TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 14th – 20th of February, 2021
Report No. : TZ-CERT/WRHP/2021/08

1. NETWORK ATTACKS

A total of **344,517** attacks have been recorded compared to last week **594,654** 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.	5.188.86.178	admin	admin
2.	5.188.86.168	nproc	password
3.	5.188.86.207	user1	123456
4.	5.188.87.53	root	1
5.	5.188.86.210	nagios	1234
6.	5.188.86.167	ftpuser	nproc
7.	45.227.255.207	webadmin	1122
8.	5.188.86.180	ceo	12345678
9.	5.188.86.169	support	download123
10.	5.188.86.165	guest	test123

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 **347,147** malicious software distributed compared to last week in which was **213,915**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	185.211.244.70	TrojanDownloader:Win32/Small.gen!B	235e9af4c6f5b5de7d30d0589bbcff14
2.	77.247.108.77	TrojanDownloader:Win32/Small	685bc2af410d86a742b59b96d116a7d9
3.	185.211.247.94	HEUR:Trojan-	02c5f1515bf42798728fac1

		Downloader.Win32.Generic	7bfe1e4c1
4.	45.126.20.70	Ransom.WannaCrypt	0ab2aeda90221832167e5127332dd702
5.	117.27.239.154	Trojan-Ransom.Win32.Wanna.m	ae12bb54af31227017feffd9598a6f5e
6.	24.10.92.158	Ransom:Win32/CVE-2017-0147.A	770adfc01ae26fe443df87619b8976ed
7.	180.248.11.90	Ransom.Wannacry	af76bbae1d51d04f1113bc225f979820
8.	188.170.192.8	Worm:Win32/Conficker.B	fbd8778d87c08492ef10a95ac7c30612
9.	45.226.148.225	Malware.Win32.Gencirc.10b8d049	8831cfc4b15416f07eb34d944641e179
10.	167.86.99.201	HEUR:Backdoor.Win32.Agent.gen.	ca71f8a79f8ed255bf03679504813c6a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week, the sensors recorded a total of **11,547** web attacks compared to last week which was **22,077**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 14th and 20th of February, 2021 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	13.90.60.46	/
2.	52.161.92.195	/ manager/html/
3.	88.198.2.248	/login
4.	107.150.22.76	http://check.bestproxies.ru/azenv.php?s=VJVJVXIJIDOOVDPCPBKDVRMUKJTRYR
5.	20.36.167.66	http://www.example.com
6.	13.92.152.24	//www/recordings/index.php
7.	78.68.234.208	/TP/public/index.php?s=captcha
8.	156.146.34.92	/TP/public/index.php?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=phpinfo&vars[1][]=1
9.	173.44.49.92	/admin-scripts.asp
10.	51.81.130.66	/GponForm/diag_Form?images/

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.