TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 20th of March – 26th of March, 2022
Report No.: TZ-CERT/WRHP/2022/13

1. NETWORK ATTACKS

A total of **353,352** attacks have been recorded compared to last week **280,113** 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.	164.92.158.213	ubuntu	ubuntu
4.	116.105.216.128	oracle	oracle
5.	116.110.3.253	test	test
6.	58.221.239.31	user	1
7.	5.188.62.196	ftpuser	ftpuser
8.	39.171.36.3	111111	$passwor
9.	142.93.105.47	postgres	abc123
10.	31.184.198.71	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 **62,554** malicious software distributed compared to last week in which was **46,910**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	5.188.62.194	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	217.66.195.27	Linux/SQLMap	844290834b6450425b146d4517cdf780
3.	116.105.216.128	TrojWare.Win32.Ransom.WannaCry.AB@75g	ae12bb54af31227017feffd9598a6f5e
4.	64.112.41.88	Linux/SQLMap	ab27f6c7634e9efc13fb2db29216a0a8
5.	104.156.155.9	Trojan.Win32.Reconyc.fuzv	414a3594e4a822cfb97a4326e185f620

6.	88.80.148.190	Trojan-Ransom.Win32.Wanna.m	ca71f8a79f8ed255bf03679504813c6a
7.	14.99.145.182	Ransom.Wannacry	996c2b2ca30180129c69352a3a3515e4
8.	123.56.144.167	Dropped:Generic.Malware.F!dld!.0204478	bb45cc7019cbe350562be2373eb42267
9.	121.37.180.150	Trojan.Win32.Swisyn.fsyi	0075281ef7cf2dcbc2b45f7d3d963a49
10.	197.149.178.42	Trojan.Agent.CZTF	01bdc6fb077098f4a3b60f4b0e479a7f

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **56,645** web attacks compared to last week which was **6,821**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 20th of March – 26th of March, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	95.217.123.117	/jenkins/login
2.	34.239.240.237	/login
3.	199.48.241.249	/manager/html
4.	20.110.150.251	/secure/ContactAdministrators!default.jspa
5.	103.179.142.129	/boaform/admin/formLogin?username=admin&psd=admin
6.	20.41.224.143	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	79.137.133.136	/config/getuser?index=0
8.	70.39.92.7	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	5.188.211.10	/hudson
10.	5.188.211.16	/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.