TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 13th of March – 19th of March, 2022
Report No.: TZ-CERT/WRHP/2022/12

1. NETWORK ATTACKS

A total of **280,113** attacks have been recorded compared to last week **415,939** 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.	116.105.212.31	admin	12345
2.	5.188.62.194	guest	guest
3.	116.105.216.128	knockknockwhosthere	knockknockwhosthere
4.	116.110.3.253	nproc	nproc
5.	5.188.62.196	test	test
6.	5.39.95.30	user	1
7.	204.44.99.6	ftpuser	ftpuser123
8.	185.246.130.20	111111	password
9.	189.42.5.74	123321	administrator
10.	91.227.16.230	1234	159753

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 **46,910** malicious software distributed compared to last week in which was **122,749**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	195.174.236.233	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	41.78.109.2	Trojan-Ransom.Win32.Wanna.m	e3120c5d322024a1c12cb8090fc820ed
3.	121.42.149.130	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	140.206.56.118	HEUR:Backdoor.Win32.Agent.gen	ca71f8a79f8ed255bf03679504813c6a
5.	122.114.18.72	Trojan.Win32.Reconyc.fuzv	0a88674c7f65336d84f75b2d610a31e6
6.	41.78.109.4	Trojan-	0ab2aeda9022183216

		Ransom.Win32.Wanna.m	7e5127332dd702
7.	89.248.165.93	Ransom.Wannacry	996c2b2ca30180129c69352a3a3515e4
8.	41.78.64.254	W32/Wanna.M!tr	a55b9addb2447db1882a3ae995a70151
9.	89.236.218.25	Trojan.Win32.Swisyn.fsyi	d64dc93e51af87e033063032191fe291
10.	59.46.124.38	Trojan.Agent.CZTF	081967adb6eaab608a891f96f520d5e3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **6,821** web attacks compared to last week which was **10,795**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 13th of March – 19th of March, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	191.101.130.150	/jenkins/login
2.	20.96.9.44	/login
3.	52.224.56.77	/manager/html
4.	70.39.92.7	/secure/ContactAdministrators!default.jspa
5.	20.124.219.15	/boaform/admin/formLogin?username=admin&psd=admin
6.	79.137.133.136	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	104.223.127.214	/config/getuser?index=0
8.	52.14.79.140	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	146.70.78.17	/hudson
10.	20.127.136.93	/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.