TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 10th of July – 16th of July, 2022
Report No.: TZ-CERT/WRHP/2022/28

1. NETWORK ATTACKS

A total of **163,556** attacks have been recorded compared to last week **262,425** 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.	116.105.73.222	nproc	nproc
3.	116.105.77.160	user	1
4.	116.105.75.87	test	test
5.	27.66.8.134	111111	$passwor
6.	116.105.72.162	guest	guest
7.	116.105.173.97	ftpuser	ftpuser
8.	183.167.199.51	ftp	ftp
9.	147.135.219.202	123321	administrator
10.	157.245.129.95	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 **149,935** malicious software distributed compared to last week in which was **95,126**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	164.77.118.66	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	179.104.35.174	Linux/SQLMap	7107326e81d955aff29f49487aa3da23
3.	201.48.58.125	TrojWare.Win32.Ransom.WannaCry.AB@75g	ae12bb54af31227017feffd9598a6f5e
4.	122.114.18.72	Linux/SQLMap	02c5f1515bf42798728fac17bfe1e4c1
5.	89.248.165.57	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702
6.	103.113.85.138	Trojan-	1a400481251fac98bc5

		Ransom.Win32.Wanna.m	74c0aed7beca8
7.	111.248.58.70	Ransom.Wannacry	449960bfef57cfc18538a7d8c83fba87
8.	196.188.192.141	Dropped:Generic.Malware.F!dld!.0204478	a55e017fc37c538cc62db87da6e959f4
9.	112.13.76.172	Trojan.Win32.Swisyn.fsyi	e9d1ba0ee54fcdf37cf458cd3209c9f3
10.	66.63.177.234	Trojan.Agent.CZTF	135c4f212bb6db70ad400551df7205b0

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **50** web attacks compared to last week which was **15,046**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 10th of July – 16th of July, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	62.183.2.190	/jenkins/login
2.	66.94.114.205	/login
3.	13.244.117.62	/manager/html
4.	222.80.76.212	/secure/ContactAdministrators!default.jspa
5.	123.175.120.235	/boaform/admin/formLogin?username=admin&psd=admin
6.	158.69.252.66	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	192.241.212.184	/config/getuser?index=0
8.	35.192.127.64	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	39.104.18.20	/hudson
10.	51.145.114.15	/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.