TZ-CERT HONEYPOTS WEEKLY REPORT
Period : 7th to 13th of May, 2023
Report No.: TZ-CERT/WRHP/2023/19

1. NETWORK ATTACKS

A total of **209,111** attacks have been recorded compared to last week **126,711** 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.	116.98.167.167	root	admin
2.	171.251.31.108	admin	123456
3.	195.3.147.52	user	12345
4.	193.105.134.95	guest	password
5.	116.98.168.231	support	1234
6.	116.110.64.37	ubnt	(empty)
7.	171.251.23.239	test	user
8.	116.105.220.36	(empty)	root
9.	151.245.3.74	oracle	ubnt
10.	95.214.27.202	ftpuser	1111

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 **637,707** malicious software distributed compared to last week in which was **203,205.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	41.59.194.240	trojan.linux/mirai	77a2c317ca9d43acc056cf8217a8c838d23af63965b33dc931877360d5919b8d
2.	41.59.211.41	trojan.linux/mirai	d42fef60e13ef1c7ccb1039044bbf307c5d4417a7abf0b271956cef6e2d593be
3.	41.59.86.254	downloader.linux/medusa	9942e0050835a2ded6ac90fc886c3100484a08c6ee08dbfb47d3442b2815ad98

4.	41.59.201.132	trojan.mirai/linux	746a154e5586816d0c3c63a84a7974135135b0b6b54f452018a20ad43fe11835
5.	41.59.200.32	trojan.linux	1d27289b1bc725c3ff2eac41a1b95036db76c3e4e40d3f227a92bf8274e6d6f9
6.	171.5.179.160	trojan.linux	77ccd5ae0a102102b1c2032ff7f1fa8cc2f1069276f964210e644e1b21d8dd1f
7.	41.59.203.192	trojan.linux/xorddos	9ec9a97605509da77411ab9b0267c25fb8074e36e2d96adb50a144d6dcf35620
8.	78.187.16.72	trojan.shelm/prometei	39b1042a5b02f3925141733c0f78b64f9fae71a37041c6acc9a9a4e70723a0f1
9.	41.59.196.23	Trojan.Win32.Eb.dqb	746a154e5586816d0c3c63a84a7974135135b0b6b54f452018a20ad43fe11835
10.	41.59.208.30	trojan.linux/zuzcj	8f8b809140a5a77a7f4c8e2ac73567be2e000510c786e29aab1d45763eaaf216

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **2,733** web attacks compared to last week which was **2,627.**

From the table the top 10 web-based attacks and their associated requests sent to web servers for the period between 7th to 13th of May, 2023 are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	122.168.198.123	/
2.	109.237.96.251	/users/sign_in
3.	152.89.196.144	/boaform/admin/formLogin
4.	109.237.96.124	/favicon.ico
5.	45.146.15.40	/robots.txt
6.	165.154.119.27	/.env

7.	41.78.174.124	/sitemap.xml
8.	41.78.75.186	/.well-known/security.txt
9.	41.78.169.54	/geoip/
10.	45.95.169.240	/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.