TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 3rd of July – 9th of July, 2022
Report No.: TZ-CERT/WRHP/2022/27

1. NETWORK ATTACKS

A total of **262,425** attacks have been recorded compared to last week **217,108** 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.	194.31.98.244	admin	123456
2.	201.166.225.176	nproc	nproc
3.	34.66.50.28	user	1
4.	116.105.165.77	test	test
5.	116.105.77.108	111111	$passwor
6.	116.105.161.80	guest	guest
7.	116.105.19.68	ftpuser	ftpuser
8.	116.105.167.224	ftp	ftp
9.	116.105.161.4	123321	administrator
10.	162.215.222.200	support	support

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 **95,126** malicious software distributed compared to last week in which was **142,565**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	112.13.76.172	Trojan Horse	e032dffe8dd0bd5689752d7fc27846d7
2.	66.63.177.234	Linux/SQLMap	857f8fc914f7879b2bc8020dfe48d4ba
3.	61.184.119.32	TrojWare.Win32.Ransom.WannaCry.AB@75g	868657db51aed0dadecf1a2a965adb09
4.	89.248.165.57	Linux/SQLMap	8735e7967258470a38dda091fa58b802
5.	45.164.23.148	Trojan.Win32.Reconyc.fuzv	ec91f05b2c68fc47dbf7c5f923f1fd89
6.	45.170.253.241	Trojan-	ae12bb54af31227017f

		Ransom.Win32.Wanna.m	effd9598a6f5e
7.	123.57.5.229	Ransom.Wannacry	0064e2641d419d2c68f9beb18246a297
8.	47.104.134.140	Dropped:Generic.Malware.F!dld!.0204478	25d6d73e9b52d3ab18c5e4f9b435a00c
9.	193.46.255.26	Trojan.Win32.Swisyn.fsyi	30c62ab1d9f5e07a4af9e25e9fbd3b3a
10.	47.112.112.30	Trojan.Agent.CZTF	cf7b39927c0354782ca75086240b0041

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **15,046** web attacks compared to last week which was **7,548**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 3rd of July – 9th of July, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	125.74.8.51	/jenkins/login
2.	194.26.74.7	/login
3.	20.229.168.212	/manager/html
4.	106.163.248.52	/secure/ContactAdministrators!default.jspa
5.	105.71.18.140	/boaform/admin/formLogin?username=admin&psd=admin
6.	34.65.197.10	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	45.134.140.177	/config/getuser?index=0
8.	114.119.147.239	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	86.111.229.152	/hudson
10.	86.111.229.228	/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.