



TZ-CERT HONEYPOTS WEEKLY REPORT

Period : 8th of May – 14th of May, 2022

Report No.: TZ-CERT/WRHP/2022/19

1. NETWORK ATTACKS

A total of **327,047** attacks have been recorded compared to last week **348,217** 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.	5.188.62.194	admin	admin
2.	45.141.84.10	guest	guest
3.	116.105.212.31	ubuntu	ubuntu
4.	116.105.216.128	oracle	oracle
5.	171.251.25.38	nproc	nproc
6.	5.188.62.196	user	123456
7.	95.85.42.40	ftpuser	ftpuser
8.	167.172.55.117	111111	P@ssw0rd
9.	5.188.62.250	postgres	abc123
10.	199.188.241.199	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 **324,941** malicious software distributed compared to last week in which was **53,972**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	60.210.9.235	Trojan Horse	685bc2af410d86a742b59b96d116a7d9
2.	154.53.53.44	Linux/SQLMap	ae12bb54af31227017feffd9598a6f5e
3.	35.185.168.157	TrojWare.Win32.Ransom.WannaCry.AB@75g	0ab2aeda90221832167e5127332dd702
4.	35.229.195.26	Linux/SQLMap	ca71f8a79f8ed255bf03679504813c6a
5.	120.77.167.107	Trojan.Win32.Reconyc.fuzv	414a3594e4a822cfb97a4326e185f620
6.	34.81.197.225	Trojan-	02c5f1515bf42798728f

		Ransom.Win32.Wanna.m	ac17bfe1e4c1
7.	34.80.122.111	Ransom.Wannacry	cf4f46336abeec03630297f846d17482
8.	34.81.50.16	Dropped:Generic.Malware.F!dld!.0204478	1584a2b5f74df97054c47543fd945fb2
9.	35.247.134.54	Trojan.Win32.Swisyn.fsyi	25d6d73e9b52d3ab18c5e4f9b435a00c
10.	58.34.196.12	Trojan.Agent.CZTF	2de98404eb4ac4a525ed1884f4ea445b

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **517** web attacks compared to last week which was **5,214**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 8th of May –14th of May, 2022, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP REQUESTS
1.	125.74.8.51	/jenkins/login
2.	199.195.249.217	/login
3.	41.59.90.66	/manager/html
4.	109.74.204.123	/secure/ContactAdministrators!default.jsps
5.	111.229.204.148	/boaform/admin/formLogin?username=admin&psd=admin
6.	101.68.211.3	/boaform/admin/formLogin?username=adminisp&psd=adminisp
7.	114.67.249.200	/config/getuser?index=0
8.	172.104.234.47	/boaform/admin/formLogin?username=ec8&psd=ec8
9.	185.162.235.175	/hudson
10.	198.199.109.11	/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.