.th	ae12bb54af31227017feffd9598a6f5e
8.	172.105.77.67	GenericRXFL-OG!B9DE290EF3EC	b9de290ef3ec191950f0550cf6d14a6f
9.	175.112.9.160	Win32:Malware-gen	685bc2af410d86a742b59b96d116a7d9
10.	195.154.150.158	Trojan.Generic.D2666D4A	0ab2aeda90221832167e5127332dd702

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **892** web attacks compared to last month which was **18,854**.

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

SN	ATTACKING IPS	TOP REQUESTS
1.	222.186.46.27	/SQLiteManager-1.2.4/main.php
2.	207.180.251.152	/test/sqlite/SQLiteManager-1.2.0/SQLiteManager-1.2.0/main.php
3.	125.77.23.55	/main.php
4.	115.159.122.71	/SQlite/main.php
5.	180.76.232.150	/hudson/script
6.	202.85.213.11	/script
7.	123.206.77.106	/setup.cgi?next_file=netgear.cfg&todo=syscmd&cmd=busybox&curpath=/&currentsetting.htm=1

8.	92.14.63.55	/robots.txt
9.	165.22.79.166	/phpmyadmin/scripts/setup.php
10.	35.229.56.85	/

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.