TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 15th of May – 21st of May, 2022
Report No.: TZ-CERT/WRHP/2022/20

1. NETWORK ATTACKS

A total of **182,688** attacks have been recorded compared to last week **327,047** 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.	106.53.135.104	admin	admin
2.	45.141.84.10	guest	guest
3.	116.110.92.78	ubuntu	ubuntu
4.	5.188.62.194	oracle	oracle
5.	5.188.62.196	nproc	nproc
6.	5.188.62.250	user	123456
7.	171.251.25.38	ftpuser	ftpuser
8.	116.105.216.128	111111	P@ssw0rd
9.	171.251.16.252	postgres	abc123
10.	171.251.20.141	git	git

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 **108,729** malicious software distributed compared to last week in which was **324,941**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	35.247.181.153	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	34.143.147.100	Linux/SQLMap	ae12bb54af31227017feffd9598a6f5e
3.	34.126.184.23	TrojWare.Win32.Ransom.WannaCry.AB@75g	0ab2aeda90221832167e5127332dd702
4.	34.126.68.101	Linux/SQLMap	996c2b2ca30180129c69352a3a3515e4
5.	35.247.182.185	Trojan.Win32.Reconyc.fuzv	02c5f1515bf42798728fac17bfe1e4c1
6.	35.198.251.170	Trojan-	beb68e9c7ef18f421df8

		Ransom.Win32.Wanna.m	230c032fe02a
7.	34.124.227.218	Ransom.Wannacry	01d87121a4a589930d580a88e4df3640
8.	34.87.64.0	Dropped:Generic.Malware.F!dld!.0204478	3622b46d0c1724779e008272ca7f7d61
9.	104.156.155.12	Trojan.Win32.Swisyn.fsyi	6e72ad805b4322612b9c9c7673a45635
10.	60.210.9.235	Trojan.Agent.CZTF	aa718a028875637e1c6eb648706340b6

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **68** web attacks compared to last week which was **517**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 15th of May –21st of May, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	199.195.249.217	/jenkins/login
2.	45.148.10.81	/login
3.	41.59.90.66	/manager/html
4.	137.184.38.61	/secure/ContactAdministrators!default.jspa
5.	192.241.213.192	/boaform/admin/formLogin?username=admin&psd=admin
6.	196.179.252.28	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	103.219.31.21	/config/getuser?index=0
8.	115.44.105.10	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	117.40.113.187	/hudson
10.	124.117.192.88	/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.