	TZ-CERT HONEYPOTS WEEKLY REPORT **Period** : 6th of March – 12th of March, 2022 **Report No.:** TZ-CERT/WRHP/2022/11

1. NETWORK ATTACKS

A total of **415,939** attacks have been recorded compared to last week **474,833** 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.	116.105.212.31	admin	12345
2.	5.188.62.194	guest	guest
3.	116.105.216.128	knockknockwhosthere	knockknockwhosthere
4.	116.110.3.253	nproc	nproc
5.	5.188.62.196	test	test
6.	62.240.132.152	user	1
7.	195.24.63.198	ftpuser	ftpuser123
8.	8.225.226.100	111111	password
9.	116.105.164.13	123321	administrator
10.	31.184.198.71	1234	159753

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 **122,749** malicious software distributed compared to last week in which was **133,525**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	89.236.218.25	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	59.46.124.38	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	122.3.131.20	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	85.173.252.88	HEUR:Backdoor.Win32.Agent.gen	e3120c5d322024a1c12cb8090fc820ed
5.	36.74.29.61	Trojan.Win32.Reconyc.fuzv	02c5f1515bf42798728fac17bfe1e4c1
6.	41.78.109.2	Trojan-	0ab2aeda9022183216

		Ransom.Win32.Wanna.m	7e5127332dd702
7.	117.239.245.218	Ransom.Wannacry	202cb962ac59075b964b07152d234b70
8.	41.78.110.2	W32/Wanna.M!tr	6414219ba88e70950c3d7282b99f5a81
9.	223.112.93.218	Trojan.Win32.Swisyn.fsyi	9f86955494146873a73f9df05bfb3d01
10.	78.111.9.21	Trojan.Agent.CZTF	a51d90f2f9394f5ea0a3acae3bd2b219

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **10,795** web attacks compared to last week which was **4,988**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 6th of March – 12th of March, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	52.224.56.77	/jenkins/login
2.	20.41.248.178	/login
3.	149.56.222.150	/manager/html
4.	70.39.92.7	/secure/ContactAdministrators!default.jspa
5.	191.101.130.150	/boaform/admin/formLogin?username=admin&psd=admin
6.	173.44.43.146	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	207.244.91.137	/config/getuser?index=0
8.	82.102.31.39	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	45.87.214.40	/hudson
10.	146.70.78.17	/favicon.ico

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.