TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 22nd – 28th of February, 2020
Report No. : TZ-CERT/WRHP/2020/08

1. NETWORK ATTACKS

A total of **133477** attacks have been recorded compared to last week **127,994** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	5.188.86.167	admin	admin1
2.	5.188.86.164	adm	7ujMko0
3.	5.188.86.168	ftp	admin12
4.	5.188.86.165	guest	manager
5.	5.188.87.58	default	admin
6.	5.188.86.169	ftpuser	changeme
7.	5.188.87.53	operator	1234
8.	5.188.87.49	nagios	12345678
9.	5.188.87.60	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 passwords 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 **1,169,781** malicious software distributed compared to last week in which was **1,069,437**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	36.232.40.249	HEUR:Trojan.Win32.Miner.b.gen	685bc2af410d86a742b59b96d116a7d9
2.	81.22.30.131	HEUR:Trojan-Downloader.Win32.Generic	26f0446df04e1097f5575445fc0e6787
3.	49.165.207.171	HEUR:Backdoor.Win32.Agent.gen.	ca71f8a79f8ed255bf03679504813c6a
4.	196.249.102.252	Win32:Malware-gen	f53134bb33e7baf7bf1d6f4da1fbb4fb
5.	196.200.133.28	Trojan-Ransom.Win32.W	ae12bb54af31227017feffd9598a6f5e

		anna.m	
6.	217.194.205.201	TrojanDownloader:Win32/Small.gen!B	235e9af4c6f5b5de7d30d0589bbcff14
7.	79.77.30.89	Ransom:Win32/CVE-2017-0147.A	414a3594e4a822cfb97a4326e185f620
8.	220.189.100.77	Trojan.GenericKD.40267082	74b16d9cf7d09b4878401401a481223b
9.	111.206.250.229	BehavesLike.Win32.RansomWannaCry.th	af76bbae1d51d04f1113bc225f979820
10.	111.206.250.198	Ransom-WannaCry!770ADFC01AE2	770adfc01ae26fe443df87619b8976ed

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **381** web attacks compared to last week which was **259**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the 4th week of February, 2020 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	39.96.87.185	/admin-scripts.asp
2.	129.232.148.50	http://www.rfa.org/english/
3.	212.129.50.159	http://www.minghui.org/
4.	78.108.177.54	http://123.125.114.144/
5.	120.79.251.131	/TP/public/index.php?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1
6.	187.23.51.203	/GponForm/diag_Form?script/
7.	39.135.1.160	/manage/html
8.	91.199.118.136	/weaver/bsh.servlet.BshServlet
9.	118.89.243.222	/favicon.ico
10.	198.108.66.192	/esps/

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.