	TZ-CERT HONEYPOTS WEEKLY REPORT **Period** : 24th of October – 30th of October, 2021 **Report No.:** TZ-CERT/WRHP/2021/44

1. NETWORK ATTACKS

A total of **627,177** attacks have been recorded compared to last week **528,849 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.	210.18.179.174	admin	Admin1
2.	5.188.62.194	guest	guest123
3.	5.188.62.196	knockknockwhosthere	123456
4.	116.105.30.143	root	111111
5.	137.184.115.252	test	test1234
6.	116.110.124.53	user	user123
7.	116.110.223.93	ftpuser	password
8.	103.231.14.184	hadoop	123456qwerty
9.	58.22.61.212	support	P@ssw0rd
10.	117.7.122.163	MikroTik	knockknockwhosthere

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 **319,758** malicious software distributed compared to last week in which was **612,427**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	213.202.233.100	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	179.106.51.77	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	73.19.218.74	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	54.38.169.1	HEUR:Backdoor.Win32.Agent.gen	02c5f1515bf42798728fac17bfe1e4c1
5.	58.240.67.140	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	218.106.124.5	Trojan-	844290834b6450425b

		Ransom.Win32.Wanna.m	146d4517cdf780
7.	118.31.187.234	Ransom.Wannacry	996c2b2ca30180129c6 9352a3a3515e4
8.	106.13.210.166	W32/Wanna.M!tr	235e9af4c6f5b5de7d3 0d0589bbcff14
9.	113.160.142.75	Ransom.Wannacry	414a3594e4a822cfb97 a4326e185f620
10.	45.143.203.2	Trojan.Agent.CZTF	ab27f6c7634e9efc13fb 2db29216a0a8

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **14,543** web attacks compared to last week which was **12,218**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 24th October and 30th of October, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	20.206.74.155	/jenkins/login
2.	91.213.50.11	/login
3.	185.220.100.249	/manager/html
4.	20.206.96.51	/secure/ContactAdministrators!default.jspa
5.	18.119.119.22	/boaform/admin/formLogin?username=admin&psd=ad min
6.	176.9.214.155	/boaform/admin/formLogin?username=adminisp&psd= adminisp
7.	181.215.176.92	/config/getuser?index=0
8.	135.148.214.9	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	51.222.56.159	/hudson
10.	20.203.176.253	/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.