

## Task 2 :- Analyze a Phishing Email Sample.

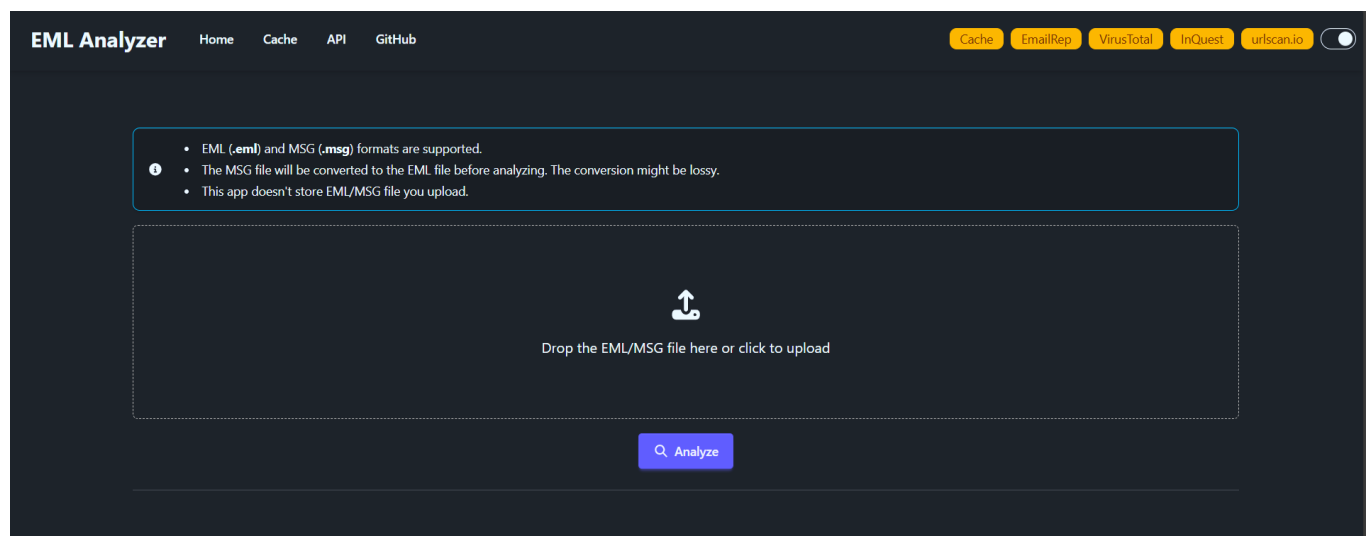
### Step 1 :-

Obtain the phishing email file with .eml extension.

File I got from :- [30-Days-SOC-Challenge-Beginner/Challenge#5/Day#22- Phishing Analysis: Suspicious Lookalike email.md at main · Oxrajneesh/30-Days-SOC-Challenge-Beginner · GitHub](#) .

### Step 2 :-

Let's examine the senders email address using EML Analyser.



Basic headers	
Message ID	<20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>
Subject	CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!
Date (UTC)	2023-09-19T18:35:49Z
From	banco.bradesco@atendimento.com.br
To	phishing@pot

Through this we are able to get the email id of sender and receiver and also to find the ip address through which the mail is been send.

### Step 3 :-

Analyze a header of the email using MX Toolbox (it is a multipurpose tool or software but we are going to use it for Header Analyser).

### Analyze Header

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, [just read this tutorial](#).

◀ Analyze New Header

Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Here we have found the suspicious attachments like :-

### 1. DMARC Compliant (No DMARC Record Found):

No DMARC record exists; the domain isn't protected from email spoofing.

## 2. SPF Alignment:

Checks if the “From” domain matches the domain in the SPF record.

### 3. SPF Authenticated:

Verifies if the sending server is authorized in the SPF record.

#### 4. DKIM Alignment:

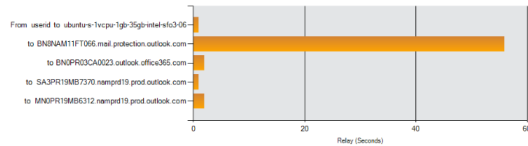
Checks if the domain in the DKIM signature matches the “From” domain.

## 5. DKIM Authenticated:

Verifies if the DKIM signature is valid and the email wasn't altered.

## Relay Information

Received Delay:	57 seconds
-----------------	------------



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	userid	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06		9/19/2023 6:35:49 PM	
2	55 seconds	ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 137.184.34.4	BN8NAM11FT066 mail.protection.outlook.com 10.13.177.138	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:44 PM	✖
3	1 Second	BN8NAM11FT066 eop-nam11.prod.protection.outlook.com 2603:10b6:408:e6:cafe::23	BN0PR03CA0023 outlook.office365.com 2603:10b6:408:e6:28	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:45 PM	✔
4	0 seconds	BN0PR03CA0023 namprd03.prod.outlook.com 2603:10b6:408:e6:28	SA3PR19MB7370 namprd19.prod.outlook.com 2603:10b6:806:317::17	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	9/19/2023 6:36:45 PM	✔
5	1 Second	SA3PR19MB7370 namprd19.prod.outlook.com ::1	MN0PR19MB6312 namprd19.prod.outlook.com	HTTPS	9/19/2023 6:36:46 PM	✖

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

## Step 4 :-

Look for any suspicious links or attachments.

text/html

tos por milhas aéreas<span> </p>

<p style="font-family: 'Signika', sans-serif; font-weight: 300; color: #ffff; font-size: 14px; line-height: 18px; margin: 0px; padding: 0px;"><span style="font-weight: 500;">Descontos de até 35% na fatura do cartão</span> </p>

<p style="font-family: 'Signika', sans-serif; font-weight: 300; color: #ffff; font-size: 14px; line-height: 18px; margin: 0px; padding: 0px;"><span style="font-weight: 500;"></span></p>

</td>

<td width="40%" style="padding-right: 20px;">

<div style="border-left: 1px solid #fff; padding-left: 40px; padding-top: 0px; padding-bottom: 0px;">

Para visualizar as imagens deste email. [Clique aqui](#)

**Banco do Bradesco (Lívolo).**

Você possui **Pontos Lívolo com seu cartão Banco do Bradesco** disponíveis para resgate que expiram HOJE, evite a perda destes pontos realizando agora mesmo o resgate da sua Pontuação Visa Infinite.

Você Clientes **Banco do Bradesco** acumulam pontos livelo todas as vezes que utilizam seus cartões na função débito ou crédito, é rápido e fácil de acumular.

**Troque seus pontos por milhas aéreas** **92.990**

Content-Type text/html

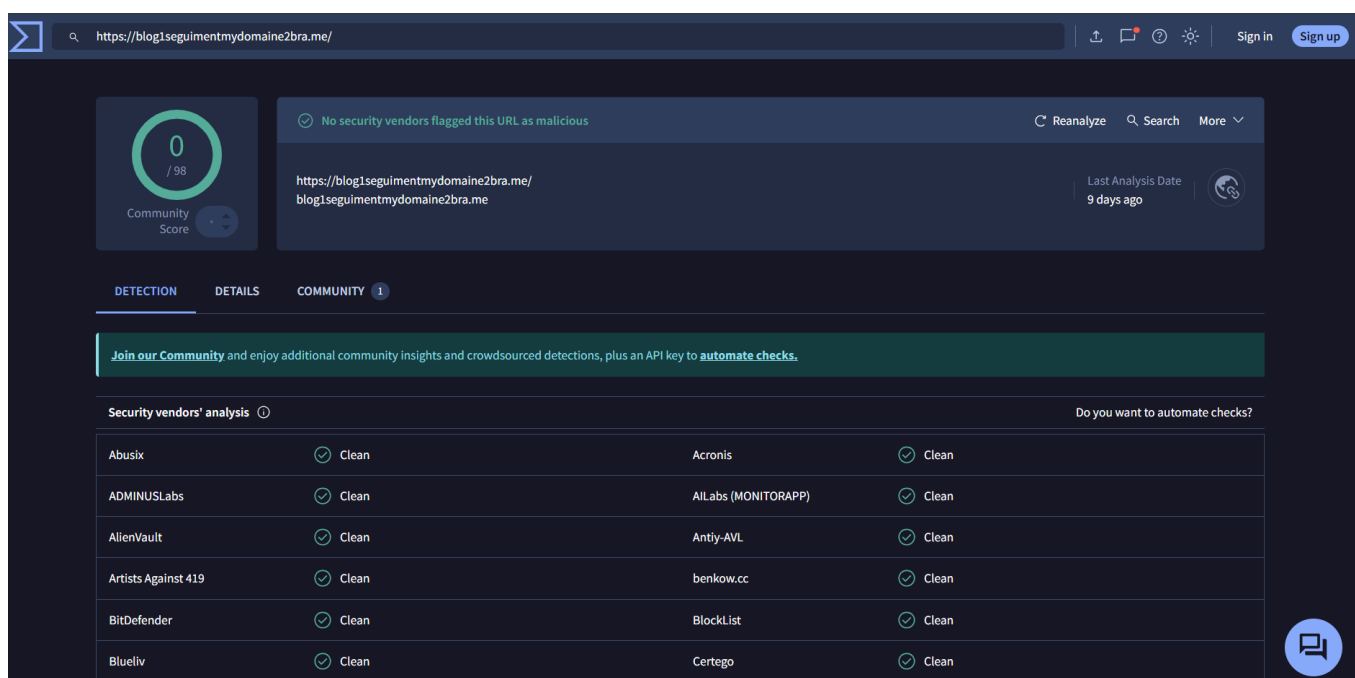
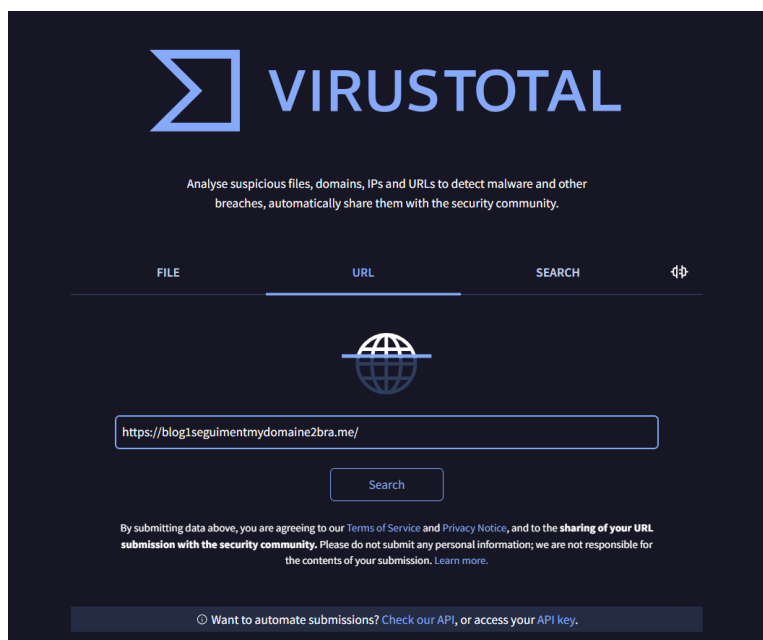
Extracted URLs <https://blog1seguimentmydomaine2bra.me/>

Extracted domains [blog1seguimentmydomaine2bra.me](https://blog1seguimentmydomaine2bra.me/) [fonts.gstatic.com](https://fonts.gstatic.com/) [fonts.googleapis.com](https://fonts.googleapis.com/)

Here we found the suspicious link stating click here (or Clique aqui).

## Step 5 :-

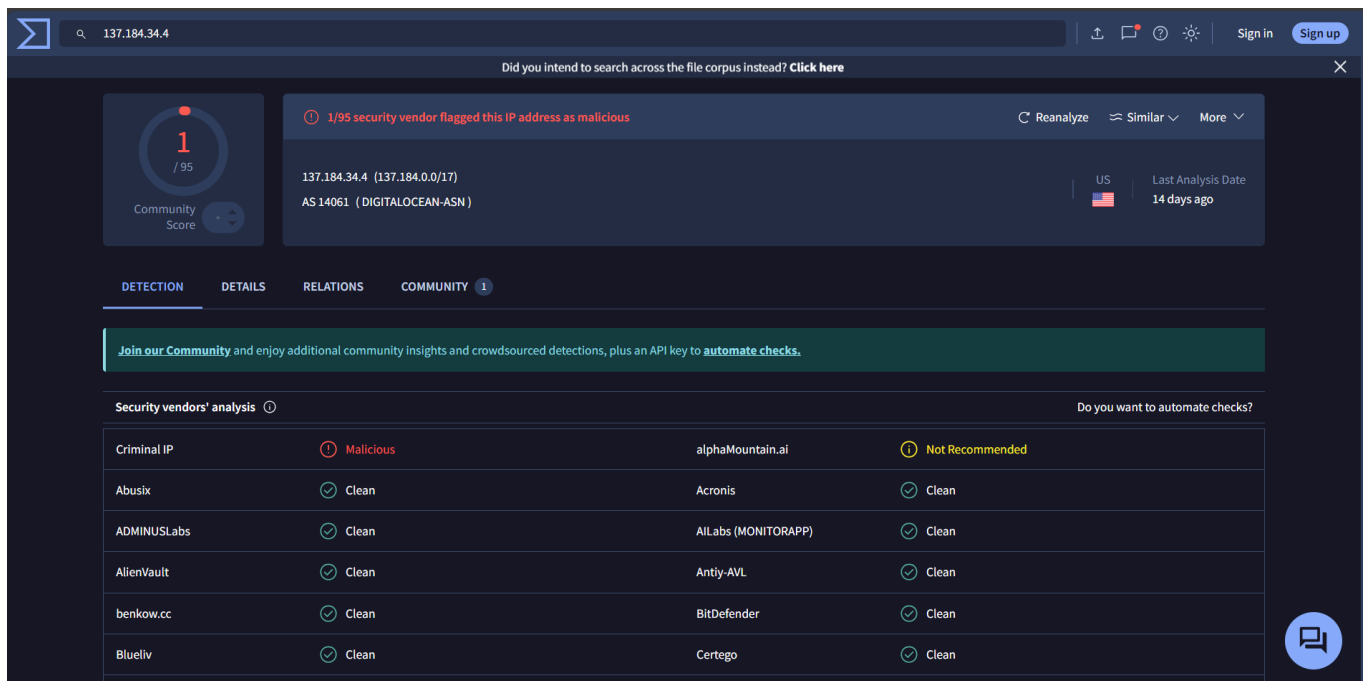
Analyze this links using VirusTool.



Using this software, we are getting clean link but the link is not clean as the software might has the pre-stored lines of code that they analysis and store it as a signature and if few of the lines gets interchange then these signature matching gets' failed and result's us as the non- suspicious link or any files.

Step 5 :-

Let's search about the ip address that we have found or the senders address.



A malicious link has been discovered.