	TZ-CERT HONEYPOTS WEEKLY REPORT **Period** : 30th of January – 5th of February, 2022 **Report No.:** TZ-CERT/WRHP/2022/6

1. NETWORK ATTACKS

A total of **310,980** attacks have been recorded compared to last week **297,084 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.	5.188.62.194	admin	Admin1
2.	116.105.212.31	guest	guest123
3.	82.157.148.23	knockknockwhosthere	1234567890
4.	5.188.62.196	root	P@ssw0rd
5.	116.105.216.128	test	test1234
6.	116.105.215.9	user	user123
7.	116.105.163.77	ftpuser	password
8.	45.141.84.10	hadoop	123456qwerty
9.	189.217.199.251	support	0987654321
10.	5.188.62.229	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 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 **9,911** malicious software distributed compared to last week in which was **170,728**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	172.124.0.21	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	38.23.229.178	Trojan-Ransom.Win32.Wanna.m	02c5f1515bf42798728fac17bfe1e4c1
3.	167.71.101.122	Ransom.Wannacry	70ccd9220cebb56eaa38b9f1bd1a1cd8
4.	117.50.120.208	HEUR:Backdoor.Win32.Agent.gen	3d26fcdacec75bf58959a378f449f91d
5.	111.68.102.206	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	47.108.233.154	Trojan-	72e284e320ba59a319

		Ransom.Win32.Wanna.m	75d2df4b080558
7.	46.17.102.90	Ransom.Wannacry	844290834b6450425b 146d4517cdf780
8.	162.251.61.34	W32/Wanna.M!tr	996c2b2ca30180129c6 9352a3a3515e4
9.	62.103.225.208	Ransom.Wannacry	ae12bb54af31227017f effd9598a6f5e
10.	164.77.118.66	Trojan.Agent.CZTF	0129086ae5fa2269d10 37ff0ac0fca48

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,789** web attacks compared to last week which was **6,149**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 30th January and 5th February, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	65.21.133.144	/jenkins/login
2.	194.110.115.42	/login
3.	162.222.198.99	/manager/html
4.	85.187.123.30	/secure/ContactAdministrators!default.jspa
5.	94.255.131.226	/boaform/admin/formLogin?username=admin&psd=admin
6.	20.101.112.26	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	45.87.212.180	/config/getuser?index=0
8.	52.179.9.87	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	191.96.180.36	/hudson
10.	37.19.218.161	/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.