TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 17th of October – 23rd of October, 2021
Report No.: TZ-CERT/WRHP/2021/43

1. NETWORK ATTACKS

A total of **528,849** attacks have been recorded compared to last week **397,994 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.	213.202.233.100	admin	Admin1
2.	5.188.62.194	guest	guest123
3.	5.188.62.196	knockknockwhosthere	123456
4.	116.110.124.53	root	111111
5.	116.105.30.143	test	test1234
6.	116.105.72.49	user	user123
7.	116.110.223.93	ftpuser	password
8.	116.98.175.228	hadoop	123456qwerty
9.	152.70.111.213	support	P@ssw0rd
10.	116.98.170.29	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 **612,427** malicious software distributed compared to last week in which was **544,713**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	92.63.196.236	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	41.78.192.214	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	51.210.78.45	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	187.195.216.16	HEUR:Backdoor.Win32.Agent.gen	0ab2aeda90221832167e5127332dd702
5.	116.52.222.198	Trojan.Win32.Reconyc.fuzv	844290834b6450425b146d4517cdf780
6.	36.154.110.46	Trojan-	c71eacf3ffaf82787a533

		Ransom.Win32.Wanna.m	eb452bcf3e7
7.	41.207.248.243	Ransom.Wannacry	996c2b2ca30180129c69352a3a3515e4
8.	39.100.210.12	W32/Wanna.M!tr	414a3594e4a822cfb97a4326e185f620
9.	73.19.218.74	Ransom.Wannacry	ab27f6c7634e9efc13fb2db29216a0a8
10.	179.106.51.77	Trojan.Agent.CZTF	a55b9addb2447db1882a3ae995a70151

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **12,218** web attacks compared to last week which was **6,139**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 17th October and 23rd of October, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	3.8.199.125	/jenkins/login
2.	18.138.34.31	/login
3.	85.187.123.30	/manager/html
4.	181.215.176.92	/secure/ContactAdministrators!default.jspa
5.	36.78.154.239	/boaform/admin/formLogin?username=admin&psd=admin
6.	13.59.252.134	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	5.133.179.221	/config/getuser?index=0
8.	20.109.124.239	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	23.96.26.153	/hudson
10.	35.180.247.167	/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.