TZ-CERT HONEYPOTS WEEKLY REPORT
Period: 31st December 2023 to 6th of January, 2024
Report No.: TZ-CERT/WRHP/2024/1

1. NETWORK ATTACKS

A total of **2,636** attacks have been recorded compared to last week **103,359** attacks within the period of this report. The top 10 Network attacks with malicious IPs, commonly used usernames and passwords are as in **table1** below:

SN	ATTACKING IPS	USERNAMES	PASSWORDS
1.	218.92.0.124	root	user
2.	139.59.75.17	admin	admin
3.	193.105.134.95	user	root
4.	146.190.159.96	guest	(empty)
5.	185.246.128.133	ubnt	1234
6.	62.210.66.43	Admin	123456
7.	164.92.67.89	(empty)	password
8.	64.23.150.81	supervisor	ubnt
9.	41.78.75.186	pi	12345
10.	95.181.239.8	support	guest

Table1: Top 10 Network attacking IP

Most of the usernames and passwords listed are commonly used, thus its advised review of usernames and passwords be made to avoid use of the above listed credentials and default ones. The use of password policies is the best practice.

2. MALICIOUS SOFTWARE (MALWARE)

During the week the sensors recorded, a total of **4,351** malicious software distributed, compared to last week in which was **43,748.**

Below listed are top ten malicious software and their hashes.

SN	ATTACKING IPS	MALICIOUS SOFTWARE	HASHES(SHA256)
1.	115.210.123.130	downloader.medusa/shell	fef1d976e94d87fc8ebcacd50f46ce5061a380d9f59ccb69093c860bf509bf52
2.	200.115.206.57	downloader.medusa/shell	45ceee2eb58c0502a87302b834e8acd5a24a822243646d324260debe1784e825
3.	196.249.224.30	Riskware/CoinMiner	2d4af503d71c8d5ebedb020adea78e35bc37c5456dd15611f5e98c90cbb3d095

4.	60.182.7.195	downloader.medusa/shell	5a72573e99f89a16f854ec47c5547d423b266f4cf5374f45019bc0729bde6e9e
5.	154.43.65.7	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
6.	36.33.24.202	trojan.hajime/genericrxic	d5601202dff3017db238145ff21857415f663031aca9b3d534bec8991b12179a
7.	35.180.203.18	trojan.xorddos/ddos	ea40ecec0b30982fbb1662e67f97f0e9d6f43d2d587f2f588525fae683abea73
8.	101.43.39.117	trojan.malxmr/multiverze	51b052a524af278366fb5527d4a5eee949b63f85168c37d4f97aefe3e73fe66a
9.	185.151.84.42	trojan.generica/xorddos	d2dda52df6dc7681b6bc687732dff93f8292adaa8b1ae95eb1a31c80547240d5
10.	41.59.211.41	trojan.genericrxss/r002c0pjf23	94f2e4d8d4436874785cd14e6e6d403507b8750852f7f2040352069a75da4c00

Table2: Top 10 Malicious attacking IP

3. WEB ATTACKS

During the week the sensors recorded a total of **1,309** web attacks compared to last week which was **1,371.**

From the table below, the top 10 web-based attacks and their associated requests sent to web servers for the period between 31st December, 2023 to 6th of January, 2024, are detailed. The requests are the payloads.

SN	ATTACKING IPS	TOP URI
1.	47.106.35.122	/
2.	115.127.35.125	/users/sign_in
3.	128.199.21.147	/favicon.ico
4.	94.225.49.250	/.env
5.	51.159.99.244	/boaform/admin/formLogin
6.	83.97.73.245	/robots.txt

7.	106.13.11.119	/actuator/gateway/routes
8.	78.153.140.37	/project/.env
9.	41.78.75.186	/.git/config
10.	115.227.19.195	/?XDEBUG_SESSION_START=phpstorm

Table3: Top 10 web attacking IP

4. RECOMMENDATIONS

The Honeypot sensors have recorded IP addresses with the 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 the 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 counteract, 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 it to flag the detection of attacks associated with the list of resources provided especially the IP addresses and the web requests.