TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 3rd of October – 9th of October, 2021
Report No.: TZ-CERT/WRHP/2021/41

1. NETWORK ATTACKS

A total of **1,473,305** attacks have been recorded compared to last week **2,179,554** 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.	192.227.150.15	admin	Admin1
2.	118.69.60.214	guest	guest123
3.	171.225.185.69	knockknockwhosthere	123456
4.	116.110.217.246	root	111111
5.	5.188.62.194	test	test1234
6.	5.188.62.196	user	user123
7.	80.255.81.61	ftpuser	password
8.	35.199.73.100	hadoop	123456qwerty
9.	42.193.220.25	support	P@ssw0rd
10.	122.114.189.240	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 **2,629,856** malicious software distributed compared to last week in which was **948,737**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	47.215.243.89	Trojan Horse	996c2b2ca30180129c69352a3a3515e4
2.	171.70.192.86	Trojan-Ransom.Win32.Wanna.m	ae12bb54af31227017feffd9598a6f5e
3.	195.2.73.234	Ransom.Wannacry	844290834b6450425b146d4517cdf780
4.	177.76.163.204	HEUR:Backdoor.Win32.Agent.gen	414a3594e4a822cfb97a4326e185f620
5.	38.141.57.165	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	31.42.191.128	Trojan-	685bc2af410d86a742b

		Ransom.Win32.Wanna.m	59b96d116a7d9
7.	212.102.38.107	Ransom.Wannacry	ca71f8a79f8ed255bf03679504813c6a
8.	206.166.216.142	W32/Wanna.M!tr	ab27f6c7634e9efc13fb2db29216a0a8
9.	212.0.211.98	Ransom.Wannacry	a55b9addb2447db1882a3ae995a70151
10.	45.55.164.23	Trojan.Agent.CZTF	1487e2b148f7a4869c212f78cb28d682

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **22,116** web attacks compared to last week which was **8,823**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 3rd October and 9th of October, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	52.149.153.227	/jenkins/login
2.	5.188.211.10	/login
3.	5.188.211.15	/manager/html
4.	5.188.211.21	/secure/ContactAdministrators!default.jspa
5.	5.188.211.13	/boaform/admin/formLogin?username=admin&psd=admin
6.	5.188.211.26	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	5.196.59.95	/config/getuser?index=0
8.	5.188.211.22	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	5.188.211.35	/hudson
10.	5.188.211.72	/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.