TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 27th of December ,2020 – 2nd of January, 2021
Report No. : TZ-CERT/WRHP/2021/01

1. NETWORK ATTACKS

A total of **993,222** attacks have been recorded compared to last week **979,863** 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.	5.188.86.206	nproc	nproc
2.	5.188.86.168	admin	admin
3.	5.188.87.57	test	password
4.	45.227.255.206	user	123456
5.	45.227.255.207	guest	123
6.	5.188.86.178	ftpuser	1
7.	5.188.86.207	root	test
8.	5.188.87.51	server	abc123
9.	5.188.86.165	ubuntu	q1w2e3
10.	5.188.86.167	git	P@ssw0rd

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 **1,378,812** malicious software distributed compared to last week in which was **380,593**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	216.245.212.218	TrojanDownloader:Win32/Small	685bc2af410d86a742b59b96d116a7d9
2.	93.216.12.37	HEUR:Trojan-Downloader.Win32.Generic	02c5f1515bf42798728fac17bfe1e4c1
3.	69.162.83.246	Ransom.WannaCrypt	0ab2aeda90221832167e5127332dd702

4.	82.82.216.226	Trojan-Ransom.Win32.Wanna.m	ae12bb54af31227017feffd9598a6f5e
5.	37.4.248.175	Ransom:Win32/CVE-2017-0147.A	996c2b2ca30180129c69352a3a3515e4
6.	85.127.26.85	Trojan:Win32/Tiggre!rfn	dede6d1500af444a9f4d67bf9fcc6088
7.	79.195.59.141	Trojan.Win32.Swisyn.fsyi	235e9af4c6f5b5de7d30d0589bbcff14
8.	178.77.72.216	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
9.	109.92.222.78	HEUR:Backdoor.Win32.Agent.gen.	ca71f8a79f8ed255bf03679504813c6a
10.	129.208.133.41	HEUR:Trojan-Downloader.Win32.Generic	8831cfc4b15416f07eb34d944641e179

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week, the sensors recorded a total of **91,139** web attacks compared to last week which was **329,072**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 27th of December, 2020 and 2nd of January, 2021 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	51.210.166.105	/boaform/admin/formLogin?username=adminisp&psd=adminisp
2.	94.102.59.105	/config/getuser?index=0
3.	51.210.137.19	/manager/html/
4.	51.81.159.145	/TP/public/index.php
5.	51.81.159.146	/es/components/com_extended_registration/enter.php?incl
6.	37.48.108.155	/servlet/proposte.php?id
7.	51.178.191.109	/admin2/perl/press.php?pref
8.	188.40.234.249	http://example.com/
9.	54.39.216.106	/login
10.	34.69.167.191	/style.css

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.