TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 20th of February – 26th of February, 2022
Report No.: TZ-CERT/WRHP/2022/9

1. NETWORK ATTACKS

A total of **996,861** attacks have been recorded compared to last week **379,327** 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.	129.205.102.242	admin	Admin1
2.	116.105.212.31	guest	guest123
3.	5.188.62.194	knockknockwhosthere	1234567890
4.	116.105.216.128	root	P@ssw0rd
5.	167.172.221.151	test	test1234
6.	116.110.3.253	user	user123
7.	5.188.62.196	ftpuser	password
8.	211.37.174.46	hadoop	123456qwerty
9.	45.232.176.3	support	0987654321
10.	116.105.175.146	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 **231,347** malicious software distributed compared to last week in which was **359,221**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	210.4.107.10	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	218.106.124.5	Trojan-Ransom.Win32.Wanna.m	e3120c5d322024a1c12cb8090fc820ed
3.	39.108.224.10	Ransom.Wannacry	ca71f8a79f8ed255bf03679504813c6a
4.	223.112.93.218	HEUR:Backdoor.Win32.Agent.gen	02c5f1515bf42798728fac17bfe1e4c1
5.	78.111.9.21	Trojan.Win32.Reconyc.fuzv	72e284e320ba59a31975d2df4b080558
6.	158.255.7.204	Trojan-	996c2b2ca30180129c6

		Ransom.Win32.Wanna.m	9352a3a3515e4
7.	20.126.49.166	Ransom.Wannacry	0ab2aeda9022183216 7e5127332dd702
8.	62.220.116.146	W32/Wanna.M!tr	ae12bb54af31227017f effd9598a6f5e
9.	223.100.22.69	Ransom.Wannacry	70ccd9220cebb56eaa3 8b9f1bd1a1cd8
10.	47.108.222.53	Trojan.Agent.CZTF	95ae8e32eb8635e7ea be14ffbfaa777b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **39,295** web attacks compared to last week which was **6,096**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th February and 26th February, 2022 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	20.126.49.166	/jenkins/login
2.	154.118.227.58	/login
3.	70.39.92.7	/manager/html
4.	194.26.74.7	/secure/ContactAdministrators!default.jspa
5.	40.121.53.68	/boaform/admin/formLogin?username=admin&psd=ad min
6.	146.70.78.17	/boaform/admin/formLogin?username=adminisp&psd= adminisp
7.	95.217.79.199	/config/getuser?index=0
8.	193.232.65.89	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	20.62.100.155	/hudson
10.	15.228.128.175	/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.