TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 1st of May – 7th of May, 2022
Report No.: TZ-CERT/WRHP/2022/18

1. NETWORK ATTACKS

A total of **348,217** attacks have been recorded compared to last week **225,203** 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.	183.82.121.114	admin	admin
2.	116.105.212.31	guest	guest
3.	5.188.62.194	ubuntu	ubuntu
4.	116.105.216.128	oracle	oracle
5.	5.188.62.196	nproc	nproc
6.	171.251.29.152	user	123456
7.	199.188.241.199	ftpuser	ftpuser
8.	5.188.62.250	111111	P@ssw0rd
9.	167.99.80.134	postgres	abc123
10.	185.246.130.20	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 **53,972** malicious software distributed compared to last week in which was **8,268**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	222.252.20.86	Trojan Horse	02c5f1515bf42798728fac17bfe1e4c1
2.	58.34.196.12	Linux/SQLMap	ca71f8a79f8ed255bf03679504813c6a
3.	188.170.216.194	TrojWare.Win32.Ransom.WannaCry.AB@75g	0ab2aeda90221832167e5127332dd702
4.	106.13.224.59	Linux/SQLMap	ae12bb54af31227017feffd9598a6f5e
5.	150.242.254.35	Trojan.Win32.Reconyc.fuzv	cf4f46336abeec03630297f846d17482
6.	103.93.97.221	Trojan-	1a633a9c0e9bbbbd1f3

		Ransom.Win32.Wanna.m	1178150e8c1c7
7.	186.1.16.166	Ransom.Wannacry	a4d49eaf60a8e333708469606ad9e1a4
8.	41.78.174.77	Dropped:Generic.Malware.F!dld!.0204478	ae12bb54af31227017feffd9598a6f5e
9.	212.143.154.229	Trojan.Win32.Swisyn.fsyi	685bc2af410d86a742b59b96d116a7d9
10.	217.161.97.163	Trojan.Agent.CZTF	c1045e165824a769408792e176290035

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **5,214** web attacks compared to last week which was **290,456**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 1st of May –7th of May, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	154.118.227.58	/jenkins/login
2.	125.74.8.51	/login
3.	102.129.153.138	/manager/html
4.	20.127.68.194	/secure/ContactAdministrators!default.jspa
5.	18.228.38.222	/boaform/admin/formLogin?username=admin&psd=admin
6.	186.136.196.7	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	94.103.84.230	/config/getuser?index=0
8.	20.190.194.239	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	177.247.80.128	/hudson
10.	185.147.212.62	/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.