TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 26th of September – 2nd of October, 2021
Report No.: TZ-CERT/WRHP/2021/40

1. NETWORK ATTACKS

A total of **2,179,554** attacks have been recorded compared to last week **663,962** 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.	171.225.185.69	admin	Admin1
2.	176.53.66.60	guest	guest123
3.	116.110.217.246	knockknockwhosthere	123456
4.	190.15.222.52	root	111111
5.	180.76.172.154	test	test1234
6.	45.240.88.239	user	user123
7.	126.77.170.137	ftpuser	password
8.	82.156.190.37	hadoop	123456qwerty
9.	206.189.35.215	support	P@ssw0rd
10.	157.245.216.88	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 **948,737** malicious software distributed compared to last week in which was **1,559,074**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	185.53.90.111	Trojan Horse	ca71f8a79f8ed255bf03679504813c6a
2.	41.59.197.83	Trojan-Ransom.Win32.Wanna.m	685bc2af410d86a742b59b96d116a7d9
3.	5.141.26.106	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	202.151.188.11	HEUR:Backdoor.Win32.Agent.gen	02c5f1515bf42798728fac17bfe1e4c1
5.	202.151.188.100	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	41.78.192.214	Trojan-	414a3594e4a822cfb97

		Ransom.Win32.Wanna.m	a4326e185f620
7.	37.255.242.68	Ransom.Wannacry	844290834b6450425b146d4517cdf780
8.	14.192.203.190	W32/Wanna.M!tr	996c2b2ca30180129c69352a3a3515e4
9.	62.148.141.250	Ransom.Wannacry	c71eacf3ffaf82787a533eb452bcf3e7
10.	171.70.192.86	Trojan.Agent.CZTF	cd99e5e4f44621978faf8df0e01d2d2b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **8,823** web attacks compared to last week which was **9,740**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th September and 2nd of October, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	18.221.66.197	/jenkins/login
2.	154.3.42.41	/login
3.	40.83.8.126	/manager/html
4.	154.21.208.222	/secure/ContactAdministrators!default.jspa
5.	3.120.186.217	/boaform/admin/formLogin?username=admin&psd=admin
6.	52.167.2.172	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	40.76.111.0	/config/getuser?index=0
8.	86.217.208.237	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	103.161.130.6	/hudson
10.	190.184.207.146	/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.