



TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 26th March to 1st of April, 2023
Report No.: TZ-CERT/WRHP/2023/13

1. NETWORK ATTACKS

A total of **235,672** attacks have been recorded compared to last week **95,892** 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.	43.156.239.229	root	admin
2.	152.67.37.182	admin	support
3.	116.98.165.107	support	123456
4.	116.105.215.107	PlcmSplp	admin1234
5.	193.105.134.95	guest	password
6.	195.3.147.52	user	PlcmSplp
7.	116.110.76.100	test	alpine
8.	171.251.22.1	default	root
9.	116.98.163.96	jenkins	abc123
10.	116.105.222.208	git	(empty)

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 the 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 **313,951** malicious software distributed compared to last week in which was **99,387**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.78.64.254	Trojan:Linux/Multiverze	d4d8cbf1a0b4a7617b6 f3a7ced737c123ed3a3 da20192862a84c1f6f7 dc75edf
2.	41.59.86.254	Trojan.Gen.NPE	a04ac6d98ad9893127 83d4fe3456c53730b21 2c79a426fb215708b6c 6daa3de3
3.	41.59.211.41	trojan.linux/hajime	020f1fa6072108c79ed 6f553f4f8b08e157bf17f 9c260a76353300230fe d09f0
4.	129.227.76.238	UDS:Backdoor.Linux.Mirai	dadd035cac52ae08767

			a9aea15761678f8a3eb ad09f55d3a36e220538 7a15bcd
5.	196.20.73.69	trojan.linux/hajime	d5601202dff3017db23 8145ff21857415f66303 1aca9b3d534bec8991b 12179a
6.	91.238.185.252	trojan.linux	ab31ea17ea415efd30a 19fdb7a68b92146692b 76584007cbbb94f55b9 761b8dc
7.	41.59.203.31	trojan.linux	8c5e2b96cb61ebb3750 f5be23fc9aca14d7ac97 efb7d57afebd85472dcc 8e015
8.	109.234.117.66	Trojan.Linux.Generic.2461 92	e6ce9937266d30a22c6 aa5c48d818dba86491 b1becf1fe0ca07b3de85 d2d88ab
9.	185.216.132.224	HEUR:Trojan- DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800 886311d208b4387a06 9b5b06f82a3c1c7cd61 67e90be
10.	41.93.47.66	Trojan.Win32.Eb.dqb	b0c1267102b7596000f 1b48965c0936b58cd18 aae35a1de97a4cf2517 18a1946

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **3,154** web attacks compared to last week which was **4,011**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 26th March to 1st of April, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	77.68.50.167	/users/sign_in
3.	79.151.37.125	/boaform/admin/formLogin
4.	193.32.162.159	/recordings/
5.	41.78.174.77	//ajax.php?yokyok=ls
6.	185.203.122.25	/favicon.ico

7.	152.89.196.54	/robots.txt
8.	109.237.96.251	/.env
9.	185.225.74.42	//_asterisk/
10.	41.78.174.124	//rr.php?yokyok=ls

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.