TZ-CERT HONEYPOTS WEEKLY REPORT
Period **:** 25th of July – 1st of August, 2021
Report No. : TZ-CERT/WRHP/2021/31

1. NETWORK ATTACKS

A total of **458,055** attacks have been recorded compared to last week **368,119** 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.	203.175.76.156	admin	admin
2.	5.188.62.249	nproc	password
3.	171.251.26.14	user1	123456
4.	45.227.255.207	root	1
5.	5.188.62.243	test	test1234
6.	45.227.255.161	user	000000
7.	45.227.255.208	admin1	123456
8.	5.182.39.65	default	1122
9.	5.182.39.71	support	support123
10.	5.182.39.70	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 **104,350** malicious software distributed compared to last week in which was **101,913**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	92.63.196.222	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	62.76.35.170	Trojan-Ransom.Win32.Wanna.m	beb68e9c7ef18f421df8230c032fe02a
3.	39.52.131.138	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	151.106.117.54	HEUR:Backdoor.Win32.Agent.gen	996c2b2ca30180129c69352a3a3515e4
5.	151.106.52.70	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	132.232.54.185	Trojan:MSIL/Cryptor	c71eacf3ffaf82787a533

			eb452bcf3e7
7.	62.76.35.170	TrojanDownloader:Win32/Small	414a3594e4a822cfb97a4326e185f620
8.	129.227.237.118	Downloader.Trojan	02c5f1515bf42798728fac17bfe1e4c1
9.	92.63.196.228	Ransom:Win32/CVE-2017-0147.A	0ab9a60a55cb40fc338e8f4988feee2f
10.	34.215.199.20	Trojan.Agent.CZTF	0e19ca510e6158adb69e2d51d35c54cd

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 **1,261**.

From the table the top 10 web based attacks and their associated requests sent to web servers for the period between 25th of July and 1st of August, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	52.188.118.217	/jenkins/login
2.	91.148.161.242	/login
3.	45.42.45.111	/manager/html
4.	181.43.243.83	/secure/ContactAdministrators!default.jspa
5.	35.180.208.85	/boaform/admin/formLogin?username=admin&psd=admin
6.	52.14.238.191	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	52.32.67.74	/config/getuser?index=0
8.	169.129.96.52	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	200.121.203.169	/hudson
10.	31.6.11.54	/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.