TZ-CERT HONEYPOTS WEEKLY REPORT

Period **:** 8th of August – 14th of August, 2021
Report No.: TZ-CERT/WRHP/2021/33

1. NETWORK ATTACKS

A total of **451,888** attacks have been recorded compared to last week **366,549 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.	116.98.171.249	admin	Admin1
2.	218.4.219.30	nproc	password
3.	5.188.62.249	user1	123456
4.	116.110.10.145	root	111111
5.	5.182.39.70	test	test1234
6.	5.182.39.65	user	1qaz2wsx
7.	5.182.39.71	admin1	123456
8.	45.227.255.208	default	1122
9.	5.188.62.219	support	letmein
10.	5.188.62.229	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 **778,315** malicious software distributed compared to last week in which was **407,304**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	40.90.249.72	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	117.27.239.1	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
3.	41.78.192.214	Ransom.Wannacry	ae12bb54af31227017feffd9598a6f5e
4.	68.10.159.35	HEUR:Backdoor.Win32.Agent.gen	996c2b2ca30180129c69352a3a3515e4
5.	45.134.144.133	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	81.35.3.25	DoS-FAE!C71EACF3FFAF	70ccd9220cebb56eaa38b9f1bd1a1cd8

7.	180.76.248.220	Trojan:MSIL/Cryptor	414a3594e4a822cfb97a4326e185f620
8.	190.216.233.211	W32/Wanna.M!tr	95ae8e32eb8635e7eabe14ffbfaa777b
9.	185.223.29.154	Mal/Generic-R + Mal/Wanna-A	cd99e5e4f44621978faf8df0e01d2d2b
10.	190.16.116.22	Trojan.Agent.CZTF	c71eacf3ffaf82787a533eb452bcf3e7

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **9,684** web attacks compared to last week which was **1,834**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 8th and 14th of August, 2021, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	35.222.89.22	/jenkins/login
2.	45.133.173.11	/login
3.	185.54.230.119	/manager/html
4.	5.133.30.125	/secure/ContactAdministrators!default.jspa
5.	52.156.140.149	/boaform/admin/formLogin?username=admin&psd=admin
6.	82.165.103.164	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	185.221.237.77	/config/getuser?index=0
8.	190.42.16.236	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	151.53.71.67	/hudson
10.	5.133.179.221	/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.