TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 16th of January – 22nd of January, 2022
Report No.: TZ-CERT/WRHP/2022/4

1. NETWORK ATTACKS

A total of **306,747** attacks have been recorded compared to last week **243,678** 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.	5.188.62.196	guest	guest123
3.	116.105.215.9	knockknockwhosthere	1234567890
4.	116.105.216.128	root	P@ssw0rd
5.	116.105.212.31	test	test1234
6.	101.43.68.139	user	user123
7.	116.105.161.83	ftpuser	password
8.	116.105.77.149	hadoop	123456qwerty
9.	133.242.178.128	support	0987654321
10.	116.105.72.245	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 **306,162** malicious software distributed compared to last week in which was **684,581**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	164.77.118.66	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	62.103.225.208	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	61.177.173.26	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	183.48.35.78	HEUR:Backdoor.Win32.Agent.gen	02c5f1515bf42798728fac17bfe1e4c1
5.	208.98.9.210	Trojan.Win32.Reconyc.fuzv	414a3594e4a822cfb97a4326e185f620
6.	206.41.112.212	Trojan-	cf4f46336abeec036302

		Ransom.Win32.Wanna.m	97f846d17482
7.	47.104.203.199	Ransom.Wannacry	0646877a031e99b620feec592841848c
8.	221.4.205.226	W32/Wanna.M!tr	07d267ca215ec3fabf1c454665c2715a
9.	110.224.174.101	Ransom.Wannacry	15f4980c0667c400d6b5c35f6a20c032
10.	41.59.89.218	Trojan.Agent.CZTF	1a400481251fac98bc574c0aed7beca8

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **10,431** web attacks compared to last week which was **2,537**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 16th January and 22nd January, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	47.102.98.20	/jenkins/login
2.	158.140.163.28	/login
3.	65.21.133.144	/manager/html
4.	135.148.99.31	/secure/ContactAdministrators!default.jspa
5.	212.102.57.152	/boaform/admin/formLogin?username=admin&psd=admin
6.	51.81.161.144	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	51.222.54.18	/config/getuser?index=0
8.	13.68.212.10	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	20.121.208.250	/hudson
10.	194.147.142.118	/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.