TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 27th of March – 2nd of April, 2022
Report No.: TZ-CERT/WRHP/2022/14

1. NETWORK ATTACKS

A total of **522,635** attacks have been recorded compared to last week **353,352** 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.	116.105.212.31	admin	admin
2.	5.188.62.194	guest	guest
3.	66.29.128.2	ubuntu	ubuntu
4.	116.110.3.253	oracle	oracle
5.	116.105.216.128	test	test
6.	83.212.116.141	user	123456
7.	5.188.62.196	ftpuser	ftpuser
8.	203.150.58.25	111111	P@ssw0rd
9.	164.92.158.213	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 **183,710** malicious software distributed compared to last week in which was **62,554**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	95.172.34.78	Trojan Horse	d3d7d3eadf02eb366d765409c1946547
2.	189.252.185.129	Linux/SQLMap	685bc2af410d86a742b59b96d116a7d9
3.	85.26.167.89	TrojWare.Win32.Ransom.WannaCry.AB@75g	ca71f8a79f8ed255bf03679504813c6a
4.	189.182.76.125	Linux/SQLMap	ae12bb54af31227017feffd9598a6f5e
5.	123.21.97.30	Trojan.Win32.Reconyc.fuzv	0ab2aeda90221832167e5127332dd702

6.	122.52.201.146	Trojan-Ransom.Win32.Wanna.m	414a3594e4a822cfb97a4326e185f620
7.	41.78.64.254	Ransom.Wannacry	02c5f1515bf42798728fac17bfe1e4c1
8.	59.5.151.144	Dropped:Generic.Malware.F!dld!.0204478	996c2b2ca30180129c69352a3a3515e4
9.	5.188.62.194	Trojan.Win32.Swisyn.fsyi	a55b9addb2447db1882a3ae995a70151
10.	217.66.195.27	Trojan.Agent.CZTF	6e72ad805b4322612b9c9c7673a45635

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **91,407** web attacks compared to last week which was **56,645**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 27th of March – 2nd of April, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	20.125.53.209	/jenkins/login
2.	34.239.240.237	/login
3.	83.38.205.249	/manager/html
4.	100.27.43.125	/secure/ContactAdministrators!default.jspa
5.	87.236.212.193	/boaform/admin/formLogin?username=admin&psd=admin
6.	20.106.98.239	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	149.104.12.25	/config/getuser?index=0
8.	3.137.163.28	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	138.68.187.228	/hudson
10.	149.104.11.196	/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.