TZ-CERT HONEYPOTS WEEKLY REPORT
**Period : ** 1st of August – 7th of August, 2021
Report No. : TZ-CERT/WRHP/2021/32

1. NETWORK ATTACKS

A total of **366,549** attacks have been recorded compared to last week **458,055** 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.	171.251.26.14	admin	Admin1
2.	5.182.39.71	nproc	password
3.	5.182.39.70	user1	123456
4.	5.182.39.65	root	111111
5.	116.110.102.97	test	test1234
6.	45.227.255.208	user	1qaz2wsx
7.	5.188.62.249	admin1	123456
8.	5.188.62.219	default	1122
9.	5.188.62.229	support	letmein
10.	116.110.82.78	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 **407,304** malicious software distributed compared to last week in which was **104,350**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	27.221.74.6	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	62.76.35.170	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	110.37.207.36	Ransom.Wannacry	02c5f1515bf42798728fac17bfe1e4c1
4.	117.27.239.29	HEUR:Backdoor.Win32.Agent.gen	ae12bb54af31227017feffd9598a6f5e
5.	117.27.239.123	Trojan.Win32.Reconyc.fuzv	beb68e9c7ef18f421df8230c032fe02a
6.	119.167.79.34	Trojan:MSIL/Cryptor	0ab2aeda90221832167e5

			127332dd702
7.	39.52.131.138	TrojanDownloader:Win32/Small	996c2b2ca30180129c69352a3a3515e4
8.	117.27.239.33	Downloader.Trojan	a55b9addb2447db1882a3ae995a70151
9.	86.96.249.162	Ransom:Win32/CVE-2017-0147.A	c71eacf3ffaf82787a533eb452bcf3e7
10.	186.4.107.8	Trojan.Agent.CZTF	e9d1ba0ee54fcdf37cf458cd3209c9f3

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,834** web attacks compared to last week which was **1,811**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 1st and 7th of August, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	113.185.47.235	/jenkins/login
2.	113.186.65.76	/login
3.	18.216.193.209	/manager/html
4.	18.159.101.30	/secure/ContactAdministrators!default.jspa
5.	40.112.49.99	/boaform/admin/formLogin?username=admin&psd=admin
6.	20.197.239.94	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	117.0.252.116	/config/getuser?index=0
8.	117.0.252.20	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	13.85.21.25	/hudson
10.	187.109.132.255	/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.