



TZ-CERT HONEYPOTS WEEKLY REPORT

Period : 12th of February –18th of February, 2023

Report No.: TZ-CERT/WRHP/2023/7

1. NETWORK ATTACKS

A total of **533,081** attacks have been recorded compared to last week 330,505 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.	45.249.100.22	root	admin
2.	180.210.186.158	admin	123456
3.	92.205.185.136	PlcmSplp	PlcmSplp
4.	143.198.115.111	support	support
5.	171.225.184.179	guest	password
6.	193.105.134.95	user	12345
7.	52.77.80.158	supervisor	1234
8.	69.70.184.254	test	root
9.	195.3.147.52	Admin	Win1doW\$
10.	171.225.185.105	default	(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 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 **1,168,494** malicious software distributed compared to last week in which was **1,179,167**.

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.86.254	Backdoor:HTML/Derflop.A	d8c8eaf6eb2313e6921 b375fc3099456d1c6b7 b656f181c359541628c 37bbca7
2.	41.59.211.41	Trojan.Generic.31654391	94dfff36061e989490ab f4b5ec7dcb7c70f89af6 136fecc632cdfdd3ca39 c223
3.	41.59.203.31	Trojan:Linux/Multiverze	ab0d10aaa8dd7f2e5d6 769cb7f09f533f22cd77 b501ea185722fcaad15 029414
4.	196.41.222.98	HEUR:Trojan.Linux.Agent.	b9e643a8e78d2ce745f

		gen	be73eb505c8a0cc4984 2803077809b2267817 979d10b0
5.	196.41.222.5	Trojan:Win32/CryptInject!M SR	39b1042a5b02f392514 1733c0f78b64f9fae71a 37041c6acc9a9a4e707 23a0f1
6.	41.78.64.254	Trojan.Linux.Generic.2461 92	48409bbbe5559ec2ea e71fcd8dcdb5ebe7472 ef864eabdcda427660 287e0fc
7.	41.59.201.9	Linux.MiraiTrojan.Linux.Ge nericKD.40003689	ea40ecec0b30982fbb1 662e67f97f0e9d6f43d2 d587f2f588525fae683a bea73
8.	41.59.203.192	Trojan.Linux.GenericKD.40 003689	a37b519f4146749aef1 e3ff0d5a76ef4cf96599 27a4a4db527e22309cc 988cd0
9.	41.59.200.32	HEUR:Trojan- DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800 886311d208b4387a06 9b5b06f82a3c1c7cd61 67e90be
10.	41.59.201.3	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 **6,874** web attacks compared to last week which was **10,454**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 12th of February, 2023 – 18th of February, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	150.95.183.161	/users/sign_in
3.	72.251.235.155	/config/getuser?index=0
4.	193.32.162.159	/.env
5.	183.136.225.32	/boaform/admin/formLogin
6.	143.244.50.172	/admin/config.php

7.	109.237.96.124	/favicon.ico
8.	103.140.108.108	/admin/config.php?password%5B0%5D=ZIZO&username=admin
9.	112.199.166.188	/robots.txt
10.	115.165.224.54	/client/get_targets

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.