TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 26th of December – 1st of January, 2022
Report No.: TZ-CERT/WRHP/2022/1

1. NETWORK ATTACKS

A total of **153,247** attacks have been recorded compared to last week **303,810 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.	171.252.186.42	guest	guest123
3.	5.188.62.196	knockknockwhosthere	1234567890
4.	116.110.92.217	root	P@ssw0rd
5.	116.110.25.208	test	test1234
6.	46.101.94.164	user	user123
7.	5.188.62.193	ftpuser	password
8.	5.188.62.232	hadoop	123456qwerty
9.	116.110.122.216	support	12wsDE34
10.	116.98.173.134	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 **127,178** malicious software distributed compared to last week in which was **229,466**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	103.147.184.143	Trojan Horse	70ccd9220cebb56eaa38b9f1bd1a1cd8
2.	103.226.249.187	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	203.238.39.182	Ransom.Wannacry	685bc2af410d86a742b59b96d116a7d9
4.	104.219.236.113	HEUR:Backdoor.Win32.Agent.gen	02c5f1515bf42798728fac17bfe1e4c1
5.	185.248.100.30	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	41.78.111.118	Trojan-	ae12bb54af31227017f

		Ransom.Win32.Wanna.m	effd9598a6f5e
7.	85.4.22.158	Ransom.Wannacry	beb68e9c7ef18f421df8230c032fe02a
8.	89.237.37.223	W32/Wanna.M!tr	996c2b2ca30180129c69352a3a3515e4
9.	204.92.21.249	Ransom.Wannacry	235e9af4c6f5b5de7d30d0589bbcff14
10.	122.186.76.102	Trojan.Agent.CZTF	07af1939f5d3ef53fde2736d28eccc90

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **6,545** web attacks compared to last week which was **39,978**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th December and 3rd January, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	135.148.112.41	/jenkins/login
2.	20.69.178.80	/login
3.	212.102.57.141	/manager/html
4.	3.65.198.173	/secure/ContactAdministrators!default.jspa
5.	20.94.67.206	/boaform/admin/formLogin?username=admin&psd=admin
6.	45.82.123.137	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	179.35.202.55	/config/getuser?index=0
8.	76.113.12.167	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	20.108.1.3	/hudson
10.	20.119.179.78	/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.