TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 23rd – 29th of December, 2019
Report No. : TZ-CERT/WRHP/2019/47

1. NETWORK ATTACKS

A total of **93,820** attacks have been recorded compared to last week **108,634** 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.	5.188.86.167	admin	admin1
2.	5.188.86.169	adm	7ujMko0
3.	5.188.86.164	ftp	admin12
4.	5.188.86.168	guest	manager
5.	5.188.87.58	default	admin
6.	5.188.86.165	ftpuser	changeme
7.	5.188.87.53	operator	1234
8.	134.19.187.75	nagios	12345678
9.	5.188.87.49	administrator	ninja
10.	5.188.86.210	manager	vertex2

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 **3,546,133** malicious software distributed compared to last week in which was **7,071,926**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	196.192.35.93	HEUR:Trojan.Win32.Miner.b.gen	685bc2af410d86a742b59b96d116a7d9
2.	91.247.90.77	BehavesLike.Win32.Generic.mh	26f0446df04e1097f5575445fc0e6787
3.	81.180.68.4	HEUR:Backdoor.Win32.Agent.gen.	ca71f8a79f8ed255bf03679504813c6a
4.	46.72.47.63	Trojan.Win32.Swisyn.fsyi	235e9af4c6f5b5de7d30d0589bbcff14
5.	122.165.174.47	Trojan-Ransom.Win32.Wanna.m	0ab2aeda90221832167e5127332dd702
6.	41.188.46.240	Ransom:Win32/CVE-2017-0147.A	9d7aa3d9958293b549ef4f4db2cc2953

7.	23.234.50.57	TrojanDownloader:Win32/Small.gen!B	b3812008522d080fcbdec1adc499df2b
8.	190.85.145.66	HEUR:Trojan.Win32.Generic	fc4bb3140f35cc8abd681b63096e7b81
9.	154.197.8.97	Worm:Win32/Conficker.B	cea5ee69108f624073631fe9029ea662
10.	196.219.237.105	BehavesLike.Win32.RansomWannaCry.tm	a55b9addb2447db1882a3ae995a70151

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **960** web attacks compared to last week which was **1,942**.

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

SN	ATTACKING IPS	TOP REQUESTS
1.	185.100.87.190	/Nmap/folder/check1577640588
2.	49.234.233.108	/TP/public/index.php?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1
3.	103.9.124.70	///vtigercrm/modules/com_vtiger_workflow/resources/vtigerwebservices.js
4.	115.159.107.118	/secure/ContactAdministrators!default.jspa
5.	195.201.77.108	///recordings/atmin/modules/backup/i18n/backup.pot
6.	103.9.124.70	///html//admin/config.php
7.	78.46.215.246	/SQLite/main.php
8.	197.232.1.182	/manager/html
9.	152.136.136.229	/users?page=&size=5
10.	167.86.74.178	/yealink/SIP-T21/y000000000052.cfg

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.