TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 17th of April – 23rd of April, 2022
Report No.: TZ-CERT/WRHP/2022/16

1. NETWORK ATTACKS

A total of **121,961** attacks have been recorded compared to last week **443,552** 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.	36.129.3.143	admin	admin
2.	116.105.212.31	guest	guest
3.	5.188.62.194	ubuntu	ubuntu
4.	190.116.43.126	oracle	oracle
5.	116.110.3.253	test	test
6.	116.105.216.128	user	123456
7.	5.188.62.196	ftpuser	ftpuser
8.	116.105.18.71	111111	P@ssw0rd
9.	171.251.21.9	postgres	abc123
10.	5.188.62.250	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 **19,060** malicious software distributed compared to last week in which was **163,124**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	183.94.244.16	Trojan Horse	d3d7d3eadf02eb366d765409c1946547
2.	223.71.102.199	Linux/SQLMap	685bc2af410d86a742b59b96d116a7d9
3.	20.126.96.245	TrojWare.Win32.Ransom.WannaCry.AB@75g	ae12bb54af31227017feffd9598a6f5e
4.	5.42.224.14	Linux/SQLMap	0ab2aeda90221832167e5127332dd702
5.	102.181.51.45	Trojan.Win32.Reconyc.fuzv	1a633a9c0e9bbbbd1f31178150e8c1c7
6.	119.5.43.135	Trojan-	3349eab5cc4660bafa5

		Ransom.Win32.Wanna.m	02f7565ff761d
7.	61.238.173.82	Ransom.Wannacry	8d43ea208e3d93c418d7154f95fa9ac5
8.	15.235.14.214	Dropped:Generic.Malware.F!dld!.0204478	0ab2aeda90221832167e5127332dd702
9.	137.184.25.40	Trojan.Win32.Swisyn.fsyi	8e6bfea06cb00553ee29b3822b349bd6
10.	2.57.121.53	Trojan.Agent.CZTF	a4d49eaf60a8e333708469606ad9e1a4

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **176,883** web attacks compared to last week which was **253,917**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 17th of April – 23rd of April, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	54.187.245.161	/jenkins/login
2.	5.188.211.72	/login
3.	5.188.211.21	/manager/html
4.	5.188.211.16	/secure/ContactAdministrators!default.jspa
5.	5.188.211.26	/boaform/admin/formLogin?username=admin&psd=admin
6.	5.188.211.22	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	5.188.211.35	/config/getuser?index=0
8.	154.12.196.103	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	154.12.199.129	/hudson
10.	5.188.211.10	/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.