TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 19th of February –25th of February, 2023
Report No.: TZ-CERT/WRHP/2023/8

1. NETWORK ATTACKS

A total of **672,978** attacks have been recorded compared to last week **533,081** 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.	77.93.239.114	admin	123456
3.	171.251.31.66	PlcmSplp	alpine
4.	171.225.184.214	support	guest
5.	116.105.217.85	guest	password
6.	190.171.169.70	user	123456
7.	193.105.134.95	supervisor	Win1doW$
8.	195.3.147.52	hadoop	1234qwer
9.	183.129.167.10	admin	admin1234
10.	116.110.1.181	test	(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 **1,539,475** malicious software distributed compared to last week in which was **1,168,494**.

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	d8c8eaf6eb2313e6921b375fc3099456d1c6b7b656f181c359541628c37bbca7
2.	41.59.211.41	Trojan.Generic.31654391	832240fe35411f451b435bf46370063be163d682d62805ddce18fe421d39acc1
3.	41.59.203.31	Trojan:Linux/Multiverze	94dfff36061e989490abf4b5ec7dcb7c70f89af6136fecc632cdfdd3ca39c223
4.	41.59.200.32	HEUR:Trojan.Linux.Agent.	055ed8915741346a7ff

		gen	a1abab6f45f3ffb69ae4717216567418f8ec10f66337e
5.	196.41.222.98	Trojan:Win32/CryptInject!MSR	39b1042a5b02f3925141733c0f78b64f9fae71a37041c6acc9a9a4e70723a0f1
6.	196.41.222.5	Trojan.Linux.Generic.246192	48409bbbe5559ec2eae71fcfd8dcdb5ebe7472ef864eabdcdca427660287e0fc
7.	41.78.64.254	Linux.MiraiTrojan.Linux.GenericKD.40003689	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	5.63.164.90	Trojan.Linux.GenericKD.40003689	a37b519f4146749aef1e3ff0d5a76ef4cf9659927a4a4db527e22309cc988cd0
9.	119.197.192.20	HEUR:Trojan-DDoS.Linux.Xarcen.d	7aa6518ffe1f152fe800886311d208b4387a069b5b06f82a3c1c7cd6167e90be
10.	41.59.201.3	Trojan.Win32.Eb.dqb	b0c1267102b7596000f1b48965c0936b58cd18aae35a1de97a4cf251718a1946

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **5,946** web attacks compared to last week which was **6,874**.

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 19th of February, 2023 – 25th of February, 2023, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	62.166.215.87	/users/sign_in
3.	193.32.162.159	/favicon.ico
4.	72.251.235.155	/boaform/admin/formLogin
5.	185.224.128.249	/admin/config.php
6.	138.197.9.106	/.env

7.	34.229.66.104	/json/
8.	185.246.220.98	/config/getuser?index=0
9.	152.89.196.211	/robots.txt
10.	109.237.96.124	/recordings/

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.