TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 04th – 10th of November, 2019
Report No. : TZ-CERT/WRHP/2019/40

1. NETWORK ATTACKS

A total of **292,085** attacks have been recorded compared to last week **410,719** 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.	5.188.87.53	admin	admin
2.	193.32.161.176	adm	admin1
3.	5.188.86.169	ftp	7ujMko0
4.	5.188.86.165	guest	manager
5.	5.188.86.164	default	1234
6.	134.19.187.75	ftpuser	master
7.	5.188.86.210	operator	12345678
8.	5.188.87.58	nagios	changeme
9.	5.188.86.168	administrator	ninja
10.	5.188.86.167	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 **1,058,547** malicious software distributed compared to last week in which was **3,816,823**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	182.184.52.30	Trojan-Ransom.Win32.Wanna.m	42e738ed97f87cd7a1da297a81fca30e
2.	14.118.251.10	RDN/Generic Downloader.x	8831cfc4b15416f07eb34d944641e179
3.	209.206.45.205	Trojan-Ransom.Win32.Wanna.m	0ab2aeda90221832167e5127332dd702
4.	121.181.211.100	Trojan-Ransom.Win32.W	996c2b2ca30180129c69352a3a3515e4

		anna.m	
5.	59.128.61.202	Net-Worm.Win32.Kido.ih	fbd8778d87c08492ef10a95ac7c30612
6.	41.205.130.194	HEUR:Trojan.Win32.Webdown.gen	0129086ae5fa2269d1037ff0ac0fca48
7.	95.175.202.54	BehavesLike.Win32.RansomWannaCry.th	ae12bb54af31227017feffd9598a6f5e
8.	31.130.162.138	GenericRXFL-OG!B9DE290EF3EC	b9de290ef3ec191950f0550cf6d14a6f
9.	174.139.9.250	Win32:Malware-gen	685bc2af410d86a742b59b96d116a7d9
10.	113.100.39.221	Trojan.Generic.D2666D4A	0ab2aeda90221832167e5127332dd702

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **804** web attacks compared to last week which was **1,272**.

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

SN	ATTACKING IPS	TOP REQUESTS
1.	47.105.160.1	/TP/public/index.php?s=captcha
2.	115.159.107.118	/TP/public/index.php?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1
3.	203.154.59.166	/TP/public/index.php
4.	201.238.154.77	/yealink/y000000000035.cfg
5.	139.162.79.87	/provisioning/y000000000035.cfg
6.	112.29.140.227	/editBlackAndWhiteList
7.	112.29.140.222	/manager/text/list
8.	47.107.183.144	/weaver/bsh.servlet.BshServlet
9.	119.29.111.58	/secure/ContactAdministrators!default.jspa
10.	66.240.205.34	/seeyon/htmlofficeservlet

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.