TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 11th – 17th of July, 2021
Report No. : TZ-CERT/WRHP/2021/29

1. NETWORK ATTACKS

A total of **588,574** attacks have been recorded compared to last week **1,061,959** 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.	5.188.62.236	admin	admin
2.	45.227.255.207	nproc	password
3.	86.98.29.171	user1	123456
4.	5.188.86.178	root	1
5.	5.188.86.165	nagios	1234
6.	5.188.86.207	ftpuser	nproc
7.	5.188.86.168	admin1	123456
8.	5.188.86.206	default	1122
9.	45.227.255.206	support	support123
10.	5.188.87.60	MikroTik	88888888

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 **1,149,002** malicious software distributed compared to last week in which was **912,936**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	23.148.145.229	HEUR:Trojan.Win32.Miner.b.gen	685bc2af410d86a742b59b96d116a7d9
2.	92.63.196.249	Trojan-Ransom.Win32.Wanna.m	ae12bb54af31227017feffd9598a6f5e
3.	5.67.138.246	Ransom.Wannacry	0ab2aeda90221832167e5127332dd702
4.	185.223.29.154	HEUR:Backdoor.Win32.Agent.gen	ca71f8a79f8ed255bf03679504813c6a
5.	190.16.116.22	HEUR:Trojan-Downloader.Win32.Generic	02c5f1515bf42798728fac17bfe1e4c1

6.	174.63.239.1	Trojan.Agent.CZTF	996c2b2ca30180129c69352a3a3515e4
7.	50.110.207.100	Trojan:MSIL/Cryptor	414a3594e4a822cfb97a4326e185f620
8.	218.6.171.47	Downloader.Trojan	70ccd9220cebb56eaa38b9f1bd1a1cd8
9.	70.177.90.134	Trojan.Win32.Swisyn.fsyi	235e9af4c6f5b5de7d30d0589bbcff14
10.	92.63.196.228	Trojan:Win32/Eqtonex.F!rfn	e9d1ba0ee54fcdf37cf458cd3209c9f3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **16,662** web attacks compared to last week which was **4,668**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 11th and 17th of July, 2021 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	45.146.166.166	/jenkins/login
2.	154.21.212.202	/login
3.	13.72.79.237	/manager/html
4.	207.244.251.177	/secure/ContactAdministrators!default.jspa
5.	13.68.149.48	/boaform/admin/formLogin?username=admin&psd=admin
6.	165.255.101.234	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	18.221.81.59	/config/getuser?index=0
8.	196.77.133.27	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	104.197.133.184	/hudson
10.	46.101.9.74	/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.