TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 21st of November – 29th of November, 2021
Report No.: TZ-CERT/WRHP/2021/48

1. NETWORK ATTACKS

A total of **24,343** attacks have been recorded compared to last week **99,417** 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.	172.106.32.143	admin	Admin1
2.	122.51.52.154	guest	guest123
3.	122.51.64.115	knockknockwhosthere	123456
4.	91.209.59.71	root	111111
5.	121.4.179.91	test	test1234
6.	116.110.252.176	user	user123
7.	38.91.102.73	ftpuser	password
8.	5.188.62.196	hadoop	123456qwerty
9.	5.188.62.194	support	P@ssw0rd
10.	81.69.240.12	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 **14,697** malicious software distributed compared to last week in which was **631,440**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	212.0.143.190	Trojan Horse	8b555eab89dd4e4dfa82d7c46c0429c6
2.	185.76.80.126	Trojan-Ransom.Win32.Wanna.m	beb68e9c7ef18f421df8230c032fe02a
3.	111.72.223.132	Ransom.Wannacry	ca71f8a79f8ed255bf03679504813c6a
4.	69.68.90.8	HEUR:Backdoor.Win32.Agent.gen	02c5f1515bf42798728fac17bfe1e4c1
5.	73.104.130.233	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	99.231.247.68	Trojan-	685bc2af410d86a742b

		Ransom.Win32.Wanna.m	59b96d116a7d9
7.	45.143.203.2	Ransom.Wannacry	70ccd9220cebb56eaa38b9f1bd1a1cd8
8.	176.111.173.206	W32/Wanna.M!tr	ae12bb54af31227017feffd9598a6f5e
9.	41.78.64.254	Ransom.Wannacry	414a3594e4a822cfb97a4326e185f620
10.	154.212.139.233	Trojan.Agent.CZTF	b420138b88eda83a51fea5298f72864a

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **187** web attacks compared to last week which was **4,636**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 21st November and 29th of November, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	13.85.7.191	/jenkins/login
2.	34.229.191.157	/login
3.	198.23.171.121	/manager/html
4.	20.124.96.109	/secure/ContactAdministrators!default.jspa
5.	188.166.212.191	/boaform/admin/formLogin?username=admin&psd=admin
6.	160.179.68.132	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	183.136.225.9	/config/getuser?index=0
8.	40.87.31.237	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	66.249.66.90	/hudson
10.	114.119.130.221	/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.