TZ-CERT HONEYPOTS WEEKLY REPORT
**Period : ** 10th of October – 16th of October, 2021
Report No.: TZ-CERT/WRHP/2021/42

1. NETWORK ATTACKS

A total of **397,994** attacks have been recorded compared to last week **1,473,305 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.	209.14.136.182	admin	Admin1
2.	5.188.62.194	guest	guest123
3.	93.92.136.31	knockknockwhosthere	123456
4.	5.188.62.196	root	111111
5.	171.225.184.186	test	test1234
6.	116.110.124.53	user	user123
7.	171.245.46.121	ftpuser	password
8.	182.162.104.239	hadoop	123456qwerty
9.	62.234.97.207	support	P@ssw0rd
10.	49.232.143.235	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 **544,713** malicious software distributed compared to last week in which was **2,629,856**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	179.106.51.77	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	73.19.218.74	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	103.160.50.48	Ransom.Wannacry	0ab2aeda90221832167e5127332dd702
4.	200.9.154.57	HEUR:Backdoor.Win32.Agent.gen	c8a89b783f0036ae5b4f840f74d1393a
5.	107.161.22.216	Trojan.Win32.Reconyc.fuzv	02c5f1515bf42798728fac17bfe1e4c1
6.	206.166.216.142	Trojan-	ae12bb54af31227017f

		Ransom.Win32.Wanna.m	effd9598a6f5e
7.	91.201.237.93	Ransom.Wannacry	c71eacf3ffaf82787a533eb452bcf3e7
8.	185.113.141.32	W32/Wanna.M!tr	414a3594e4a822cfb97a4326e185f620
9.	80.62.116.99	Ransom.Wannacry	996c2b2ca30180129c69352a3a3515e4
10.	13.73.31.185	Trojan.Agent.CZTF	1da27fb4c43e88a57b6215bf828eb314

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **6,139** web attacks compared to last week which was **22,116**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 10th October and 16th of October, 2021 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	85.187.123.30	/jenkins/login
2.	185.209.21.73	/login
3.	34.229.65.146	/manager/html
4.	52.255.155.45	/secure/ContactAdministrators!default.jspa
5.	40.79.28.149	/boaform/admin/formLogin?username=admin&psd=admin
6.	181.215.176.92	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	191.252.153.203	/config/getuser?index=0
8.	52.237.126.11	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	40.70.80.151	/hudson
10.	23.95.186.169	/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 mechanism 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.