TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 14th of August – 20th of August, 2022
Report No.: TZ-CERT/WRHP/2022/33

1. NETWORK ATTACKS

A total of **145,976** attacks have been recorded compared to last week **97,785** 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.	202.7.202.209	nproc	nproc
2.	78.46.46.131	admin	admin
3.	78.47.166.111	user	P@ssword1
4.	180.141.175.108	root	root
5.	206.189.46.147	test	test
6.	179.60.147.161	ubuntu	ubuntu
7.	109.206.241.17	telus	123456
8.	79.110.62.47	admin1234	password
9.	193.142.147.10	Postgres	abc123
10.	193.105.134.95	oracle	oracle

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 **1,556,674** malicious software distributed compared to last week in which was **755,162**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	45.95.147.34	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	41.59.89.218	A Variant Of Win32/TrojanDownloader.Small.AVZ	7107326e81d955aff29f49487aa3da23
3.	113.107.69.10	TrojWare.Win32.Ransom.WannaCry.AB@75g	ae12bb54af31227017feffd9598a6f5e
4.	221.229.220.195	HEUR:Trojan-Downloader.Win32.Generic	0ab2aeda90221832167e5127332dd702

5.	197.250.198.6	Trojan-Ransom.Win32.Wanna.m	996c2b2ca30180129c69352a3a3515e4
6.	122.2.8.148	Trojan-Ransom.Win32.Wanna.m	414a3594e4a822cfb97a4326e185f620
7.	103.90.213.141	Trojan-Ransom.Win32.Wanna.m	a55b9addb2447db1882a3ae995a70151
8.	164.92.105.179	Gen:Trojan.Malware.eC5@a0JB20mi	ca71f8a79f8ed255bf03679504813c6a
9.	45.169.140.102	Trojan.Agent.CZTF	cd99e5e4f44621978faf8df0e01d2d2b
10.	42.157.129.157	HEUR:Trojan.Win32.Miner.b.gen	95ae8e32eb8635e7eabe14ffbfaa777b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,285** web attacks compared to last week which was **2,765**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 14th of August – 20th of August, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	197.250.198.6	/jenkins/login
2.	188.68.61.6	/login
3.	120.208.103.205	/manager/html
4.	45.134.144.140	/secure/ContactAdministrators!default.jspa
5.	139.87.71.160	/boaform/admin/formLogin?username=admin&psd=admin
6.	185.255.89.134	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	192.241.203.234	/config/getuser?index=0
8.	112.248.107.64	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	113.219.192.36	/hudson
10.	115.50.58.189	/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.