TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 19th of June – 25th of June, 2022
Report No.: TZ-CERT/WRHP/2022/25

1. NETWORK ATTACKS

A total of **145,812** attacks have been recorded compared to last week **82,284** 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.	195.3.147.76	admin	123456
2.	2.58.149.116	nproc	nproc
3.	116.98.162.249	user	1
4.	116.105.20.120	test	test
5.	5.188.62.253	111111	$passwor
6.	116.105.74.96	guest	guest
7.	116.105.72.212	ftpuser	ftpuser
8.	116.105.168.224	ftp	ftp
9.	116.105.196.108	123321	administrator
10.	116.105.164.191	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 **54,964** malicious software distributed compared to last week in which was **2,666**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	104.156.155.11	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	89.248.165.57	Linux/SQLMap	0ab2aeda90221832167e5127332dd702
3.	101.78.167.70	TrojWare.Win32.Ransom.WannaCry.AB@75g	ca71f8a79f8ed255bf03679504813c6a
4.	122.172.178.72	Linux/SQLMap	414a3594e4a822cfb97a4326e185f620
5.	138.19.249.166	Trojan.Win32.Reconyc.fuzv	3553aeb71299e94c2549f1b34f6c1a43
6.	89.248.165.60	Trojan-	ae12bb54af31227017f

		Ransom.Win32.Wanna.m	effd9598a6f5e
7.	103.218.115.78	Ransom.Wannacry	0064e2641d419d2c68f9beb18246a297
8.	20.226.94.162	Dropped:Generic.Malware.F!dld!.0204478	25d6d73e9b52d3ab18c5e4f9b435a00c
9.	121.175.74.103	Trojan.Win32.Swisyn.fsyi	30c62ab1d9f5e07a4af9e25e9fbd3b3a
10.	41.59.199.207	Trojan.Agent.CZTF	ea075b59a185e8cac084cc39ee95d74b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **53** web attacks compared to last week which was **32**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th of June – 25th of June, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	137.184.12.127	/jenkins/login
2.	45.195.69.61	/login
3.	111.75.246.105	/manager/html
4.	172.104.234.47	/secure/ContactAdministrators!default.jspa
5.	193.123.87.5	/boaform/admin/formLogin?username=admin&psd=admin
6.	194.163.163.50	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	202.83.31.224	/config/getuser?index=0
8.	206.189.140.43	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	35.77.105.66	/hudson
10.	1.202.117.63	/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.